Cybersecurity Trends

UK edition n.3 / 2022

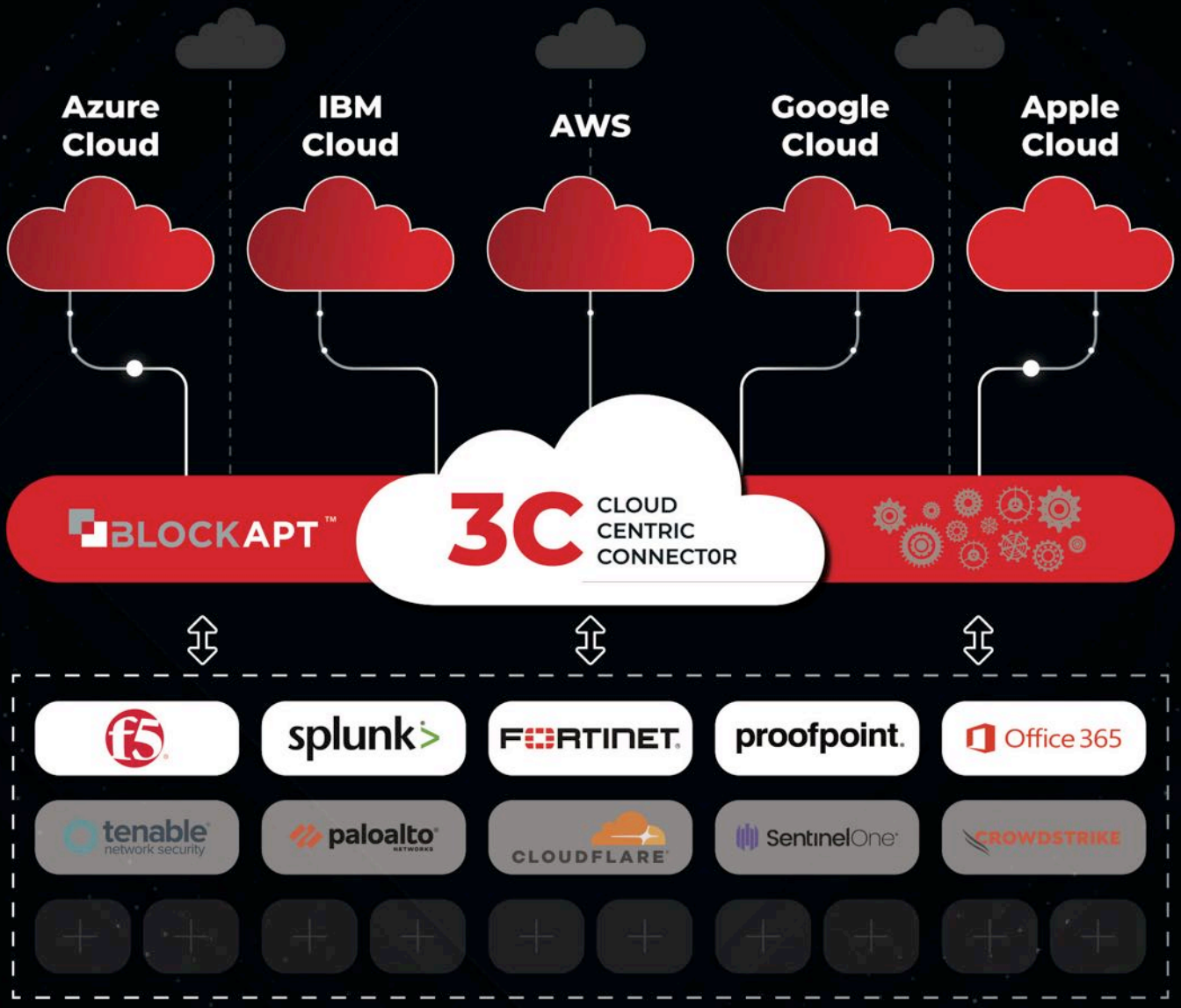
VIP Interview - A conversation with Walt Greene

BLOCKAPT™

Espionage… Crypto... Insider Threats...

BLOCKAPT™

Centralised Cloud Management & Native Control



- Seamless Orchestration
- Optimise your Cost & Efficiency
- Automated Config Management

blockapt.com

Contents

A dangerous world, even when encrypted...



Authors: Raj Meghani, Marco Essomba, Laurent Chrzanovski

This issue reveals the multiple aims of espionage, irrespective of whether it's state-sponsored or not. As part of a huge non-regulated market, you can now buy the most sophisticated espionage tools via "Business Intelligence Services" companies, which – upon extra cost – will discharge you from any legal binding matter around the means they will use to gather the data you demand. We are living in the most highly developed and persistent cyber espionage times, which have brought critical infrastructures, companies, and people down on their knees. It's a cut-throat world that has no limits.

You no longer need to buy a $2.5 million piece of spyware: as Jack Schafer and Marvin Karlins demonstrate so vividly in their article. Knowing how a corporation works and the fact that besides directors, specific department employees have never even actually met with other department members, makes it easier to deploy a malicious spear-phishing email which can open access to the most remote server gates...

As the Davos 2022 Cybersecurity report states, more than 80% of successful attacks were made possible by an insider – mostly by forgetting the security policies but, more and more, by ego or for money. Read about the solutions you can easily use to prevent this risk from the outset. There is no room for complacency here, as Raj Meghani references in her article, pressing for companies to stay on top alert.

Finally, we venture into the world of all things crypto, and the challenges virtual currencies bring with encryption vulnerabilities. Today, the most powerful cyber-criminal groups utilise both quantum computing and artificial intelligence within their attack toolkit.

And the perfect example of reformulation – or constant evolution – takes us to blockchain technologies. Walt Greene sheds a professional light on what blockchain has been, what it is now and what it could become tomorrow. It's a fascinating insight into Walt's mindset and how a new wave of technology in the form of a decentralised network architecture will shape and change the way in which humans interact with digital technologies.

Enjoy this issue with its thought-provoking articles and pay heed to the words of caution: The biggest threats are often those staring you straight into your eyes – you just don't know it. Until it's too late. ■

Cyber espionage - from detection to counteraction.

Author: General Anton Rog

Cyber espionage, usually carried out through *Advanced Persistent Threat* (APT) cyber operations, is the main cyber threat to Romania's national security, given that such activities are aimed at obtaining strategic information from networks and information systems with critical value for national security.

BIO

Brigadier General Anton Rog is Director of the National Cyberint Centre of the Romanian Intelligence Service (SRI). Cyberint is responsible for conducting 24/7 activities to proactively discover, characterise and combat cyber threats against systems and networks critical to Romania's national security. Anton Rog has held numerous technical development positions, including software and systems design. He was also Deputy Director of the central SRI IT&C department. He is active with the academic community as an associate professor at DRESMARA Brasov. Anton Rog graduated from the University of Bucharest in 1998 with a B.S. degree in Information Technology, and in 2011 he obtained a postgraduate degree in Program and Project Management from DRESMARA. He was appointed Knight of the Order of Man and Faith in 2014 and Knight of the Order of Military Virtue in 2005 by two presidents of Romania.

For a better conceptual clarification of cyber espionage operations, it is necessary to briefly review some elements of the international legal framework applicable in cyberspace, with reference to the Tallinn Manual 2.0[1], the Vienna Convention on Diplomatic Relations and the Vienna Convention on Consular Relations, as follows:

- **Cyber operation** - an action in cyberspace that may cause inconvenience or disruption to computer systems, but does not cause physical damage. It can be part of a cyber attack.
- **Cyber attack** - a defensive or offensive cyber operation capable of causing physical and/or human damage.
- **Cyber espionage** - activity conducted clandestinely using cyber capabilities to obtain information. The targets of cyber espionage can be both states and commercial entities.

Although a cyber attack causes physical damage, such as the disabling of networks and computer systems or the loss of financial assets, cyber operations are carried out to steal information, usually of strategic value, from government networks and systems.

Thus, depending on the objectives targeted, cyber espionage can be of two types: strategic-political and economic-industrial. As regards strategic-political cyber espionage, it mainly targets major government institutions in order to obtain information in areas such as defence, foreign affairs, internal affairs or intelligence. Economic-industrial espionage is carried out to gain economic advantage by obtaining intellectual property from research and development institutes and private companies.

Beyond this differentiation, these types of cyber attacks involve substantial financial resources, in the order of millions of euros, and are characterised by the high level of complexity of the applications and infrastructures used, including the exploitation of 0-day vulnerabilities.

In this context, it is worth noting that cyber espionage operations target institutions in several states simultaneously, without being designed specifically for a particular state, but rather for an area.

Stages of a cyber espionage operation and elements of modus operandi

Targeting

In the first stage, known as *targeting*, the attacker establishes the targets of the cyber espionage operation, in relation to the objectives he sets and the specifics of the state/organisation from which he seeks to extract information. There are situations when the actual activities may be carried out by other hostile cyber groups, thus creating a close coordination relationship.

Recognition

Later, in the *reconnaissance* stage, the attacker begins an extensive process of getting to know the target, through means such as open sources, passive interaction with the target, or acquiring such data from specific forums. It also aims to provide knowledge of the architecture of the victim's networks and systems.

Custom malware development

Based on previous activity, attackers develop a complex of malware and other technical tools, each performing specific functions in the future cyber espionage operation. *Exploits* are also used to ensure specificity and adaptability for each individual victim. It is also at this stage that the method of infecting the victim is determined, the most commonly used technique being *spear-phishing*.

Data extraction methods

In the experience of the National CYBERINT Centre, hostile cyber actors use a variety of methods to extract data from target infrastructures, such as:

- Creating a dedicated server/partition on which the data to be extracted, encrypted and segmented into packets is moved in order to optimise the process and reduce the risks of identification;
- Creating mailboxes on the organisation's dedicated server whose usernames are similar (by replacing some letters with numbers or capital letters) to those of employees in the organisations concerned and extracting data packets by sending e-mails with attachments;
- Steganography - the use of photographic or video files already on the targeted network to hide and manipulate files that are desirable to be extracted.

In order to make the extraction of data of interest more efficient, attackers can use *malware* types that have search engines that index the items of interest on the targeted server, which are usually names of dignitaries.

Detecting cyber espionage operations

It is clear that the increased sophistication of these operations often makes it impossible for standard solutions to detect them, so artificial intelligence-based technologies are becoming the ally of cybersecurity experts, making it possible to identify cyber threats by analysing anomalies in network behaviour.

In order to make detection more difficult with artificial intelligence-based solutions and to ensure persistence for long periods of time, cyber attackers can perform optimisations of the victim's network configuration. Furthermore, attackers create multiple *backdoor* paths into the network to ensure that even though they have been detected and removed from the network, they can resume their activity and make lateral moves within the network.

Specific investigative methods, such as *reverse engineering* or analysis of compromise and/or attack indicators, have shown us that attackers have a long presence in the victim network, often being detected after years of presence.

Such cyber operations have also been identified in real time by the National CYBERINT Centre, including through the use of cybersecurity solutions based on artificial intelligence, but also by leveraging information sharing with similar organisations.

After detection, in order to mitigate the effects of a cyber espionage operation, it is necessary to conduct a public attribution, *blame and shame*, process to discourage actors of cyber operations from giving up or at least making it impossible for them to use the same technical methods and tools. Although few will be the cases where state actors will give up, *blame and shame* approaches provide a pause in activity and force new investment and reconfiguration on the part of attackers. ■

1 Coordinated research work at the NATO Cyber Defence Centre of Excellence (CCDCoE)

Economic and industrial espionage and cyberspace.

Author: **Olivier Kempf**

The cyber revolution has been going on for almost forty years now. Computing started with powerful computers but remained a matter for large professional structures. Everything changed in the 1980s with a revolution that went through several phases:

- 1980s: arrival of the *personal computer* (the PC, in its DOS-Windows and Mac versions);
- 1990s: eruption of the Internet: computers communicate with each other. A web is set up;
- 2000s: Arrival of Net 2.0 with the multiplication of blogs and other personal websites. From now on, the individual is no longer a consumer of information, s/he becomes a producer. Their traffic is analysed by massive data algorithms *(Big Data)*. The GAFAMs are taking off.
- 2010s: widespread use of *smartphones*. Connectivity becomes ultra mobile. New artificial intelligence techniques (using neural networks and machine learning) become widespread. *Cloud computing* becomes the norm.
- 2020s: The current wave is expected to build on the implementation of 5G and the massification of increasingly autonomous connected objects.

These successive waves have brought about a real anthropological revolution. Our societies now operate entirely on the basis of cyberspace and its multiple layers (physical, software and information). What affects the citizen has also turned the business world upside down.

In the past, IT modernisation came from the business world to the individual. Now, the company is obliged to carry out two activities simultaneously: on the one hand, an increase in its equipment and the digitalisation of its procedures.

Today, a medium-sized company uses dozens of professional software packages and hundreds of machines, servers and cloud services: all of this is for its internal operations.

BIO

After a military career in addition to operations, he was involved in international affairs and transformation, General (ret.) Olivier Kempf is an independent consultant and associate researcher at the FRS), He is the author of "Introduction à la cyberstratégie" and "Gagner le cyberconflit, comment lutter dans l'espace sémantique" (Economica). He is the director of publication of La Vigie, a strategic synthesis firm he founded in 2014, which publishes a bi-monthly newsletter and writes various studies for its clients.

At the same time, it has to modify its procedures in depth to take account of the radical decentralisation of behaviour: relations with employees who have to be increasingly mobile, a trend accentuated by teleworking; but also relations with customers, as more and more B-to-C commercial activities are now carried out online. This explosion in IT usage brings with it obvious cybersecurity constraints.

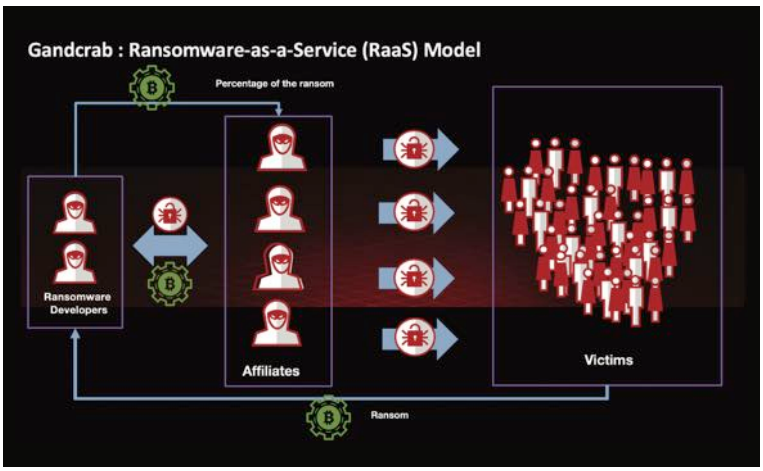
Most companies have taken security measures and Information Systems Security Managers (ISSMs) have become essential links in professional organisations, even if their role is not always properly recognised. However, most of the time, their action is focused on the two primary layers of cyberspace, the physical and the software layer. The informational layer is generally less covered.

Information, at the heart of the third layer, is becoming an essential production factor in contemporary business. It takes many forms. For example, the analysis of customer data via Big Data *(know your customer)* uses micro-data collected in large numbers and processed to provide value.

But specific, more elaborate information is also essential to the company: it may be the price structure of an offer at the time of a commercial negotiation, or research and development projects, or the company's strategic plan. Finally, the range of information processed by the company is enormous.

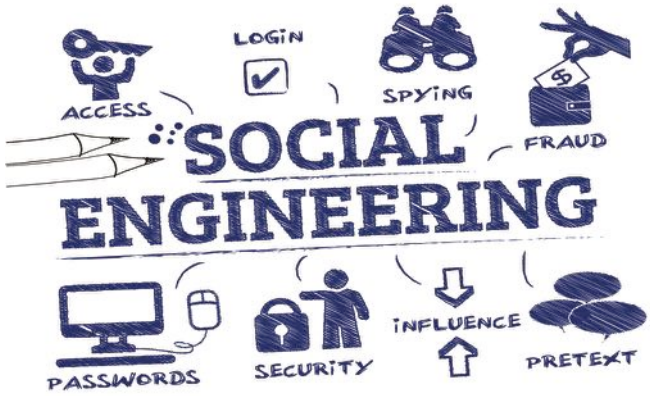
They are obviously not all on the same footing, but basically they are of interest to others: competitors as well as bandits. In the second case, it is a matter of stealing them in order to be paid: either by reselling them to a third party or by holding the company directly to ransom with a coding device (*ransomware* technique).

In this case, the attacker aims to take hostage as much data as possible, whether sensitive or not, but essential to the company's operations. This risk weighs on all companies, whatever their size. In fact, in recent years, this technique has been industrialised *(ransomware as a service)* and all organisations can now be targeted.



Thinking that a small size organsation allows you to fly under the radar is a fatal strategy: just look at the number of small local authorities that have been taken hostage in the last three years. The phenomenon has become even more pronounced with the pandemic, which has forced most organisations to move to teleworking without having anticipated not only the technical aspects of this transition, but above all the security and data protection aspects linked to it.

But behind these criminal activities, it is clear that competitors can also spy on organisations: it is not a question of blocking a company's activity, but of knowing its information capital (what is the status of a particular research project? what is its pricing position? what is its ambition with this customer?) in order to adjust its own strategy.



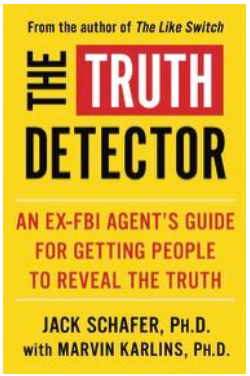
Several techniques exist: a lot of information can be detected by social engineering or so-called open source intelligence: for example, many company employees express themselves on social networks without realising what data they are communicating. But also, competitors can use spying methods, which is fraudulent.

The fact remains that many companies are not aware of these risks and do not see that the dilapidation of their information capital is a major obstacle. Before even thinking about taking measures, there is a need to convince management to become aware of this risk.

This risk is both highly probable and at the same time has maximum effects. Any risk mapping should deal with these risks as a priority. The protection of information capital must therefore become a priority for company management.

This is unfortunately not the case. ■

Hacked by bits and pieces: What can we learn from an example of corporate espionage?



This paper is reproduced and translated thanks to the authors' kind authorisation. Its original version was first published as a short example in Schafer, J. and Karlins, M. (2020) ,The Truth Detector. An *Ex-FBI Agent's Guide for getting people to reveal the truth*,. Simon & Schuster, New York, 144-150 (epub version) then as a full article: Schafer, J. and Karlins, M. (2021), Hacked by Bits and Pieces: What Can We Learn from an Example of Corporate Espionage? *Journal of Information Security*, 12:3, 224-231. (https://doi.org/10.4236/jis.2021.123012)

Authors: Jack Schafer, Marvin Karlins

1. Introduction

As it becomes standard business practice to store proprietary and confidential information on company computers, the need for cybersecurity becomes increasingly important [1] [2].

This need has been highlighted due to numerous security breaches involving organisations well-known to the public, including Adobe, eBay, Equifax, LinkedIn and Yahoo [3] [4].

When well-publicised cases of corporate espionage at major American companies are reported to the public, most people conjure up Hollywood inspired images of darknet super-techno-geeks with banks of computers and James Bond type hacking devices who use their superior knowledge and cutting-edge inventions to blast through firewalls and extract the data they want.

Although this highly sophisticated means of espionage does occur, as was the case with the recent ransomware attack on the Colonial Pipeline (the largest gasoline pipeline in the United States), oftentimes the same results can be achieved through far simpler means.

In fact, all it takes is a person, a cellphone, some readily available software and an action plan to crack through the most advanced corporate security barriers and gain proprietary business information.

The purpose of this paper is to emphasise, through an actual example,

1. How important it is to realise and recognise that each individual in an organisation can be a portal for cyber intrusion; and
2. The need to properly train individuals how to be vigilant for cyber-scams and be wary whenever requests for computer access are made.

2. Procedure

To demonstrate how simple it is for a clever hacker to gain access to computer information—even when that data is protected by advanced cybersecurity measures—we have provided an example of just one such data breach. The authors thank Nathan House, a cybersecurity expert, for supplying us with this eye-opening example of corporate espionage. His challenge—as the would-be hacker—is to break into a secured computer network using only his wits and a cellphone.

3. Results

Nathan's goal is to access a specific Company's computer so he will be able to extract information otherwise unavailable to him. Below, he explains, step by step, what he does and why he does it (what information he is trying to gain).

Call #1: To the Company's Main Switchboard

NATHAN: Hi, I'm having a problem with my desk phone. Can you put me through to someone who may be able to sort this out for me?

RECEPTIONIST: Connecting you.

PHONE SERVICES: Hi.

NATHAN: Hi. I'm having a problem with my desk phone. Sorry, I'm new here. Is there any way I can find out who is calling me when they call my desk phone? Is there a caller ID?

PHONE SERVICES: Not really, because we use hot desks here. [A hot desk is a desk shared by more than one person, sometimes several people over three separate

shifts]. Because people usually use their mobile phones, the caller ID isn't often related to a name. Is this a problem for you?

NATHAN: No, it's fine now. I understand. Thanks. Bye.

I now know that the company uses hot-desks and that phone caller ID is not always expected. Therefore, it is not an issue if I call from outside the company. If it was expected, then I could work around it anyway.

Call #2: To the Company's Main Switchboard

NATHAN: Hi, could you put me through to building security?

RECEPTIONIST: Okay.

BUILDING SECURITY: Hello, how can I help you?

NATHAN: Hi, I don't know if you will be interested, but I found an access card outside the building which I think someone must have dropped.

BUILDING SECURITY: Just return it to us. We are in Building 3.

NATHAN: Okay, no problem. May I ask who I'm speaking to?

BUILDING SECURITY: My name's Eric Wood. If I'm not here, give it to Neil.

NATHAN: Okay, that's great. I will do. Are you the head of building security?

BUILDING SECURITY: It's actually called Facilities Security, and the head is Peter Reed.

NATHAN: Okay, thanks a lot. Bye.

This exchange told me the names of a few people in Security, the correct name of the department and the head of security, and that they are the ones who deal with physical access cards.

Call #3: To the Company's Main Switchboard

NATHAN: Hi, I'm calling from Agency Group Associates and I wonder if you could help me. I had a meeting about a month ago with some of your HR people, but unfortunately my computer crashed and I have totally lost their names.

RECEPTIONIST: Sure, no problem. Let me look up that department. Have you any idea at all of their names?

NATHAN: I know that one of them was the head of HR. There were a number of people at the meeting, though.

RECEPTIONIST: [Pause.] Okay, here we are. Head of HR is Mary Killmister. XXX-XXXX.

NATHAN: Yes, that rings a bell. What are the other names in HR?"

RECEPTIONIST: In HR, Jane Ross, Emma Jones...

NATHAN: Yes, definitely Jane and Emma. Could I have their numbers, please."

RECEPTIONIST: Sure. Jane Ross is XXX-XXXX and Emma Jones is XXX- XXXX. Would you like me to put you through to any of them? NATHAN: Yes. Could you put me through to Emma, please?

I now know the names of the three people in HR, including the department head.

Call #4: To the Company's Human Resources Department

HUMAN RESOURCES: Hello, Emma Jones.

NATHAN: Hi, Emma. This is Eric from Facilities Security in Building 3. I wonder if you can help me. We have had a problem here with the access card database computer. It crashed last night, and some of the data for the new employees got lost. Do you know who would be able to tell us who the new employees were over the last two weeks, as their access cards will have stopped working? We need to contact them and let them know ASAP.

EMMA: I can help you with this. I'll look up the names and email them to you if that's okay. For the last two weeks, did you say?

NATHAN: For the last two weeks, yes. That's great, thanks, but would it be possible to fax it, as we share one computer for email and that was affected by the computer crash, too.

EMMA: Yes, okay. What is your fax number? Oh, and what's your name again?

NATHAN: Mark it to the attention of Eric. I'll have to find out the fax number for you and call you back.

EMMA: Okay.

NATHAN: Do you know how long it will take you to find out the information?

EMMA: It shouldn't take me more than thirty minutes.

NATHAN: Will you be able to start working on it straightaway? It's quite ur- gent.

EMMA: I have a few things to do this morning, but I should have the names by this afternoon.

NATHAN: That's great, Emma. Thanks. When you're done, would you be able to call me straightaway so I can start reactivating their cards?

EMMA: Yes, sure. What is your number?

NATHAN: I'll give you my mobile number. That way you'll be guaranteed to get me. XXX-XXX-XXXX.

EMMA: Okay, sure. I'll call you when I have the list.

NATHAN: Excellent. Thanks. I really appreciate this.

Call #5: To the Company's Main Switchboard

NATHAN: Hello. Could you put me through to IT Support?

RECEPTIONIST: Connecting you... [Long wait in the queue].

IT SUPPORT: Hello, can I have your I S number or your case reference?

NATHAN: I've just got a quick question. Is that okay?

IT SUPPORT: What is it?

NATHAN: A guy from Reuters is trying to send me a presentation and is asking me what the maximum size is for attachments.

IT SUPPORT: It's 5 megabytes, sir.

NATHAN: That's great, thanks. Oh, one more thing. He said it's an .exe file and sometimes those get blocked or something.

IT SUPPORT: He won't be able to send an executable file, as the virus scanners will stop it. Why does it need to be an .exe file?

NATHAN: I don't know. How can he send it to me, then? Could he zip it or something?

IT SUPPORT: Zip files are allowed, sir.

NATHAN: Okay. Oh, one more thing: I can't seem to see my Norton Antivirus icon in my system tray. The last place I worked, there was a little icon.

IT SUPPORT: We run McAfee here. It's just a different icon-the blue one.

NATHAN: That explains it, then. Thanks. Bye.

I now know that to send an executable via email, it will have to be zipped first and less than 5 MB. I also know that they are using McAfee antivirus.

Call #6: A Few Hours Later, a Call from Emma in Human Resources

EMMA: Hi, is this Eric?

NATHAN: Yes, hi.

EMMA: I have the new employees list for you. Do you want me to fax it?

NATHAN: Yes, please. That would be great. How many are there?

EMMA: About ten people.

NATHAN: I'm not sure the fax is working properly here. Could you possibly read them out to me? I think it would be quicker.

EMMA: Okay. Do you have a pen?

NATHAN: Yes, go ahead.

EMMA: Sarah Jones, Sales. Manager is Roger Weaks... [Reads off the rest of the list].

NATHAN: Okay, thanks. You have been a real help. Bye.

I now have a list of the new employees over the last two weeks. I also have the departments they belong to and their managers' names. New employees are many times more susceptible to social engineering (influence or control by an outside source) than long-term employees.

Call #7: To the Company's Main Switchboard

NATHAN: Hi, I'm trying to email Sarah Jones but am not sure what the format of your email addresses are. Do you know?

RECEPTIONIST: Yes. It would be sarah.jones@targetcompany.com.

NATHAN: Thanks.

Social Engineering Email

Minutes later, a spoofed email [email message with a forged sender address] is sent.

> **From:** itsecurity@targetcompany.com.
> **To:** sar.jones@targetcompany.com.
> **Subject:** IT Security.
>
> Dear Sarah, As a new employee with the company, you will need to be made aware of the company's IT security policies and procedures and, specifically, the employee's "Acceptable Use Policy".
>
> The purpose of this policy is to outline the acceptable use of computer equipment at [target company]. These rules are in place to protect the employee and [target company]. Inappropriate use exposes risks, including virus attacks, compromise of network systems and services, and legal issues.
>
> This policy applies to employees, contractors, consultants, temporaries, and other workers at [target company], including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by target company].
>
> Someone will contact you shortly to discuss this with you.
>
> Regards, IT Security

Call #8: A Couple of Hours Later, a Call to the Company's Main Switch-board

NATHAN: Hi. Could you put me through to Sarah Jones, please?

RECEPTIONIST: Connecting you.

SARAH: Hello. Sales. How can I help you?

NATHAN: Hi, Sarah. I'm calling from IT Security to brief you on IT security best practices. You should have gotten an email about it.

SARAH: Yes, I got an email about it today.

NATHAN: Okay, excellent. It's just standard procedure for all new employees and only takes about five minutes.

BIO

Dr. John R. "Jack" Schafer is a retired FBI special agent who is currently employed as an associate professor at Western Illinois University. Dr. Schafer served as a behavioral analyst assigned to the FBI's National Security Behavioral Analysis Program, where he developed many of the ideas presented in this paper. Dr. Schafer earned a Ph.D. in psychology from Fielding Graduate University in Santa Barbara, California. He owns his own consulting company and lectures and consults in America and abroad. He authored a book titled *Psychological Narrative Analysis: A Professional Method to Detect Deception in Written and Oral Communications*. He also coauthored the text *Advanced Interviewing Techniques: Proven Strategies for Law Enforcement, Military, and Security Personnel*. He has published numerous articles on a wide range of topics, including the psychopathology of hate, ethics in law enforcement, detecting deception, and the universal principles of criminal behavior. Dr. Schafer's most recent coauthored book is the bestseller *The Like Switch: An Ex-FBI Agent's Guide to Influencing, Attracting, and Winning People Over.*

BIO

Dr. Marvin Karlins received his Ph.D. from Princeton University in social psychology. He is currently senior full professor of management at the University of South Florida's Muma College of Business. Dr. Karlins consults worldwide and, for twenty years, trained all operational staff at Singapore Airlines. He has published 30 books and more than 150 articles in professional, academic, and popular journals. Several of his co-authored books have become international bestsellers, including *What Every BODY Is Saying: An Ex-FBI Agent's Guide to Speed-Reading People and The Like Switch: An Ex-FBI Agent's Guide to Influencing, Attracting, and Winning People Over*. His most recent book, coauthored with Tony March, is *Paying It Backward: How a Childhood of Poverty and Abuse Fueled a Life of Gratitude and Philanthropy,* and was published in 2020. Dr. Karlins is a member of the Authors Guild and the International Federation of Journalists.

How are you finding things here? Everybody being helpful?

SARAH: Yes, thanks. It's been great. It's a bit daunting starting somewhere new, though.

NATHAN: Yes, and it's always difficult to remember everyone's name. Has Roger introduced you around? [The small talk is designed to build rapport interspersed with trust building.] Emma Jones is very nice in HR if you need any help with that side of things.

SARAH: Yes, Emma did my HR interview for the job.

NATHAN: Well, I better run through the security presentation with you. Do you have your email open? I'll send you the security presentation now and I can talk you through it.

SARAH: Okay, I see the email.

NATHAN: Okay, just double click on the Security Presentation .zip attachment.

SARAH: Okay....

The executable that she ran is, in fact, a cleverly packaged series of scripts and tools created by our wrapper program including within it the RAT (remote access Trojan malware program used to gain control of a computer), a rootkit (allows access to a computer while hiding its existence), a keylogger (keeps track of keystrokes on the computer keyboard), and anything else I may want to add.

When Sarah clicks on the file, the presentation immediately starts. This is just a series of PowerPoint slides telling her not to run executables that she is sent, etc., and other good security practices.

The presentation is branded with all the company logos that were conveniently copied from their public web server, just to add a little more trust. A few seconds later, as she is being taken through the presentation, scripts within the package start to try to disable McAfee and any other PC security that may be found that may help protect the user. Then the rootkit installs itself, hiding all future actions from the operating system or anybody doing a forensic investigation.

Next the RAT is hidden and installed. The RAT is made to start every time the machine reboots, and these actions are all rootkitted and hidden.

The RAT then looks up any proxy settings and other useful information and tries to make its way out of the network and onto the Internet, ready to get its commands from its master. Obviously, all processes and TCP (Transmission Control Protocol) connections are hidden and even running things like netstar (network statistics) and task manager (procedures that can be bused to detect unsanctioned computer manipulation) will not reveal them.

The RAT connects to the master. I now own the PC and it's time to start looking around and really start hacking! Job is done.

4. Discussion

The authors hope that by reading the example just provided, describing the step-by-step calculated takeover of a target company's computer system, employees at all levels of an organisation's hierarchy will become more aware (and recognise) how:

1. Bits and pieces of seemingly harmless and easy-to-acquire information can be used for sinister purposes;
2. Building rapport and trust with a person can make them more likely to become unknowing co-conspirators in a devious undertaking; and
3. How one must be constantly alert not to give out information without carefully considering the authenticity and justification of the source requesting it.

When teaching our students — whether they be at the FBI Academy or the School of Business — we always present them with a quote that reminds them of the role they play in keeping national and/or corporate information safe: "Proprietary information can be protected in locked safes, behind a series of physical and electronic barriers. The weakest link in any security chain is humans. Once a lock is locked, it will not unlock itself ... but a tied tongue easily unties itself." That comment is followed by this observation: "Whenever someone involves you in a conversation—particularly when they are seeking information—don't go into 'automatic response' mode! Think about any possible hidden motive the person talking to you might have as the dialogue unfolds. Be cautious about giving up information, particularly the kinds of data that could be used in identify theft or corporate espionage, and remember that the one piece of information you give up might not seem significant, but, combined with other pieces, might just be the critical item that brings the entire jigsaw puzzle together" [5].

5. Conclusion

The information presented in this article illustrates how bits and pieces of information, carefully and cleverly collected, can lead to a major security breach in an organisation's computer network. It is meant to give the reader an advance warning of just how such a process works so as to reduce the risk of it happening in the future. ■

[1] Brooks, C.J., Grow, C., Craig, P. and Short, D.D. (2018) Cybersecurity Essentials. Sybex, Hoboken. https://doi.org/10.1002/9781119369141

[2] Sai, H. (2019) Next Level Cyber Security. Leader's Press, Santa Barbara.

[3] Swinhoe, D. (2021) The 15 Biggest Data Breaches of the 21st Century. https://www.csoonline.com/

[4] Daswani, N. and Elbayadi, M. (2021) Big Breaches: Cybersecurity Lessons for Everyone. Apress, New York, USA. https://doi.org/10.1007/978-1-4842-6655-7

[5] Schafer, J. and Karlins, M. (2020) The Truth Detector. Simon & Schuster, New York, USA.

Organized by:

NTT DATA

web for your business
swiss webacademy

Hosted by:

COUNTY COUNCIL SIBIU

CYBERSECURITY CONGRESS | SIBIU, 8TH EDITION | SEPTEMBER 21-23 2022

CYBERSECURITY DIALOGUES
ROMANIA, SIBIU
8th Edition - September 21-22, 2022

A WAR-TORN POST-PANDEMIC WORLD: ATTACKS AT 360°

SOLUTIONS FOR SECURING YOUR BUSINESS

www.cybersecurity-dialogues.org

Under the aegis of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

In partnership with:

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GUVERNUL ROMÂNIEI

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

IGPR POLIȚIA ROMÂNĂ

ROMÂNIA CYBERINT SERVICIUL ROMÂN DE INFORMAȚII

Centre de recherche de l'EOGN

CMCS INTERNATIONAL

Gendarmerie nationale

ULBS Universitatea "Lucian Blaga" din Sibiu

Media partner:

BURSA ZIARUL OAMENILOR DE AFACERI

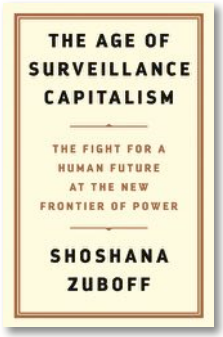
Location: Sibiu County Council - Parliament Hall, Str. Gen. Magheru, Nr. 14

Live streaming upon inscription: www.bursa.ro

Intelligence increasingly relevant in a company's cyber strategy.

Author: Nicola Sotira

We are living in a period that is increasingly characterised by exponential development of technology. Technology that also has within its potential threats to us, namely, the specter of a ubiquitous surveillance architecture that



is active 24 hours a day, 365 days a year. Architecture that, we have seen, serves the interests of large OTTs (Over the Top), i.e., those who manage the buying and selling of our personal data and, importantly, the predictive part of our habits and behaviours. A scenario in which Facebook is now one of the authoritative sources of behavioural models. This economic model is referred to in Zuboff's book as the "Capitalism of Surveillance"; a scenario in which data is the basis of real wars and power movements that challenge even democracies. Also complicating this scenario, is the Russian/Ukrainian conflict that has had major repercussions on NATO countries in terms of cyber warfare. As I prepare this article, newspapers are reporting on attacks by pro-Russian groups on government organisations and financial institutions.

These developments have reshaped the role of intelligence by powerfully inserting it into organisations' cybersecurity strategies. But what are we talking about? What is the meaning of the acronyms we read in the newspapers? The relationship between intelligence in the physical world and that implemented in the digital world?

BIO

Head of CERT at Poste Italiane Group, Nicola has been working in the field of IT and network security for over twenty years, with experience gained in international environments. The contexts he has dealt with cover cryptography, infrastructure security, but also mobile networks and 3G. He has collaborated with several IT magazines as a journalist, contributing to the dissemination of knowledge related to security and its technical and legal aspects. Member of the Association for Computing Machinery (ACM) since 2004, Nicola has collaborated with several start-ups in Italy and abroad. In this field, he has participated with several companies in the design and development of mobile services; he is co-editor of the Italian version of Cybersecurity Trends (www.cybertrends.it) and has been on the board of the Global Cyber Security Foundation (GCSEC).

Intelligence Activity

Intelligence activity is the product resulting from the collection, evaluation, analysis, and interpretation of the information gathered.

The development of an intelligence product requires the collection of information from a variety of sources, sources that must be selected according to the objectives required by the organisation.

The intelligence product of this activity provides states with the information they need to promote their national interests. Intelligence organisations generally seek information regarding military capabilities, issues that threaten national security, economic programs, and diplomatic positions.

In the digital/cyber scenario, similar scenarios are used for the purpose of preventing threats or to gather strategic information; increasingly sophisticated programs are now part of the defensive/offensive cyber protection strategy both at the government level and in companies that are part of the critical infrastructure, with the latter being limited to the defensive part. Intelligence activity is divided into strategic and operational. The former provides information needed by decision makers to make choices or decisions of long duration, normally this information must then be supplemented with information on politics, economics, social interactions, and technological developments. Operational intelligence, on the other hand, concerns current or otherwise short-term events and does not involve long-term projections.

Information gathering techniques

There are several disciplines used for information gathering. These disciplines include human intelligence (HUMINT), intelligence derived from signals (SIGINT), intelligence derived from images (IMINT), intelligence derived from radio frequency and radioactive emission detections (MASINT), and open-source intelligence derived from open sources (OSINT). On the topic of open-source intelligence, it should be noted that the more open an organisation/state is, the more successful this type of activity is. Journals, sites, online databases, social are often profitable sources of information regarding government and commercial activities.

Human intelligence activities, HUMINT, are synonymous with espionage and clandestine activities such as those described in Fabrizio Gatti's book (Educazione Americana), but the activities carried out by diplomats and military attachés should also not be overlooked. This discipline represents the oldest method of information gathering and remains, until the end of the 20th century, the main source of intelligence for governments/organisations.

HUMINT activity includes overt, sensitive, and clandestine activities using people who control, supervise, and support the necessary sources. Overt activities are handled openly, in which case the people collecting the information may be diplomats, seconded military personnel, members of official delegations participating in or handling unclassified publications or conferences. Clandestine activity, on the other hand, requires agents who are infiltrated into countries/organisations by performing undercover roles. Managing this discipline requires a significant number of personnel both among those who gather information and those who support and coordinate the various activities.

HUMINT in Onlife

Today, both threat actors and cybersecurity professionals have at their disposal increasingly efficient and lethal technologies. Along with these tools we have the tools that can be considered most useful of all, human knowledge, and experience.

For these reasons, it is easy to see how the use of HUMINT is critical both for those working to detect cyber criminals and for those involved in threat management and prevention. Understanding the motivations, trends, and reasons behind adversaries is key to any type of warfare, including cyber warfare. As the literature on the subject confirms, one must know one's enemy by becoming their enemy; one must always keep in mind that the enemy in this cyber warfare may be virtual, anonymous but never invisible. The technique used in the digital world is like that used in the physical world, a Threat Hunter to be successful in using HUMINT must learn and think like the actors implementing the threats, identify the tools, techniques used and understand their objectives.

All this requires good skill and ability in infiltrating cyber threat actors, gaining their trust and learning how

they operate. The same effort equivalent to that put in by agencies when they insert an undercover agent to infiltrate a criminal organisation. It is painstaking work that tests our nerves; identifying the digital places where threat actors gather to share information, dark web forums, IRC chats, virtual rooms and black markets. An activity just as dangerous as that which takes place in the physical world, no matter how experienced or skilled one is. When you enter these dark sides of the web, where there are actors from all parts of the world and who are also often in conflict with each other, you are constantly being scrutinised. In these forums the administrators or moderators examine everything about us for the purpose of determining if you are an infiltrator. At the very least, mere suspicion causes us to be banned. Certainly before starting this activity, it is important to guard yourself by managing your security very well, Threat Hunters need tools that hide their real identity; tools as simple as a VPN, TOR, up to proxies and virtual machines. Being unmasked can pose a serious threat to oneself and to the organisation for which one works.

In these activities, it is also possible to clash with law enforcement, with some activities, not to mention the possible clash with the legal department of our company. Collecting data through HUMINT techniques can be very time-consuming, and it is therefore necessary to rely on state-of-the-art technologies while always having in mind the organisation's goals and targets, i.e., the infrastructure and critical business processes. To manage HUMINT initiatives one should not only rely on oneself, but I strongly suggest working in teams with cybersecurity companies that are reputable and in general the more information one has the better the quality of our work.

Information comes from multiple sources, dark web, social media, etc., so it is essential to create the right mix of analysts, internal and external. The work that is done cannot be based on random research of actors in the dark web, one must come to qualify specialised sources on the assets that are of interest to us. For example, it might be useful, in the financial sector, to have sources among developers who trade and buy credit card or PIN information as well as moderators of forums on the subject. There are lists on Jabber, and on this decentralised messaging system questions are asked, or clues sought to investigate. In this activity one must also manage and maintain several avatars, each of which has its own list of people it can contact on Jabber. Clearly, care must be taken not to do anything illegal, not to buy anything, and not to handle illegal material. Another point that needs to be resolved is the hours.

If you want to maintain the credibility of avatars you have to get out of the 9-5pm and work week paradigm, the absence of the avatar would surely make our sources suspicious. To be credible you need a constant online presence, you will have to ensure the presence of avatars even outside office hours and access even on Saturdays and Sundays.

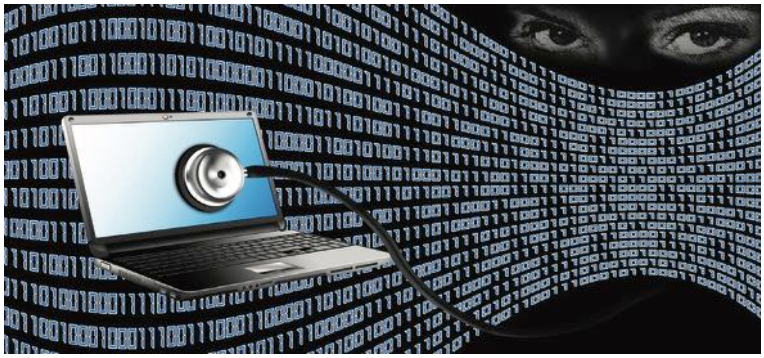
Conclusions

Software, tools, and technologies change rapidly, but even in this complex scenario there is the human factor; all cyber-attacks are human-driven. This is precisely why knowing the motivations of adversaries, the trends behind campaigns and attacks can help us define strategic decisions and target investments that best protect our infrastructure.

As described, HUMINT activity can be a critical piece in our cyber defense strategy, but it can also be incredibly dangerous. Care must be taken to conceal one's identity and goals. To begin with, one can certainly start with intelligence platforms that also include this service or rely on companies that offer this type of service. Traditional tools and HUMINT tactics combined give us the ability to identify criminal behaviour and allow us to move to a more proactive approach to cybersecurity, an approach that focuses on preventing attacks, because the best form of mitigation is to stop threats before they affect our infrastructure and critical processes. ■

International espionage needs a new global law standard.

Author: Kurt Sanger



While nations have laws that prohibit and punish espionage, its status under international law is ambiguous. While it is not legal, it is not illegal either. There is no broad multinational agreement or customary international law banning espionage. Similarly, there is no agreement acknowledging its legality.

Most national governments include organisations whose raison d'être is to gather information outside their borders, often secretly, often in ways that violate the law of the state from which the information is gathered. While the pervasive practice of espionage by states does not necessarily make it legal in their eyes, states are not held accountable for their espionage activities as a matter of international law.

Perhaps traditional espionage was not regulated as a matter of international law because so many other factors restrained it … the cost, the difficulty of infiltrating a nation under false pretenses or without detection, the risk to a spy of being killed or captured, the risk to a nation of having its interests revealed, the difficulty of accessing documents and exporting them for analysis without taking the originals. Where international law did not regulate, the limits of the physical world, the fear of personal consequences, and the difficulty of finding success restrained espionage.

In the age of cyberspace, many of these natural restraints are not meaningful. Spies may now ply their trade from a distance without

BIO

Kurt Sanger is a Lieutenant Colonel and Judge Advocate with the US Marine Corps. He is a 2015 graduate of the Georgetown University Law Center's National Security Law program. Since 2014, Kurt has advised senior military and policy leaders on cyberspace operations and national security issues. He retires from the Marine Corps in November 2022. As a well-respected military industry veteran, Kurt is sought after for his thought leadership and contributes writing, producing and hosting conferences, speaking at webinars and events with a global presence. Kurt was a panelist at the June 2022 RSA Conference in San Francisco and can be followed via his LinkedIn profile. These opinions are Kurt's own and do not necessarily reflect official positions of the Department of Defense.

subjecting themselves to the risks of moving among their targets. They need not travel to and work in jurisdictions where their targets control the levers of state power, and they no longer need to contemplate the prospect of death, capture, torture, or any personal consequence. They may spy without leaving the friendliest of territories … their surreptitious activities will go unpunished and more likely will be rewarded.

Cyberspace provides more than distance and safety for postmodern spies. Working through a medium that facilitates the bulk transfer of vast amounts of information enables spies to succeed in ways their predecessors could not imagine. For example, China's theft of millions of U.S. Government records and countless volumes of private enterprise intellectual property across the world would have been impossible had the information been stored on paper rather than digital files. Additionally, through cyberspace one can steal information at scale without depriving it from the victim, making the theft less likely to be detected … a feat far harder to accomplish in the physical world.

As Harvard law and leadership professor Lawrence Lessig observed, "We do not have special laws about the theft of skyscrapers. Skyscrapers pretty much take care of themselves. The laws of nature help skyscrapers in just the way that the laws of nature hinder the owners of automobiles. Nature makes it hard to steal a skyscraper, but easy to steal an automobile."

The laws of nature that once protected information have been defeated by the unfathomable advance of data technology. Now that nature does not protect information as it once did, perhaps it is time to reconsider international law's role in regulating espionage.

A simple aspect of law is so straightforward that it is rarely mentioned, but it is important to state here: law is useful because it makes certain conduct more or less likely to occur. Perhaps cyberspace's transformation of information from skyscraper-like to auto-like should motivate a reexamination of whether law can be used to make certain types of bulk espionage less likely.

The Obama administration made inroads with the Chinese Government when they agreed to forego espionage intended to gain an economic advantage to their industries. This provides the most realistic model for any effort to develop binding commitments to restrain espionage. Nations are compelled to spy to protect their national security, but there are discrete categories in which governments may see value in foregoing opportunities in the name of international stability.

In addition to economic targets, nations may explore putting off limits cyber espionage targeting particularly sensitive data, such as nuclear weapons triggering mechanisms, personal health information, other sensitive personal information, and information related to children. More broadly, nations could agree to ensure certain thresholds related to national security concerns have been met before spying on individuals, or collecting personal information in bulk and indiscriminately, and agree to limit retention and dissemination of personal information. For the time being, however, the best course of action for all organisations is to assume that any information of value will be targeted. Considering how creatively spies and criminals have made use of stolen information, the safest course of action is to prioritise data protection based on its potential value to thieves.

The variables that traditionally limited espionage in real space have yet to reach an appropriate balance in cyberspace. Law is not the only tool that can reshape that balance, but it has been remarkably effective in reducing conflict since World War II. If the effect of spying in cyberspace is to increase the probability of escalating conflict, states should be prepared to reevaluate international law's role in regulating espionage. ■

The case of the cyber attack on RUAG Holding AG in 2016.

Author: Marc-André Ryter

On 4 May 2016, the Swiss State owned military weaponry company RUAG announced that it had suffered an elaborate cyber attack and was able to find traces that suggest that the attack had been going on since at least September 2014.

Together ahead. RUAG

Page 1 / 2

Communiqué de presse

RUAG visé par une cyberattaque: les dommages ont pu être limités

Berne, le 12.05.2016. La cybercriminalité ne s'arrête pas aux frontières de la Suisse: RUAG est spécialisé en informatique et intervient avec succès dans le domaine de la sécurité depuis de nombreuses années. Cependant, la sécurité à 100% n'existe pas – une attaque visant RUAG a pu être détectée et stoppée grâce au soutien des instances fédérales compétentes. Et tout autre préjudice a ainsi pu être évité.

This announcement followed internal information given in January 2016 by the Department of Defence, Civil Protection and Sport (DDPS) to the Delegation of the Management Committees of the Federal Chambers (DélCdG) *"that a serious incident had compromised IT security within the Swiss federally-owned RUAG arms group"*[1]. A detailed report, which is the main source of this article, was subsequently published to provide members of the cyber community with information to improve the protection of their systems[2].

The main objective of this article is not to analyse the technical aspects of the attack, nor even to analyse the political debate that followed the attack, but rather to highlight the means used and the possibilities of protection.

It is interesting to note, that a great deal of information has been gathered about this attack, and that the availability of the technical report shows a high willingness to share this information. This sharing is generally considered to be one of the essential keys in the fight against cyber attacks, and the RUAG case is also a very good example in this sense.

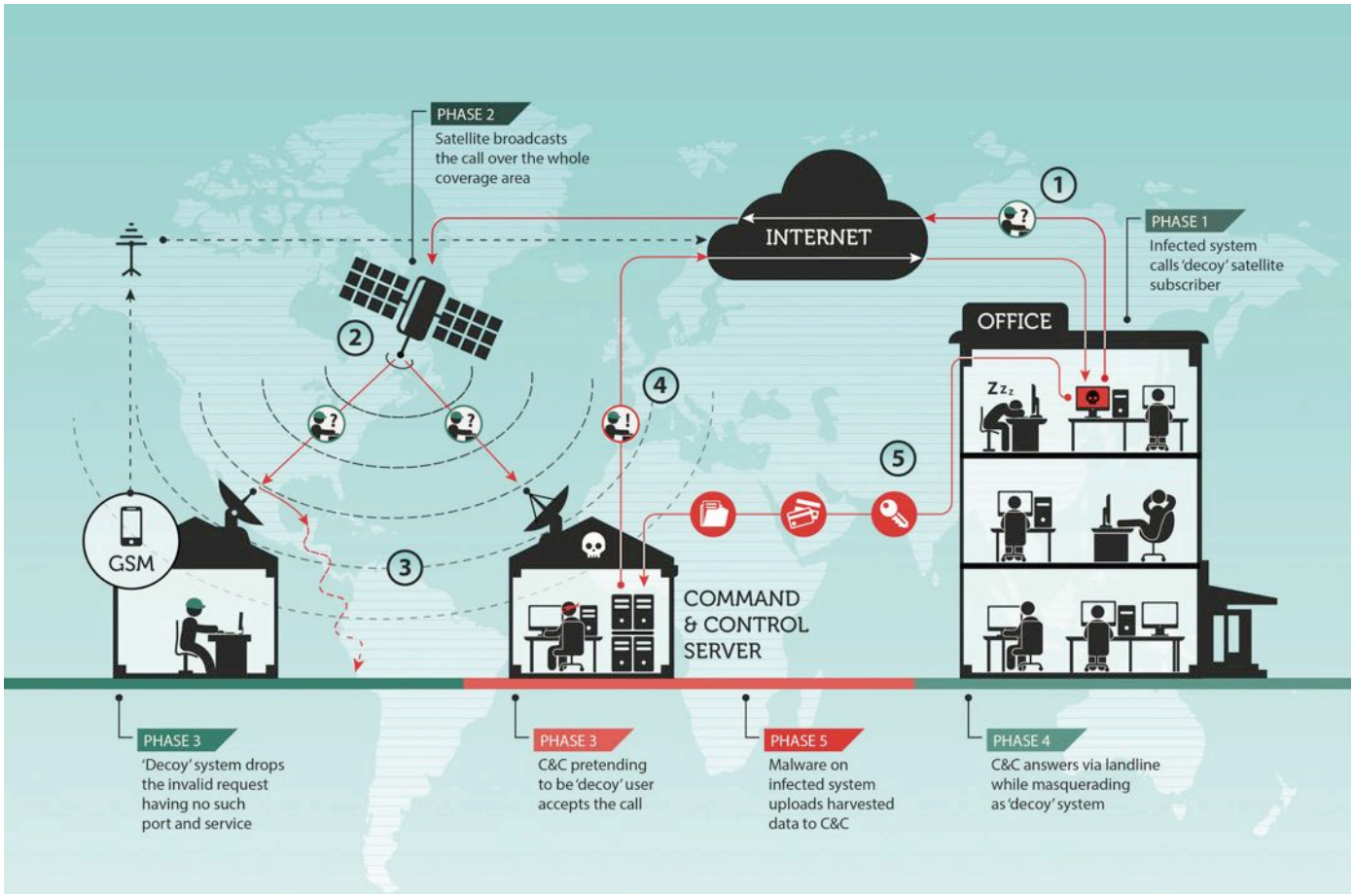
The main focus was on information about Indicators of Compromise (IoC) and the attacker's modus operandi, especially since the attacker has been identified as having infiltrated numerous governmental organisations and private companies in the last decade[3].

The malware used in the RUAG attack was part of the Turla family[4], which is a family of malware designed for espionage. According to malware researcher Matthieu Faou, this malware is among the most complex and uses hidden features of Windows[5]. Although it is several years old, its specific features still make it difficult to detect. Specialists from the Reporting and Analysis Centre for Information Assurance (MELANI/GovCert) of the Federal Department of Finance (FDF) took almost a month and a half to establish its presence in the RUAG system[6].

Of particular interest is the fact that the attacker likely acted over a long period of time and was very patient before extracting the intended data. He was also very careful during the whole infiltration, fingerprinting and

BIO

With university diplomas in Security Policies, after graduating in Political Sciences, Col. Marc-André Ryter is currently Chief of Staff at the Division of Military Constructions within the Staff of the Armed Forces. As part of his military role, he follows and studies the technological evolutions which may prove relevant for the Armed Forces and for different operation fields, with a particular aim to adapt the military doctrine.



exploration phase with lateral movements, which allowed him to act on the specific targets afterwards. The lateral movements can be repeated over several months, in order to continuously check the information available and update it if necessary[7].

RUAG also identified a progressive attack process, with additional devices being infected and gaining increasingly higher privileges within the system. The attacker created an internal communication network between the infected devices, and established various functions to limit the number of devices and channels used to extract data. In addition, the intensity of the espionage activities was very irregular in order to make it difficult to identify the leak.

The course of the attack provides valuable insights. Three main phases were identified.

Phase 1 - a preparation phase. The target was assessed in detail and the attacker had to gather as much information as possible and place the malware that was later used. It is possible that the attacker, in the case of RUAG, had an idea of the kind of information potentially available within the company's system. The use of social engineering may have taken place during this phase, but is not confirmed. The attacker used reconnaissance malware, which allowed him to confirm the interest of the target.

Phase 2 - preparing and carrying out the infection of the target. As the first phase confirmed the potential of the target, more powerful malware was installed, also with a view to gaining greater persistence[8]. This malware had access to system administrator privileges. One of the obstacles encountered by RUAG was that the recognition malware as well as the malware installed during the second phase used already existing processes, without affecting current operations. For almost a year, RUAG did not notice that its system was infected[9]. In addition, rootkit tools that were very advanced at that time were also used[10], as well as processes that avoid using hidden files that may become visible (Carbon DLL)[11]. The malware installed at this stage contained instructions on how the attacked system should operate at the chosen time.

Phase 3 - the attacker was fully present within the target and began his exploitation. This exploitation phase continued to take place almost undetected by the victim. The attacker was able, over an extended period of time, to continue his exploration of the system, complete his arsenal, set up a network within the attacked system and gain more privileges using lateral moves. The report mentions that lateral moves took place during the first 8 months of the attack[12]. The attacker thus created paths to the desired information, and set up the necessary system to exfiltrate it. During the extensive reconnaissance of the system, very little data was exfiltrated. Only when the attacker was satisfied with the level reached, and thought he had all the necessary elements, did he implement the exfiltration of data in large quantities.

This phase was the most delicate, as this is the moment when the victim is most likely to be aware of the attack due to the unordered data traffic on his part, or even the sudden volume of this traffic. When the malware sends the extracted data using processes that normally use an internet connection, as in the case of the RUAG attack, detection is very difficult. In addition, the attacker had taken care to decouple the different phases of the task execution, which made the whole extraction process more secure[13]. Thus, data was collected by drones within the system, without communication with the outside, and then specific communication drones used the internet for data exfiltration[14]. The attacker also used tools available on the internet, such as Mimikatz, to obtain passwords[15].

It is also possible that RUAG itself neglected to make the necessary investments in cyber security to protect its own systems during the three phases, which would have made it easier for the attacker[16].

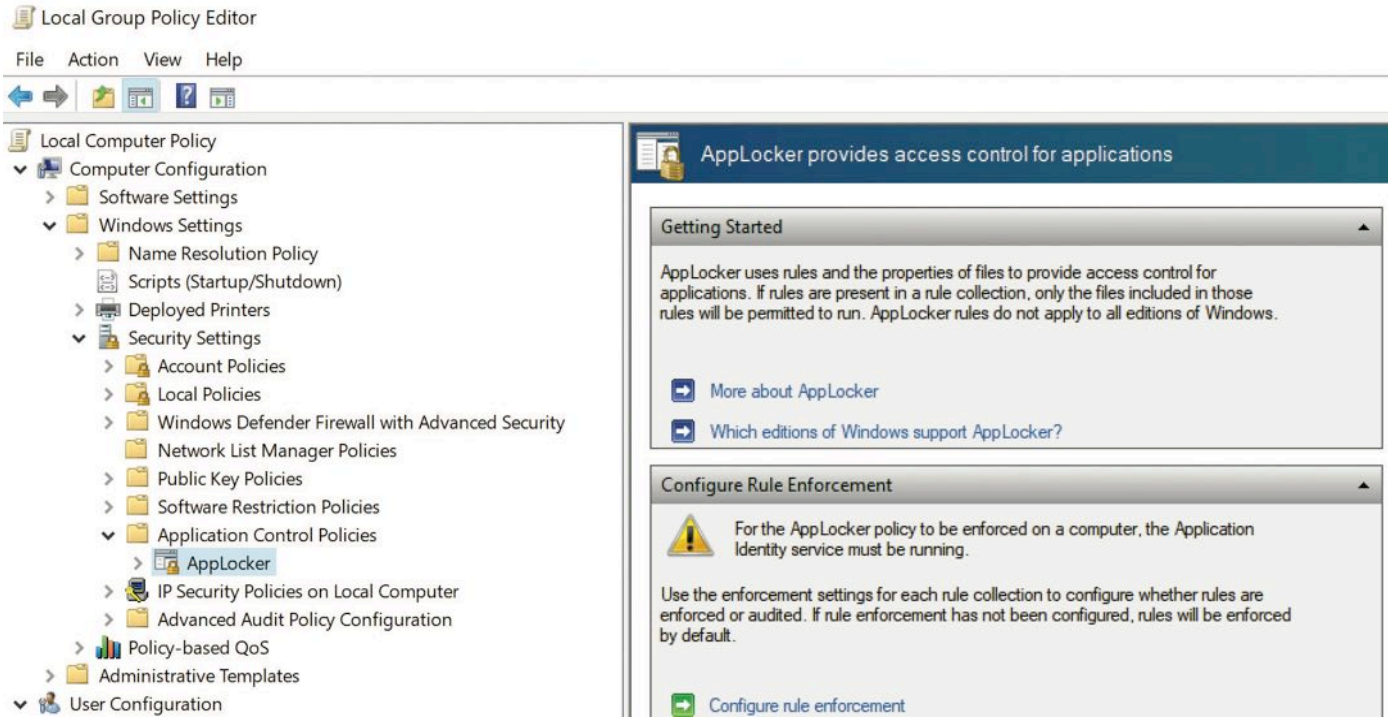
Lessons learned and recommendations

RUAG mentions that a total of around 23 GB of data was extracted, although it is stated that some data was extracted several times. However, it was not possible to determine whether the extracted data was confidential and what its value was[17]. Other sources mention serious attacks, although the damage is difficult to estimate[18].

It is also possible that, due to the IT interfaces between RUAG and the DDPS, data from the Confederation's messaging directories was affected[19]. The report mentions that the rate of extraction was very irregular, and that on some days almost 1 GB was extracted, while other periods, sometimes quite long, saw very little activity. In total, the main extraction phase lasted 4 months, from September to December 2015[20].

On the basis of the experiences made and the information gathered in the course of subsequent work after the attack, RUAG makes a series of recommendations in its report in order to make it more difficult for potential attackers. These recommendations consist of various countermeasures that should be implemented at different levels. We will limit ourselves here to highlighting certain recommendations that we consider particularly important[21].

At the system level, the use of Applocker (Microsoft) is recommended. This makes it possible to create rules that limit the applications allowed for users and thus make it more difficult to install malware. Similarly, limiting the privileges of normal users is also an effective barrier. Other system-related measures seem obvious, but are not yet widespread enough. In particular, RUAG mentions the need to constantly monitor systems, to ensure that they are regularly updated and to eliminate all unnecessary applications that increase the possible attack surface.



Measures can also be taken at the level of the active directory (Active Directory). RUAG recommends monitoring requests to the directory, in particular to identify requests for large amounts of information, as well as the use of two-factor identification. As far as the networks are concerned, it is a question of increasing resilience and detection capabilities by creating a choke point that allows better supervision of what is going out to the internet. Server log files should also be backed up for a minimum of two years and the system should be managed from a separate network from the day-to-day business traffic.

These few fairly basic recommendations, sometimes even described as simple and inexpensive[22], together with the more technical measures as recommended, should massively increase security against cyber attacks, even if they are technically sophisticated and complex.

The RUAG report on this attack reminds us that the aim is not to avoid all attacks, but to make them as difficult as possible, respectively to create as many obstacles as possible to ultimately deter the attacker. The point of entry must be difficult to find and failed attacks must be identifiable, thus saving time and allowing the development of new defences.

RUAG reiterates that sharing information about such attacks, including at the international level, is the best countermeasure. Without specifying the sources, RUAG mentions that the attack on it was discovered precisely because of information sharing. According to the Aargauer Zeiutung, it was the Swiss Federal Intelligence Service that warned RUAG in December 2015[23], which had itself been informed by a foreign intelligence service[24].

In general, users of cyberspace should be aware of their responsibilities, keep their networks and data secure and ensure that their servers cannot be used to attack other targets. RUAG itself does not give any indication of the source of the attack it suffered. However, the "Handelzeitung", quoting DelCdG President Alex Kuprecht, clearly mentions Russia as the attacker in this case[25]. These certainties come from the fact that the origin of the software, which had already been used in a previous attack on the Department of Foreign Affairs, is known, and that such a sophisticated attack can only come from a state actor[26].

The attack also had consequences within the federal administration. On 23 May 2016, the Federal Council took 14 short and medium-term measures to eliminate the risk of data theft[27]. However, these measures cannot be described and commented on as they have not been published. However, the information disclosed mentions measures "mainly relating to internal procedures and checks"[28] as well as organisational measures between RUAG and the Confederation, such as the disentanglement of networks[29].

Similarly, a specific Task Force, called RHINO, was set up "to take the necessary emergency measures and assess the damage caused"[30]. In general, it is interesting to note that this attack served as a wake-up call. It demonstrated the importance of cybersecurity and the absolute and urgent need for the federal administration and federal enterprises to improve the protection of their systems. ■

1 According to the Report of the Control Committee of the National Council: "Assessment of the management of the cyber attack against RUAG" of 8 May 2018, available at https://www.parlement.ch, accessed on 27.05.2022.
2 APT Case RUAG: Technical Report, by MELANI GovCert, 23.05.2016, available at https://www.govcert.ch/whitepapers/apt-case-ruag-technical-report-govcert-ch/.
3 APT Case RUAG: Technical Report, p. 2.
4 APT Case RUAG: Technical Report, p. 1.
5 See https://www.01net.com/actualites/les-malwares-les-plus-sophistiques-au-monde-sont-ceux-du-groupe-turla-2052740.html, accessed on 24.05.2022.
6 Report of the Control Committee of the National Council: "Assessment of the management of the cyber attack against RUAG" of 8 May 2018, available at https://www.parlement.ch, accessed on 27.05.2022, p. 6.
7 APT Case RUAG: Technical Report, p. 21.
8 APT Case RUAG: Technical Report, p. 8.
9 https://www.handelszeitung.ch/politik/ruag-hackerangriff-es-war-russland-1071536, accessed on 25.05.2022
10 APT Case RUAG: Technical Report, p. 13.
11 APT Case RUAG: Technical Report, p. 15.
12 APT Case RUAG: Technical Report, p. 25.
13 APT Case RUAG: Technical Report, p. 15.
14 APT Case RUAG: Technical Report, p. 23.
15 APT Case RUAG: Technical Report, p. 21.
16 https://www.aargauerzeitung.ch/schweiz/verteidigung-wie-die-ruag-warnungen-ihrer-experten-ignorierte-und-die-cybersicherheit-verschlampte-ld.2093294, accessed on 25.05.2022.
17 APT Case RUAG: Technical Report, p. 25.
18 https://www.handelszeitung.ch/politik/ruag-hackerangriff-es-war-russland-1071536, accessed on 25.05.2022.
19 https://www.letemps.ch/monde/cyberattaque-ruag-reveille-suisse, accessed on 27.05.2022.
20 APT Case RUAG: Technical Report, p. 25.
21 All measures are described in detail in the report, APT Case RUAG: Technical Report, pp. 27-29.
22 https://www.letemps.ch/monde/cyberattaque-ruag-reveille-suisse, accessed on 27.05.2022.
23 https://www.aargauerzeitung.ch/schweiz/verteidigung-wie-die-ruag-warnungen-ihrer-experten-ignorierte-und-die-cybersicherheit-verschlampte-ld.2093294, accessed on 25.05.2022.
24 https://www.letemps.ch/monde/cyberattaque-ruag-reveille-suisse, accessed on 27.05.2022.
25 https://www.handelszeitung.ch/politik/ruag-hackerangriff-es-war-russland-1071536, accessed on 25.05.2022.
26 https://www.swisscybersecurity.net/news/2018-08-27/ruag-hacker-kommen-davon, accessed on 25.05.2022.
27 https://www.handelszeitung.ch/politik/ruag-hackerangriff-es-war-russland-1071536, accessed on 25.05.2022.
28 Report of the Control Committee of the National Council: "Assessment of the management of the cyber attack against RUAG" of 8 May 2018, available at https://www.parlement.ch, accessed on 27.05.2022, p. 7.
29 Report of the Control Committee of the National Council: "Assessment of the management of the cyber attack against RUAG" of 8 May 2018, available at https://www.parlement.ch, accessed on 27.05.2022, p. 11.
30 Report of the Control Committee of the National Council: "Assessment of the management of the cyber attack against RUAG" of 8 May 2018, available at https://www.parlement.ch, accessed on 27.05.2022, p. 7.

UKSEC

22nd - 23rd November 2022

Millennium Gloucester Hotel, London

Join FREE
With Code:
CYBERTRENDS

Join Us at the UKsec: Cyber Security Summit on 22nd - 23rd November!

The 5th annual **UKsec Cyber Security Summit** brings together **100+ IT security leaders** from across the **Retail, FMCG, Banking & Finance, Automotive, Utilities, Food & Beverage industries** for 2-days of insight building and expert knowledge exchange on **22nd - 23rd November.** Join us in **London, UK** to hone your skills in areas including:

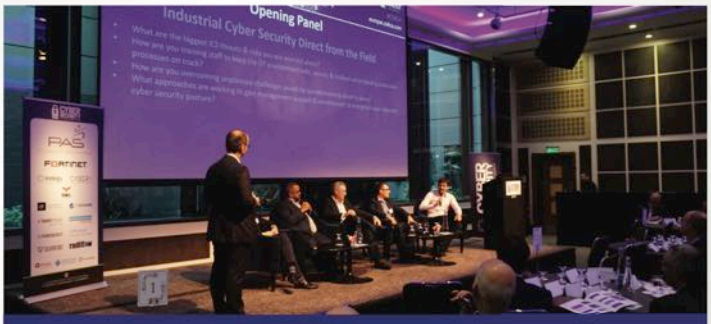
- *Learn How to Utilise Technology to Maximise Cyber Security*
- *Obtain Steps for Reacting to an Increasing Attack Surface*
- *Assess The Link between Cyber Security and Business Strategies*
- *Explore Regulations and the Role of the State*
- *Enhance the Protection of UK Companies*

CPD CERTIFIED
The CPD Certification Service

100+

CISOs, VPs, Heads of IT Security at:

HSBC, Missguided, Photobox, News UK, Barclays, and more...



Join Interactive Panel Discussions

Hear from 25+ Expert Speakers

Enjoy 6+ Hours of Networking

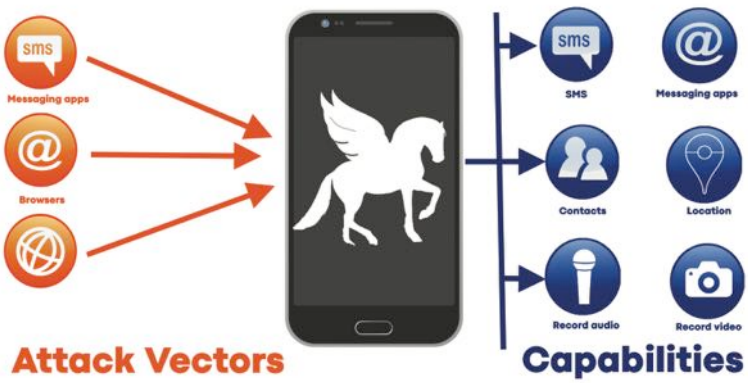
This is an unique opportunity for cyber security leaders across the UK to come together and safeguard their assets. View the agenda & **secure your place for FREE** using the discount code: **CYBERTRENDS** at: **uk.cyberseries.io/register/** T&Cs apply.

The Pegasus mobile spyware - how it works and how to protect against it.

Author: Costin G. Raiu

One of the biggest cyber stories of 2021 is an investigation by The Guardian and 16 other media organisations, suggesting that over 30,000 human rights activists, journalists and lawyers across the world may have been targeted using the Pegasus spyware (Pegasus is a so-called "legal surveillance software" developed by the Israeli company NSO). The report published in July 2021, called the Pegasus Project, alleged that the malware was deployed widely through a variety of exploits, including several iOS zero-click zero-days. Based on forensic analysis of numerous mobile devices, Amnesty International's Security Lab actually found that the software was repeatedly used in an abusive manner for surveillance. The list of targeted individuals includes 14 world leaders and many other activists, human rights advocates, dissidents and opposition figures. Later that month, representatives from the Israeli government visited the offices of NSO as part of an investigation into the claims. And in October, India's Supreme Court commissioned a technical committee to investigate the use of Pegasus to spy on its citizens. In November, Apple announced that it was taking legal action against NSO Group for developing software that targets its users with "malicious malware and spyware". Last but not least, in December 2021, Reuters published that US State Department phones were hacked with the NSO Pegasus malware, as alerted by Apple. Over 2022, the disclosures continued - on May 2, 2022 the Spanish government announced that the prime minister, Pedro Sánchez, and the defence minister, Margarita Robles, were both infected with Pegasus. The Spanish government has also sacked the country's spy chief Paz Esteban following the disclosures.

Detecting infection traces from Pegasus and other advanced mobile malware is very tricky, and complicated by the security features of modern OSs such as iOS and Android. Based on our observations, this is further complicated by the deployment of non-persistent malware, which leaves almost no traces after reboot. Since many forensics frameworks require a device jailbreak, this results in the malware being removed from memory during the reboot. Currently, several methods can be used for detection of Pegasus and other mobile malware. MVT (Mobile Verification Toolkit) from Amnesty International is free, open source and allows technologists and investigators to inspect mobile phones for signs of infection. MVT is further boosted by a list of IoCs (indicators of compromise) collected from high profile cases and made available by Amnesty International.

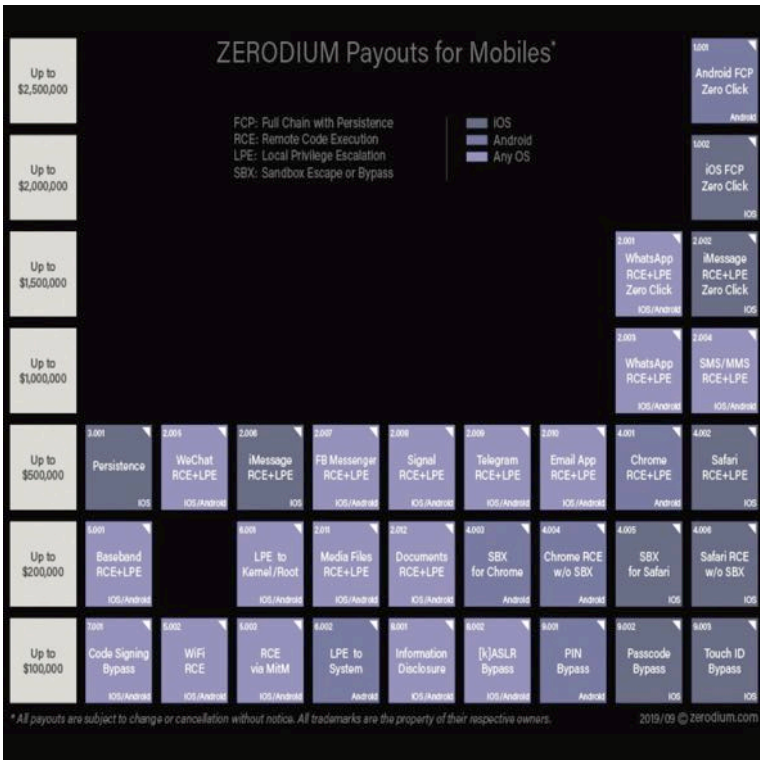


In these uncertain times, a lot of concerned users worldwide are asking how to protect their mobile devices from Pegasus and other similar tools and malware. Similarly, governments are trying to evaluate their weaknesses and come up with strategies to identify these breaches, or,

prevent future breaches from occurring. In this current article we will take a look at the latest attack techniques used to deploy mobile phone malware and how to defend against them, with the observation that no list of defense techniques can ever be exhaustive. Additionally, as attackers change their modus operandi, defense techniques should also be adapted.

How do we stay safe from sophisticated mobile malware?

First of all, we should start by saying that Pegasus is a toolkit sold at relatively high prices. The cost of a full deployment may easily reach millions USD. Similarly, other mobile malware may be deployed through 0-click 0-day exploits. These are extremely expensive - as an example, Zerodium, an exploit brokerage firm paid up to 2.5 million USD for an Android 0-click infection chain with persistence:



From the start, this draws an important conclusion - sophisticated cyber espionage is a vastly resourceful endeavor. When a threat actor can afford to spend millions, potentially tens of millions or even hundreds of millions of USD on their offensive programs, it is very unlikely that a target will be able to avoid getting infected. In practice, or to put this in simpler words, it's not a question of "whether you can get infected", it's actually just a matter of time and resources before you get infected. Now, for the good news - exploit development and offensive cyberwarfare are often more of an art rather than an exact science. Exploits need to be tuned for specific OS versions and hardware and can be easily thwarted by new OSes, new mitigation techniques or even small things such as random events.

With that in mind, infection and targeting is also a question of cost and making things more difficult for the attackers. Although we may not always be able to prevent the successful exploitation and infection of the mobile device, we can try to make it as hard as possible for the attackers. How do we do this in practice? Here's a simple checklist:

1. On iOS:

a) Reboot daily. According to research from Amnesty and CitizenLab, the Pegasus infection chain often relies on 0-click 0-days with no persistence, so a regular reboot helps clean the device. If the device is rebooted daily, the attackers will have to re-infect it over and over again. In time, this increases the chances of detection; a crash might happen or artifacts could be logged that give away the stealthy nature of the infection. Actually, this is not just theory, it's practice - we analysed one case in which a mobile device was targeted through a 0-click exploit (likely FORCEDENTRY). The device owner rebooted their device regularly and did so in the next 24 hours following the attack. The attackers tried to target them a few more times but eventually gave up after getting kicked a few times through reboots.

b) Disable iMessage. iMessage is built into iOS and is enabled by default, making it an attractive exploitation vector. Because it's enabled by default, it is a top delivery mechanism for 0-click chains and for many years, iMessage exploits were in high demand, with top payouts at exploit brokerage companies. "During

BIO

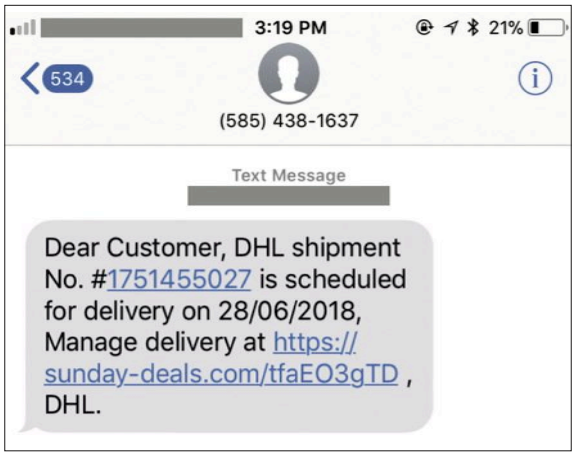
Director of the Global Research and Analysis Team (GReAT) (Kaspersky) Costin specialises in analysing advanced persistent threats, zero-day exploits and complex malware. He is leading the world-known Global Research and Analysis Team (GReAT) that researched the inner workings of many high-profile attacks, including RedOctober, WannaCry, ShadowPad and ShadowHammer and Moonlight Maze. His current work is focused on the development of code similarity technologies and systems for enriching threat intelligence. Costin has over 28 years of experience in anti-virus technologies and security research. He is a member of the Virus Bulletin Technical Advisory Board, a member of the Computer AntiVirus Researchers' Organization (CARO) and a reporter for the Wildlist Organization International. Before joining Kaspersky Lab, Costin worked for GeCad as Chief Researcher and as a Data Security Expert with the RAV antivirus developers group. Costin holds a blue belt in Taekwondo. Some of his hobbies include chess, photography and Science Fiction literature.

the last few months, we have observed an increase in the number of iOS exploits, mostly Safari and iMessage chains, being developed and sold by researchers from all around the world. The zero-day market is so flooded by iOS exploits that we've recently started refusing some (of) them," Zerodium's founder Chaouki Bekrar wrote back in 2019 to WIRED. We realise this may be very difficult for some (more later), but if Pegasus and other high end APT mobile malware is in your threat model, this is a tradeoff worth taking.

c) Disable Facetime. Same as above.

d) Keep the mobile device up to date; install the latest iOS patches as soon as they are out. Not everyone can afford 0-click 0-day's, actually many of the iOS exploit kits we are seeing are targeting already patched vulnerabilities. Nevertheless, many people run older phones and postpone updates for various reasons. If you want to be ahead of (some) nation state hackers, update as soon as possible and teach yourself not to need Emojis to install the patches.

e) Don't ever click on links received in SMS messages. This is simple advice yet effective. Not all Pegasus customers can afford to buy 0-click 0-day chains at a cost of millions so they rely on 1-click exploits. These arrive in the form of a message, sometimes by SMS, but can also be via other messengers or even e-mail. If you receive an interesting SMS (or by any other messenger) with a link, open it on a desktop computer, preferably using TOR Browser, or using a secure non-persistent OS such as Tails.



SMS with a malicious link used to target a political activist - credit: Citizenlab

f) Browse the internet with an alternate browser such as Firefox Focus instead of Safari or Chrome. Despite the fact that all browsers on iOS pretty much use the same engine, Webkit, some exploits do not work well (see LightRighter / TwoSailJunk APT case) on some alternate browsers:

```
detect_os()

return {
        mobile: (typeof window.orientation !== "undefined") || (navigator.userAgent.indexOf('IEMobile') !== -1),
        webkit: parseFloat(/AppleWebKit\/([\d.]+)/.exec(navigator.userAgent)[1]) || 0,
        safari: window.navigator.userAgent.indexOf('Safari') > -1,
        version: function()
        {
                var match = (navigator.appVersion).match(/OS (\d+)_(\d+)_?(\d+)?/);
        if(match) {
                var version = [
                    parseInt(match[1], 10),
                    parseInt(match[2], 10),
                    parseInt(match[3] || 0, 10)
                        ];
                        return parseFloat(version[0]+'.'+version[1]+version[2]);
            } else {
                return "unknown";
            }
```

LightRiver exploit kit check for "Safari" in the user agent string

User agent strings on iOS from Chrome (left) /Firefox (right):

Chrome user agent string on iOS	Firefox Focus user agent string on iOS
Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/96.0.4664.53 Mobile/15E148 Safari/604.1	Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) FxiOS/39 Mobile/15E148 Version/15.0

g) Always use a VPN that masks your traffic. Some exploits are delivered through GSM operator MitM attacks, when browsing HTTP sites or by DNS hijack. Using a VPN to mask the traffic makes it difficult for your GSM operator to target you directly over the Internet. It also complicates the targeting process if the attackers have control over your data stream, such as while in roaming. Do note that not all VPNs are the same and not any VPN is fine to use. Without favoring any specific VPN, here's a few things to consider when purchasing a VPN subscription:

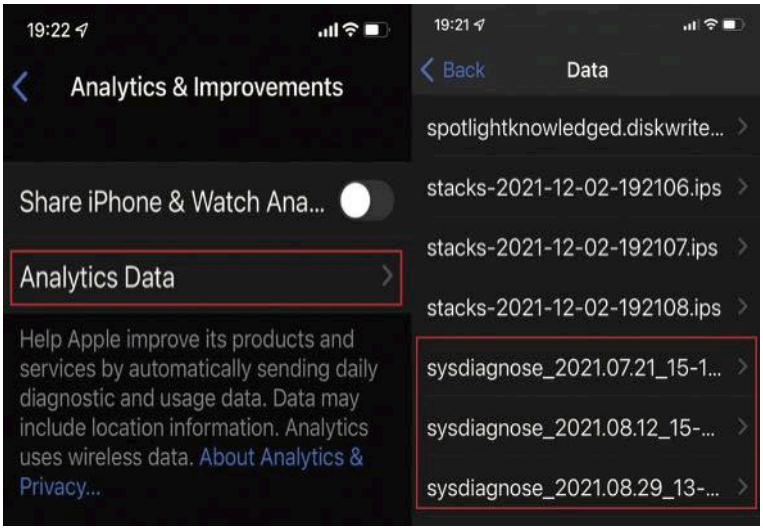
- Purchase means just that - no "free" VPNs
- Look for services that accept payment with cryptocurrencies
- Look for services that do not require you to provide any registration info
- Try to avoid VPN apps - instead, use opensource tools such as WireGuard and OpenVPN and VPN profiles

Avoid new VPN services and look for established services that have been around for some time

h) Install a security application that checks and warns if the device is jailbroken. Frustrated from getting kicked over and over, the attackers will eventually deploy a persistence mechanism and jailbreak your device in the process. This is where the chance of catching them increases tenfold and we can take advantage of the fact that the device is jailbroken.

i) Make iTunes backups once per month; this allows diagnosing and finding infections later, through the use of the wonderful MVT package from Amnesty.

j) Trigger sysdiags often and save them to external backups. Forensics artifacts can help you determine at a later time if you have been targeted. Triggering a sysdiag depends on the phone model - for instance, on some iPhone's, this is done by pressing VOL Up + Down + Power at the same time. You may need to play with this a couple of times, until the phone buzzes. Once the sysdiag is created, it will appear in diagnostics:



2. Android

a) Reboot daily. Persistence on latest Android versions is difficult, many APTs and exploit sellers avoid persistence whatsoever!

b) Keep phone up to date; install latest patches

c) Don't ever click on links received in SMS messages

d) Browse the internet with an alternate browser such as Firefox Focus instead of Chrome.

e) Always use a VPN that masks your traffic. Some exploits are delivered through GSM operator MitM attacks, when browsing HTTP sites or by DNS hijack.

f) Install a security suite that scans for malware and checks and warns if the device is jailbroken

At a more sophisticated level - always check your network traffic using live IOCs. A good setup might include a Wireguard always-on VPN to a server under your control, that uses pihole to filter out bad stuff and logs all the traffic for further inspection.

A zero-sum game?

Famous security commentator Ryan Naraine has famously said - "iMessage and FaceTime - these are the reasons why people use iPhones!" and for sure, he's right. iMessage and FaceTime were two of the greatest things Apple added to this ecosystem.

Luckily, Apple greatly improved the security sandbox around iMessage with BlastDoor in iOS 14. Nevertheless, the FORCEDENTRY exploit used by NSO to deliver Pegasus bypassed BlastDoor and of course, no security feature is ever 100% hack-proof.

So, what is the best of both worlds, you may ask? Some people, including myself, have several phones - one where iMessage is disabled, and a "honeypot" iPhone where iMessage is enabled. Both are nicely associated with the same Apple ID and phone number. If someone decides to target me this way, there's a good chance they will end up in the honeypot phone.

Of course, people might follow these recommendations carefully and still get infected. Sadly, this is the reality we live in nowadays. When someone tells me they've been targeted with mobile spyware, I tell them to think about these questions:

- Who targeted you and why? Try to figure out what it was that brought you into the attention of the big guys. Is this something that you can avoid in the future through more stealthy behavior?
- Can you speak about it? The thing that eventually brought down many surveillance companies was bad publicity. Reporters and journalists writing about abuses and exposing the lies, wrongdoing and all the evil. If you've been targeted try to find a journalist and tell them your story.
- Change your device - if you were on iOS, try moving to Android for a while. If you were on Android, move to iOS. This might confuse attackers for some time; for instance, some threat actors are known to have purchased exploitation systems that only work on a certain brand of phone and OS.
- Get a secondary device, preferably running GrapheneOS, for secure comms. Use a prepaid card in it, or, only connect by Wifi and TOR while in airplane mode. Avoid messengers where you need to provide your contacts with your phone number. Once an attacker has your phone number they can easily target you across many different messengers via - iMessage, WhatsApp, Signal, Telegram, they are all tied to your phone number. An interesting new choice here is Session, which automatically routes your messages through an Onion-style network and doesn't rely on phone numbers.
- Try to get in touch with a security researcher in your area and constantly discuss best practices.
- Share artifacts, suspicious messages or logs whenever you think something is odd. Security is never a single snapshot solution that is 100% proof; think of it like a stream that flows and you need to adjust your sailing depending on the speed, currents and obstacles.

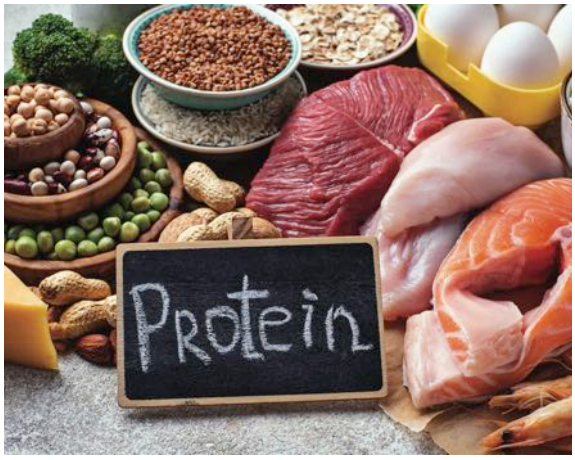
At the end of this, I'd like to leave you with a thought. If you get targeted by nation states, that means you are important. Remember: it's nice to be important, but it's more important to be nice. Alone, we are weak, together, we are strong. The world may be broken, but I believe we are living at a time when we can still change things. According to a report from the nonprofit group Committee to Protect Journalists, 293 journalists were imprisoned in 2021, the highest number CPJ has ever reported since it started tracking it, in 1992. It's up to us to shape how the world will look like for us in 10 years, for our children and our children's children. ■

2020-2022: A wave of cyber attacks against agricultural cooperatives and industries.

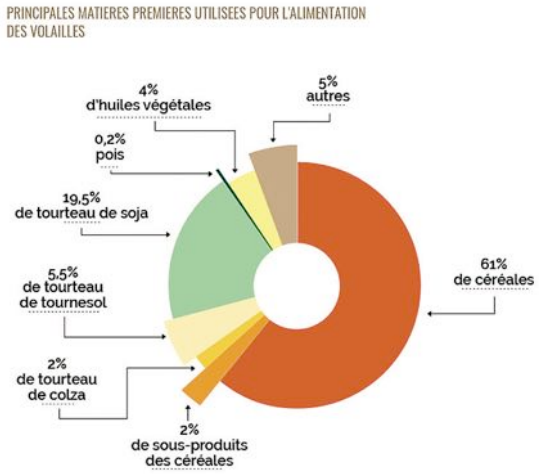
The beginning of a global earthquake around plant protein?

Author: **Stéphane Mortier**

The period 2020-2022 is marked by numerous cyber attacks on agricultural cooperatives and industries around the world. Beyond the attacks itself, often by ransomware, what might the attackers be looking for? Is there a desire to destroy agricultural sectors? If so, what are their *ultimate* objectives?

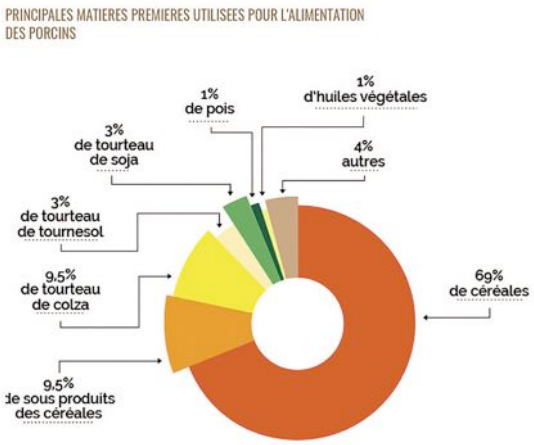


The basis of the human diet is plant protein, which makes it a particularly strategic material. On average, humans consume 2/3 animal proteins and 1/3 plant proteins. However, plant proteins make up the bulk of animal feed, thus producing animal proteins.



Humans are therefore totally dependent on plant proteins! In the context of a growing world population, whoever masters the production of plant proteins will master the world!

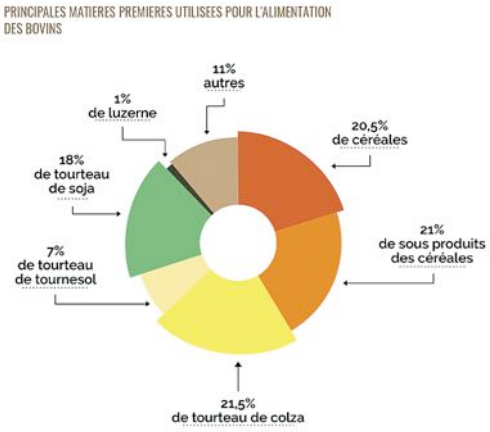
Faced with this situation, France has implemented a national strategy to develop plant proteins since the end of 2020. It currently produces only 50%



of its needs and is therefore aiming for an increase (40%) over the next three years. The objectives are as follows:

- Reduce dependence on imports and secure supplies;
- Improve the economic situation of farmers;
- Responding to climate and environmental challenges;
- Develop a range of local products.

Strategic interest, national strategy,... all of which can fuel the desire for predation. This is where both espionage and cyber come into play.



Espionage, in this case economic espionage, is the illegitimate search for technical information or information of any kind for economic purposes when this information has a value, even potential, the disclosure of which would be likely to harm the essential interests of the victim[1]. What happens when the perpetrator, in order to obtain a strategic or competitive advantage, can, instead of appropriating the information sought, simply destroy it or make it inaccessible? If the final effect sought is achieved (harming the target and reducing its competitiveness on a given market), by extension, this would then be an act of espionage. Indeed, it is the information that is targeted and not the infrastructure. Beyond that, if the action to harm comes from a state power, it could be an act of economic warfare.

Cyber espionage is, as stated in an ENISA paper in 2020[2], the use of computer networks to gain illicit access to confidential information, usually held by a government or other organisation. Attacks by Advanced

BIO

Stéphane Mortier is currently deputy head of the Centre for Economic Security and Protection of Enterprises (CSECOPE) within the General Directorate of the French Gendarmerie and a member of the Gendarmerie National Research Community (CREOGN). He is assiciate lecturer at the University Gustave Eiffel. He has a degree in political science, sociology and international relations from the Université libre de Bruxelles (ULB), in strategic management and economic intelligence from the École de Guerre Économique, and a doctorate in management at Paris 1 Panthéon-Sorbonne. He is also the representative of the foreign sections of the ULB Alumni Union and chairs the French section (UAEF). Within this framework, he develops cooperation projects in Africa. He is a lecturer at the Ecole de Guerre Économique (Anti-Money Laundering), at the University of Likasi – DRC (Stategy, Business law). He is a founding member of the Cercle K2 and an active member of the Association pour l'Unification du Droit en Afrique (UNIDA). He is the author of some publications on economic intelligence.

Persistent Threat (APT) groups indicate that financial attacks are often motivated by espionage. But what about ransomware attacks? Ransomware attacks render the victim's information unavailable, which means that the target organisation is unable to function at all. The notion of "nuisance" is therefore proven. Moreover, some cybercriminal groups using ransomware are also known for data theft.

For example, the Lockbit group, which is known for carrying out ransomware attacks but which has claimed responsibility for data theft on several occasions (in particular during an attack against THALES and the French Ministry of Justice). Espionage (search for information

Company	Nationality	Activity	Type of attack	Supposed origin of the attack	Date
Lion	Australia/New Zealand	Drinks/Milk	Ransomware	China (?)	2020/06
Campari Group	Italy	Drinks	Ransomware	Ukraine	2020/11
Ceresia	France	Seeds/Viticulture/Animal feed	Ransomware	Russia	2020/11
Sollio	Canada	Agricultural inputs/ Grains/Meat	Ransomware	Ukraine	2020/11
Lactalis	France	Dairy products	Intrusion	?	2021/03
Molson Coors	USA/Canada/Great Britain	Drinks/Beer	Ransomware	?	2021/03
JBS Foods	Brazil/Australia/USA/ Canada	Meat	Ransomware	Russia	2021/05
Cristal Valley	USA	Cereals/Seeds	Ransomware	Eastern Europe(?)	2021/06
La Martiniquaise-Bardinet	France	Wine and spirits	Data theft	Russia	2021/09
New cooperative	USA	Seeds	Ransomware	Russia	2021/09
April	France	Animal processing/ Agri-food	Ransomware	?	2021/11
Jean Floc'h	France	Meat/Food	Ransomware	Russia	2021/11
Eureden	France	Animal feed, meat, eggs, vegetables	Ransomware	?	2022/03
AGCO	USA/Germany/China/ France/Finland	Agricultural equipment	Ransomware	Russia (?)	2022/05

with the aim of harming) and weakening (prevention of functioning, blocking of activity) by accessing and/or blocking a company's information therefore go hand in hand.

Let's go back to the cyber attacks that have plagued the agricultural cooperatives and industries in 2020-2021. Most of them are ransomware attacks and affect all agri-food sectors. The table above gives an overview of the most impacted cooperatives and industries over the period. With the exception of JBS Foods (Brazil), all of them are companies headquartered in Western states. However, the JBS Foods sites impacted by the May 2021 attack are mainly located in Western democracies. Is this a coincidence? It seems that the geographical origin of the attacks is concentrated in Russia and Ukraine. As it is extremely complex to attribute a definite geographical origin to a cyber attack, this finding should be taken with the utmost circumspection.

Of these attacks, very few, a priori, would involve data theft. This does not mean, however, that these attacks are not espionage, as mentioned *above,* but in a broader context than the simple capture of strategic information or data. Such attacks can then conceal three distinct strategies:

- Economic predation (takeover, seizure of decision-making power) ;
- Disorganisation/weakening (putting the relevant market in difficulty) ;
- Destruction (disappearance of the targeted actor) ;

These strategies are fully in line with systemic economic warfare. This is a mode of domination that avoids the use of military power to impose lasting supremacy. It is no longer a question of subjugating the other by force but of making them dependent through technology or the *supply chain*. Control of the supply chain is an inescapable condition of strategic independence for both economic players and states. Could the strategic interest of plant proteins be the source of such a conflict?

Of the thirteen agricultural and agri-food cooperatives or industries attacked between 2020 and 2022, nine have an activity centred around plant proteins, three of which are also positioned on animal proteins, and four exclusively on animal proteins. As already mentioned, the production of

animal proteins is only possible through the use of plant proteins in animal feed. The keystone of the food system is therefore the production of plant proteins. Therefore, regardless of the cooperative or company involved, the impact on the production of plant proteins is unavoidable (from production to use at the end of the chain).

The impact is direct on cooperatives such as Eureden, Cérésia, Sollio and Cristal Valley, for example, since cereals are at the heart of their activities. On the other hand, the impact will be more diffuse for other players, such as Molson Coors, whose beer production requires cereals; Lactalis, whose milk production requires animal feed based on plant proteins; La Martiniquaise-Bardinet, whose alcohol is made from plants (cereals, beet, etc.). If we take these three examples, for Molson Coors, the impact on the plant sector may be felt through an overstock due to the cessation or slowdown of activity, or even a halt in orders from suppliers. For Lactalis, a slowdown or stoppage of production impacts on dairy farms, which cannot sell their milk stocks, thus weakening them and, by rebound, impacting the animal feed sector. In the case of Martiniquaise-Bardinet, the impact of the cyber attack may have an impact on the production of alcohol, which is based on...vegetable proteins.

It is interesting to look at one of the attacks in particular. The case of Ceresia shows how significant the consequences for the victims can be. Ceresia is a French cooperative with multiple activities: agricultural solutions and supplies (seeds, fertilisers, phytopharmaceutical products, collection), viticulture (viticultural solutions, supplies, services), logistics (storage of plant production), livestock (agricultural supplies and animal feed), energy (methanisation, photovoltaics), distribution (garden centres, DIY). It is therefore a real agricultural ecosystem representing more than 4,400 farmers and more than 620 employees.

"The attack took place on 20 November 2020, on a Friday evening. The first alerts were given on Saturday morning when several employees were unable to connect to the company's intranet from their mobile phones," recalls Olivier Bacon, Operations Director at Cérèsia. *The IT staff quickly went to the head office and found that the company was under cyber attack. Our entire system, internal and external, was paralysed. There was no ransom demand clearly displayed but a message, in Russian, 'Good luck to you'.*[3] Nearly a year after the attack, the cooperative had still not returned to its normal rhythm of activity. In addition to the attack itself, the attempts to recover data and get the system up and running again, the financial and human consequences have slowed down the resumption of activity. A real psychological trauma was felt by the staff and cooperators. Ceresia and its entire ecosystem avoided total destruction and therefore disappearance, but found themselves in a weak and fragile position for over a year.

On 05 May 2022, AGCO, a global manufacturer and distributor of agricultural equipment, announced in a statement that the company had been subject to a ransomware attack that affected some of its production facilities. It is possible that the company's commitment

to supporting Ukrainian farmers was behind the attack. Indeed, the AGCO Agriculture Foundation launched a humanitarian aid programme to Ukraine in March 2022 (funded by the Ukrainian NGO BORSCH)[4].

This could be an extension of the armed conflict in cyberspace, but once again targeting the agri-food sector (through the supply of agricultural equipment). It is therefore the entire *supply chain* (from the crop to the finished product via the production tool) that is targeted and all potential vulnerabilities are exploited.

Are the agricultural and agri-food sectors, which depend on plant proteins, facing a global earthquake? The few elements of analysis presented here suggest that a real economic war is being waged over such strategic materials. Reinforced by a conflict between two agricultural powers since 20 February 2022, the strategic issue of plant proteins is at the forefront of the media. However, for more than two years now, the major players in the sector have been victims of large-scale cyber attacks, paralysing their activities and weakening them. Is this a simple coincidence or rather a succession of acts of economic warfare aimed at the global restructuring of plant protein production?

In such a case, the current major geo-economic balances could be largely modified. The vector used here is the ransomware-type cyberattack... The economic security reading grid shows a hidden dimension of ransomware which, beyond and in the same way as espionage, is a real weapon of economic warfare and is able to meet strategic objectives on a global scale. ■

1 Jérôme DUPRE (2001), „Espionnage économique et droit : l'inutile création d'un bien informationnel", Lex Electronica, Vol.7, n°1. http://hdl.handle.net/1866/9506
2 https://www.enisa.europa.eu/publications/report-files/ETL-translations/fr/etl2020-cyber-espionage-ebook-en-fr.pdf
3 https://www.reference-agro.fr/sept-mois-apres-ceresia-nous-raconte-sa-cyberattaque/
4 https://www.businesswire.com/news/home/20220427005230/en/AGCO-Agriculture-Foundation-Donates-to-Farmer-Focused-Initiative-BORSCH-in-Ukraine

QNTYM RAILWAY ™

Mission

To provide inherently quantum secure, self defending, resilient digital infrastructure that removes complexity in your environment.

The BlockAPT Platform's **automated orchestration** and **centralised management** provides the integration and universal scalability required for the QNTYM Railway™.

... at the speed of possibility

NO COMPROMISES!

BLOCKAPT™

In conversation with Walt Greene.

Interviewer: Raj Meghani

Q: Hello Walt – great to speak with you. Let's start off by understanding where your interest in technology stemmed from.

Hi – great to speak with you Raj. Actually, when I was approached to contribute to the Cybersecurity Trends publication, I was honoured... and then it immediately dawned on me that I don't know any of you and you don't know me. I like to keep things conversational so, if you don't mind, I'll give you a little of my backstory and then we'll tackle a little of my personal exploits in Crypto tech!

For as long as I can remember, I always had a fascination and great affinity for technology. Though my family socioeconomics prevented me from actually owning a computer or anything 'high tech' personally, until much later in my teens, access to my elementary school's PC with Load Runner booting from that 5.25 inch Floppy Disk in 4th grade to time spent with my Grandparents' Mac Performa 550, with a processor rated at a scorching 33MHz, stacked just enough for Chuck Yeager's Air Combat, after I added 32MB more RAM to the integrated 4MB, of course, served as a catalyst fuelling and solidifying that love for tech.

By the age of 11, I had already helped my friends and family add RAM, overclock PC processors (overheating a couple which didn't go over well ... I digress), built my first computer, even connected my Grandparents computer to this new thing called the World Wide Web with a brand spanking new, 'insanely fast', 9600 baud modem.

Q: So it's fair to say, you were a 'fixer' or 'inventor' of technology at a young age although you didn't realise it at the time?

Inventiveness, and a distinct aversion to mathematical and physics-based 'presuppositions and laws' coursed through my veins from that early age and I had this way (sometimes much to the chagrin of my teachers!) of challenging the norms and coming up with solutions to (or creating) problems that hadn't even presented themselves to others yet (e.g. the very concept of factorials are the mathematical equivalent to, and an exercise in, logical absurdity - and I said as much to my teacher ... that didn't go over well ... at all).

On the inventive side, I have a vivid memory when, in fourth grade (9 or 10 years old), I drew a 'childish' schematic of an integrated, universal, all-in-one, magnetised computer cable on graph paper ... you know the

kind. As you may know, CRT monitors weren't too fond of magnets and the teacher immediately dismissed my idea, throwing the proverbial baby out with the bath water because that's all they knew at the time. 7 years later, the USB cable came on the scene and nearly 20 years after that, the MagSafe power cable debuted and would come to be a standard on 'a certain brand' of laptops. You know, that childish schematic doesn't seem so silly now ... it's too bad I didn't have my patent lawyer then - I think that was my first time 'seeing into the future' and recognising that there was a solution to a need that no one else even knew existed. Oh, and I still think factorials are absolute garbage but that's another story for another time - even though I did end up 'fixing' them in an essay to a university-level instructor of advanced mathematics (basically, my first white paper I suppose).

Q: Wow, impressive Walt. So how did you fall into this complex world of Cybersecurity?

By my mid 20s, I had the spectacular misfortune of encountering the Sasser Worm Virus. I had set up boot camp on my Grandparent's computer so my Grandma could use it for certain school activities - I forget what exactly she needed it for - and so the story goes: my Grandparents loved the Internet but the Internet did not love them back - it was the age-old anecdote of a Windows OS partition being active, websites were navigated to, things were downloaded, you know, the usual tragic romance. It only took about two days to figure out there was a serious problem as the machine slowed

and then started rebooting like mad ... which is nearly an eternity. Of course, I just really hadn't been aware of the virus or the symptoms until then. Luckily, for me, Sasser was more annoying than anything and didn't cause any real damage. Admittedly, those were a ROUGH couple of days entrenched in battle with a relentless foe that kept the computer in an unusable state but the ordeal did have a silver lining and managed to spark a deeper interest in cybersecurity, network technologies, architecture, topologies, and creating alternative approaches to them (which, of course, led to the multiple creations I have with QDEx Labs). That and meeting Marco Essomba: a now dear friend of mine, a world-class cybersecurity expert, a fellow inventor, and one of the most brilliant men I have ever had the pleasure of meeting.

Oh yeah, eventually, I did remove the virus from the computer; didn't mean to leave you hanging.

Q: How did you get involved in Crypto and Blockchain technologies?

After a decent stint in the broadcast and Live Video Production field, I turned back to my first love: tech. The year was 2012 and I had been hearing about a technology that had come out a few years before and had the potential to 'change everything' which everyone was calling it 'Bitcoin'. Of course, that's not the technology, merely the name of a project. Bitcoin and Blockchain are not interchangeable.

The underlying technology behind Bitcoin was actually called Blockchain, mixed with algorithmic hashing functions and transactional protocols but it was interesting all the same - even elegant in its bid to become the 'digital

gold standard' encoded with truth and transparency in the wake of the financial collapse of 2008.

Long before it's hyped-up use case as the unlikely replacement for fiat that the fanatics swear by, I recognised that Bitcoin's creation served as a proof of concept for the ability to eradicate the less-than-ethical practices of banking systems and their misuse of the fiat funds they were entrusted with via purely mechanical means. Blockchain represented a sort of digital truth, a catalyst in the realisation that not only can there be total transparency in business and financial dealings, but also individual sovereignty could be had on a global scale with the right technology. In reality, fiat was never really the issue; it's the widely accepted, terribly flawed allowances given to the financial facilitators and 'middlemen'.

Q: So you threw yourself specifically into blockchain technologies?

I spent serious time where I focused solely on the different technologies surrounding Bitcoin (i.e., before the hype, the digital glitz, and the virtual extremist ideological glamour took hold of everyone and spread like a virus). This was before the shallow, snarky hashtag term HODL came onto the scene causing focus of the limelight to highlight sentiment, charts, and candles rather than assigning a proper value based on the underlying tech.

From the decentralized mesh topology used in conjunction with blockchain tech for distributed ledgering to the algorithmic, hash-based guessing game used for 'Proof of Work' in 'mining' (for validating transactions while also releasing new Bitcoins into the

wild for validating rewards), I walked through every part of what has often been illegitimately dubbed the 'first digital currency' (fun fact: there were at least 3 cryptocurrencies predating Bitcoin - one as early as the late1980s).

I began my decent into the new tech's 'rabbit hole' by diving into 4 topical generalities that formed the basis of Bitcoin. Generally speaking, when looking at the underlying tech of Bitcoin, I found:

1. A decentralized network (mesh) topology for nodes;
2. Blockchain technology used for the accurate, chronological, immutable record keeping of transactions;
3. Interconnected, distributed databases;
4. Algorithms that include hashing functions used for validating transaction lists and 'mining' (or releasing new Bitcoins, up to the 21 Million Coin limit) but most importantly for validating transactions ... again, this is an elaborate, automated 'guessing game' (a kind of 'brute-forcing', if you will, for the cybersecurity reader).

Q: What did you find in terms of some of the misconceptions surrounding cryptocurrencies?

One of the biggest misconceptions about Bitcoin, and the many other crypto projects that have come after, is that it was a technological revolution of some kind but that's simply not the case. Bitcoin may have made certain blockchain related techs popular, but they were far from being revolutionary at the time of Bitcoin's inception and white paper:

- The UTxO balancing system, which is very similar to how bank notes are used, is based on an idea that was created at least 11 years earlier called HashCash (these Unspent Transaction Outputs serve as the inputs to fulfil future transactions)
- A mesh topology (albeit in slightly different form as opposed to the very specific, decentralized network called a distributed network) is a network architecture developed in the 80s by the US military
- Blockchain technologies (chronological, cryptographic-based databasing) were developed long before Bitcoin ever came into existence (circa 1991 and even some aspects as early as the 1970s)
- 'Hashing' (as it is used for Bitcoin in the Proof of Work guessing game) also derived from HashCash

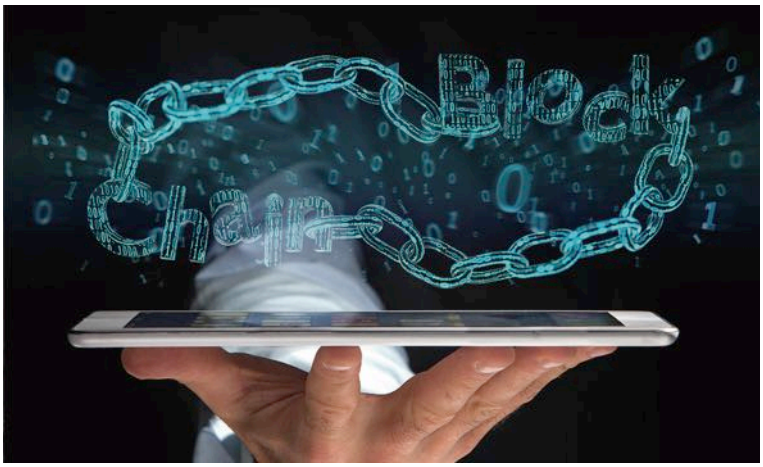
So many people have asked me to explain Bitcoin and Blockchain; they come to me completely confused about blockchain techs, all the buzz words, cultish maximalism, ideological trope, and hype - I cut through all that and give them the blunt truth of blockchain and the network system crypto projects are predicated on: what you find

behind any 'crypto' project is that it's just a network of identical computer databases that uses encryption (a standard security protocol) in a specific way to ensure the historical records cannot be changed and remain accurate. In crypto, the protected data consists of simple lists of exchanges of value that have occurred (or digital transaction tallies). For all the fanfare, there's really nothing new under the hood of Bitcoin nor is there anything mysterious - it's just a different way to duplicate and use databases.

The true innovation really stems from the popularity of the use case itself.

Q: Tell me Walt, what was your 'Eureka' moment having delved into blockchain technologies?

My reasoning for looking at blockchain-based technologies, like that which undergirds Bitcoin's entire digital ecosystem, was very specific - I knew fairly quickly that blockchain was not the missing piece to my puzzle but what I was working on could benefit greatly from one VERY specific aspect that the crypto industry made popular, and that piece was: a decentralized network.



What I also came to a conclusion on was that as interesting as blockchain-based digital ecosystems were, the realities of the serious constraints in speed, security, and sustainability (largely due to the fundamental security tech called encryption) would prevent any crypto project's network (labelled Layer 1 in the crypto industry) from scaling to the point of usefulness without the need for third-parties again (these are called Layer 2s in crypto

or really just fancy middlemen) ... and even then, they were just not going to cut it. This was ESPECIALLY true where current cybersecurity standards and hygiene were concerned, (e.g. 70% - 80% of all DeFi hacks are carried out on Layer 2 platforms) ... not to mention the existential threat that the exponential advancements in quantum computing pose to encryption.

I needed to create something else; something new for my project with new pieces.

Although I am a realist when it comes to the hype and wild claims associated with so many crypto projects out there, I do not believe that the technology is 'garbage' as some anti-blockchain/anti-crypto extremists claim.

If blockchain isn't what the fanatics say it is and the networks can't possibly support what they claim they can, because of the inherent limitations, then what good is it?

Though blockchain tech, in my opinion, should not continue to be pushed and worshipped as the general catch-all technological 'saviour', that it obviously is not, it does make perfect sense to use it in a privatised setting for individuals or companies needing chronological, accessible databases that cannot be tampered with from inside or outside the organisation performing multiple functions with mechanisms that allow for pruning, to keep ledgers smaller, and with better options for optimisation.

Moreover, the technology that permanently connects the blocks in a chain is ironclad. The unchangeable nature of validated, written blockchain records is where the real value and use lies. A validated blockchain entry is tantamount to digital truth and the historicity of a blockchain is the only aspect of the tech that is, in fact, quantum resilient. Everything else in the crypto industry is under serious threat when considering quantum computing that utilises and/or further optimises the usability of Shor's Algorithm whether hardware or software related.

Q: Something you said earlier, before our Q&A, while we were conversing about the differences between innovation and invention was interesting. Could you sum that up Walt?'

Yes, it's true that I've designed an entirely new digital infrastructure based on an alternative form of cryptography, involving proprietary algorithms, agents, automated playbooks, and a completely new decentralized network architecture; I'm an inventor, it's what we do.

> ***"Mechanics think inside the box, innovators think outside the box, but inventors, they smash the box into tiny pieces and create something altogether new."***
>
> **- Walt Greene**

Q: So what does the future hold for you and your teams, Walt?

I still believe that blockchain tech has value and even now, my team and I are working on optimisation methods for current blockchain techs in order to bring them into the future with true usability in a real-world setting. They just need to be used properly. Watch this space...

It's just now starting to get really interesting, friends. I'm glad we got this chance to chat and hope to get the opportunity to meet in person in the future so you can tell me about your journeys in tech!

Until then, keep your thinking cosmic level! ■

BIO

Walt Greene is Founder, CEO & CIO of QDEx Labs. As an inventor, technologist, self-taught physicist (multiple patents pending), amateur mathematician, and enthusiastic entrepreneur, Walt has successfully run a tech holding company, DHCT, that started out as a cybersecurity consulting firm, for over 5 years. Greene has further ventured into the medical tech field, with his business partner Dr. R. Gillis, under Sector 3. He serves as Co-Founder, CEO, and CIO of Sector 3 with multiple patent filings for tools and devices that are being reviewed by some of the largest Med Tech companies in the US. Greene is a proven inventor, technologist, leader and visionary who has strategically surrounded himself with industry veterans, high-ranking officials, and thought leaders. With next-gen technologies Greene has orchestrated and developed, as a major contributor to the QDEx Network, he envisions QDEx Labs' technology drastically elevating, not only the current blockchain industry but the entire global digital infrastructure for generations to come. Watch this space!

QNTYM RAILWAY ™

SECURITY

Deep iniegration through multiple layers of security enabling a single view of all applications and simplified reporting.

SIMPLICITY

Integrated with leading vendors, users benefit from having threat intel, vulnerability, device & incident response management capabilities reducing complexity.

SPEED

Single command and control & control of devices with automate responses enables scans, threat detection and response - 24/7, resulting in faster MTTD/MTTR response rates.

SUSTAINABILITY

QNTYM technology will decrease energy consumption by 10,000 fold or more for any system that utilises the QNTYM Railway™.

BLOCKAPT™

Why are cryptocurrencies so attractive to cybercriminals?

Author: Marco Essomba

Introduction

Unless you have been living under a rock since the Global Financial Crisis of 2008-09, you would have noticed continuous headlines of crypto technology and cryptocurrency scams that are making the news on a regular basis.

Cybercriminals in general and crypto fraudsters in particular are always on the lookout for a way to exploit their victims for financial gains. Whether used as a store of value or as a pure speculative financial instrument,

cryptocurrencies as a digital currency do not provide the same level of security as traditional currencies provided by financial institutions like banks.

Why are digital currencies so attractive to cybercriminals? What advice and guidance can you or your organisations follow not to fall prey to crypto fraudsters/scammers? This article will provide some insights and specific guidance.

Understanding crypto technology and why it is a game changer

To understand the underlying foundation of crypto technology and cryptocurrencies, it is worth exploring how the current banking system operates. Traditional banking relies on trusted institutions that play the role of proxies to ensure that all parties taking part in financial transactions are verified, authenticated, and authorised accordingly.

Those proxy institutions provide the confidence required for the banking system to operate effectively and securely. It is a centralised system where trusted entities at the national or international level are carefully selected to enforce and keep the trust between participating entities in financial

BIO

Marco Essomba is the Founder & CTO of BlockAPT – a UK based innovative cybersecurity company.
An influential thought leader in cybersecurity with almost 2 decades of working with some of the largest and well known institutions. Marco's passion, expertise and knowledge has culminated in the design of the unique central management, command and control BlockAPT platform which allows businesses to stay ahead of cyber threats 24/7.
Marco is often called upon as a panellist at cybersecurity conferences and has been a host ambassador at CyberTalks, one of London's largest cybersecurity events. With 16,000+ followers on LinkedIn and 35,000+ on Twitter, he is sought after for his quick problem-solving approach and helping businesses futureproof their security infrastructure.

To find out more about BlockAPT, please visit https://www.blockapt.com
To find out more about Marco Essomba, please visit https://www.linkedin.com/in/marcoessomba/ or https://twitter.com/marcoessomba

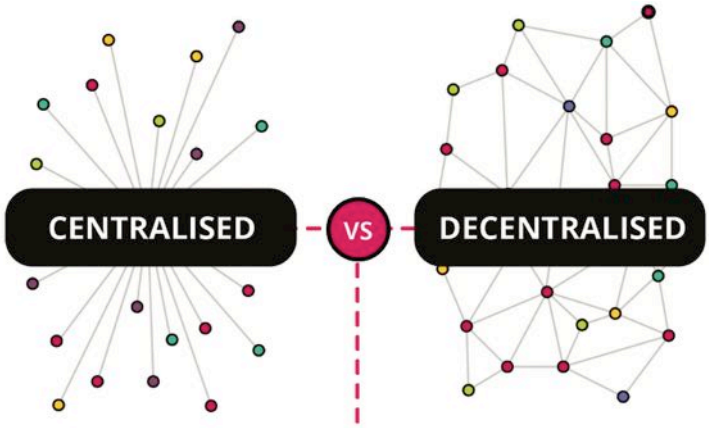
transactions at national or international boundaries. Some of those institutions include central and commercial banks.

Cryptocurrencies on the other hand relies on technology to enforce the trust. Unlike the traditional banking system where physical banks are required to keep the whole system working as per the agreed rules of trust, cryptocurrencies rely on cryptography *technology* to enforce the trust between participating entities.

To centralise or to decentralise - that is the question

In a completely decentralised crypto financial system or DeFi (decentralised finance), cryptography technology is used to ensure that parties participating in transactions are verified, authenticated, and authorised. Technology, rather than a centralised physical entity, is used to enforce "trust and peace".

On the other hand, in a centralised crypto financial system, an entity such as a crypto exchange is used to enforce the trust. Popular exchanges include FTX, Binance, and Coinbase. This is similar to traditional banking in a way, however, crypto technology is still used to verify, authenticate, and authorise transactions.



Exchange controls funds	User controls funds
Not anonymous	Anonymous
Hacks & server downtime	No hacks & server downtime
Easy to use	Not easy to use
Advanced tools	Basic features
Liquidity	Low liquidity

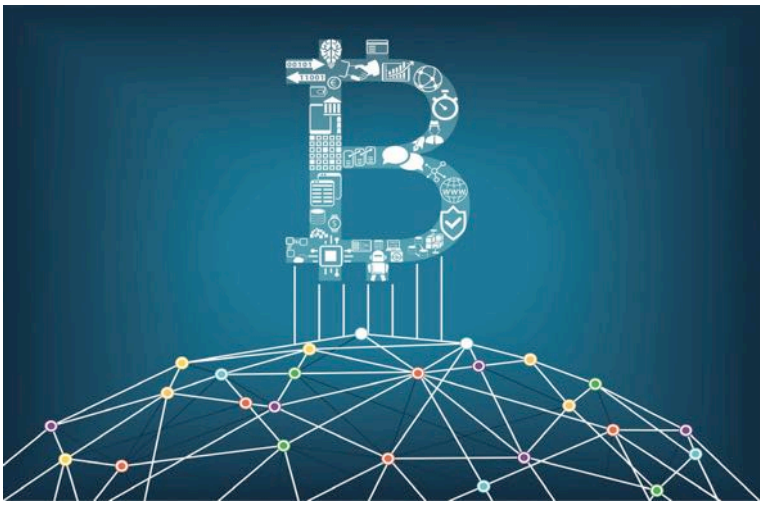
For both centralised and decentralised crypto architectures, the underlying technology that makes up the foundation of cryptocurrencies is *blockchain*.

In mathematics & cryptography we trust

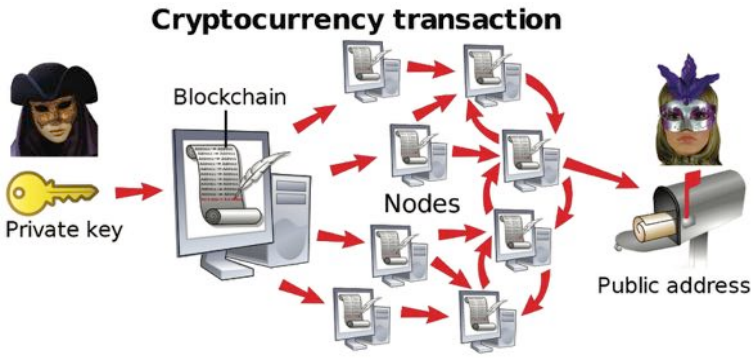
Think of blockchain as a secure database backed by cryptography technology, that is, at least up to now, "unbreakable". This means the information written on the blockchain cannot be falsified. In other words, blockchain can provide non-repudiation by giving participating entities the assurance that a person or system cannot deny the validity of the data stored on the blockchain, and by doing so providing a proof of the origin and the integrity of the data stored on the blockchain.

The underlying cryptography technology that is the foundation of blockchain is based on public-key cryptography, often called asymmetric cryptography. A technology that uses a pair of keys. Each pair consists of a private key and public key. The private key is secret and only known to the source that generated it. On the other hand the public key can be shared widely and openly published. The public key can also be used as an address or as a means to identify the originator of a message or a transaction, and to encrypt data. The private key is used to decrypt the data encrypted by the public key. The public and private keys are mathematically linked.

Both keys are interdependent and linked by a cryptographic algorithm based on mathematical functions. Those maths functions rely on prime



numbers. The prime numbers are kept secret. Messages or transactions can be encrypted by anyone, via the public key which is shared with anyone, but transactions encrypted by the public key can only be decoded by someone who knows the prime numbers (private key).



With classical computers, finding those prime numbers is very difficult, which is known as the «factoring problem». It is this factoring challenge that makes blockchain a robust and secure technology that can be used as a way to verify, authenticate, and authorise transactions, hence replacing traditional banks as a centralised *trusted* entity. With blockchain, in technology we trust!

Cybercriminals and cyber heists

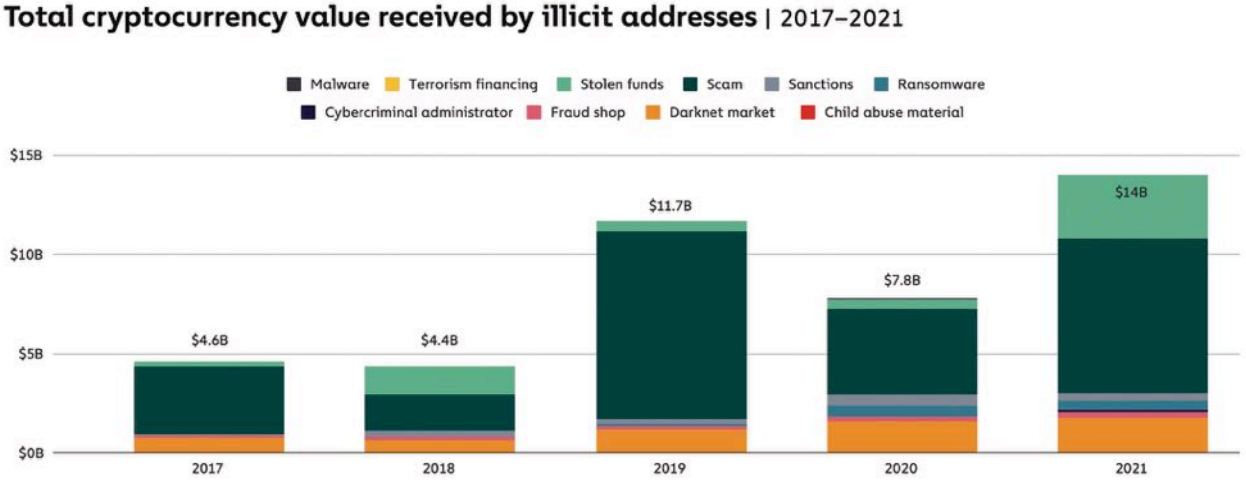
The amount of cyber heists have increased dramatically over the past years. This is not surprising as criminals in general and cybercriminals in particular are always looking for ingenious ways to exploit the general public. This is true for the physical world and even more so in the digital world. Attempting to physically break into a bank vault successfully and getting away with it is today an increasingly challenging if not an impossible task. Even if you are successful, the chances of an escape are slim.

In contrast, in the digital age, transactions are anonymous. One can hide behind a computer, and conduct malicious activities almost undetected. Tracing back an attacker in a global web of computer networks can prove technically and legally an insurmountable task even for institutions or international organisations with the legal and technical expertise.

Cybercriminals are winning

For cybercriminals and crypto fraudsters/scammers, crypto is a golden opportunity. As an example of recent hacks worth highlighting:

1. An anonymous hacker stole roughly $600 million in cryptocurrency from Poly Network;
2. Hackers stole at least $150 million from crypto exchange Bitmart;
3. The Badger DAO hack resulted in the loss of $120 million;
4. Coincheck attack in 2018 saw roughly $530 million stolen, making it the biggest crypto heist ever recorded;
5. Theft of more than US$326 million (A$457.7 million) of Ethereum tokens from a blockchain bridge;
6. Crypto criminals stole a record US$3.2 billion (A$4.48 billion) worth of cryptocurrency, according to Chainalysis.



Source: *Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity, JANUARY 6, 2022 | BY CHAINALYSIS TEAM [https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/]*

It's all about the money

Although these cyber heists appear stunning, cybersecurity incidents like this are not new in the crypto world. However, the sophistication and the size of these heists appear to be growing and more frequent. This can be explained by the fact that the general public are drawn to the crypto world by many "get rich quick schemes" by speculating or "investing" into crypto as cryptocurrency prices have significantly surged over the past years.

There is a lot of money to be made in the digital world, and cybercriminals know it. It's digital. It's seamless. It's anonymous. For those with the skills and resources to conduct such attacks, the risk of getting caught is relatively low compared to physical heists at traditional financial institutions. As the usage of cryptocurrencies grows, it is expected that these cyber heists will also increase.

Centralised or decentralised here they come

Cybercriminals will continue to target centralised exchanges and decentralised finance (DeFi) services. Centralised exchanges are targeted by cybercriminals because they store users' assets in "hot wallets" or digital wallets that are connected to the internet. Anything connected to the internet can be considered hackable by default. Therefore, centralised exchanges will continue to be under attack and potentially more vulnerable to sophisticated cybercriminals.

Whilst traditional banks offer certain guarantees such as deposit insurance up to a certain amount, there are no such guarantees when holding cryptocurrencies assets. Some exchanges or third-party crypto services providers might have liability insurance to cover losses, but the level of coverage — if there is any at all — varies greatly.

Decentralised exchanges or DeFi have also been targeted. DeFi which is supposed to be more secure as it does not rely on a centralised exchanges where assets are stored (hot wallets), runs directly on top of blockchain platforms such as Ethereum which is an open-source blockchain with smart contract apps or Bitcoin which is renowned for his financial speculative usage.

Usually, cybercriminals will exploit vulnerabilities found in the smart contracts or applications running on Decentralised platforms. These types of attacks require sophisticated knowledge on how to exploit these types of software flaws caused by the way those are designed and deployed.

Guidelines to protect yourself as an individual or as an organisation

From my own experience, I go by the mantra that anything that is connected to the internet is hackable. Only, disconnected systems that are completely offline or behind an "air-gapped" system can claim to be

'unhackable'. One can assume that there is always a risk for any online system. However, certain guidelines can help mitigate these risks dramatically.

1 Do your own research and due diligence on your crypto service provider:

a. When using a crypto wallet or exchange, scrutinise and research the service provider, and look at the certification and credential they hold in relation to cybersecurity

b. Do they have a person responsible for security such as a CISO?

c. What is the track record of the organisation in defending against cybercriminals?

d. Is it a public or private organisation?

e. Has the organisation received any accreditation by known trusted bodies such as NIST, ISO, etc.?

2 Do your due diligence on service providers technology:

Scrutinise and research their technology:

i. What type of encryption standards are they using? (b) Are they using 2-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) for their external-facing web services such as website and crypto account logins?

ii. What security measures do they have in place for their APIs (Application Programming Interface)?

iii. Do they use secure hardware keys or HSM (Hardware Security Modules) to provide extra security for sensitive data such as crypto keys?

iv. Do they provide mechanisms for extra checks before approval transactions such as transfers and withdrawals by enforcing IP addresses filtering and whitelisting, or 2FA or MFA?

3 On a personal level, ensure that your "crypto devices" are as secure as they can be:

Trust no one with your personal devices security

i. On devices used for your crypto transactions, ensure you maintain an updated version of your security software such EDR (Endpoint Detection & Response).

ii. Ensure you have multi layers defence in place, for example using traditional anti-virus, and an Advanced EDR technology on your laptop or mobile device.

iii. Use a secure Virtual Private Network (VPN) where possible

iv. Avoid carrying secure transactions on public places using public WiFi.

v. Use a secure cold storage device for your hardware wallet, and always ensure that you buy your hardware device from a trusted manufacturer, and brand new. Do not buy your devices on eBay or second hardware stores.

vi. Encrypt everything and use 2FA or MFA everywhere possible.

vii. Backup your data, and store your private key or backup mnemonic recovery phrases in a trusted physical vault such as in bank where possible.

Conclusion

The world is changing and technology is changing even faster. Crypto technology will revolutionise how we carry out financial transactions and how people use technology to transfer, store, and exchange value.

The first well known applications of crypto technology are Bitcoin and Ethereum, just to name a few. The applications of crypto technology in centralised and decentralised financial transactions are gaining momentum. Bitcoin is already on track for mass adoption as it grows even faster than the internet.

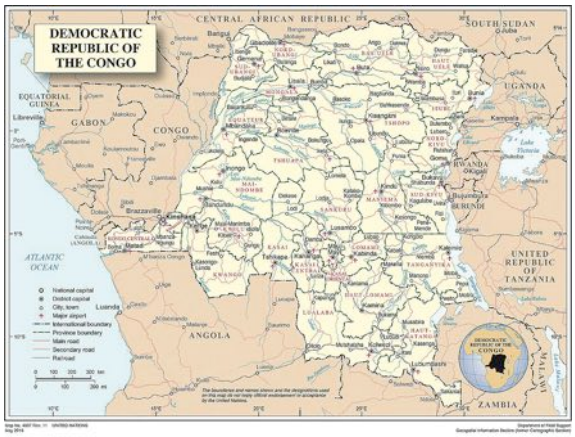
Cyber heists are scary no doubt. But the fundamental question for you personally is: are you in or out of the crypto revolution? ■

[1] https://cointelegraph.com/bitcoin-price
[2] Poly Network hack: Some $600 million stolen in biggest crypto theft in history - CNN
[3] Crypto exchange Bitmart says hackers took $150 million
[4] https://www.coindesk.com/tech/2022/02/02/blockchain-bridge-wormhole-suffers-possible-exploit-worth-over-250m/
[5] https://www.cnn.com/2021/08/11/tech/crypto-hack/index.html
[6] https://www.cnn.com/2021/12/06/tech/bitmart-ethereum-bsc-hack/index.html
[7] https://money.cnn.com/2018/01/29/technology/coincheck-cryptocurrency-exchange-hack-japan/index.html
[8] https://www.coindesk.com/tech/2022/02/02/blockchain-bridge-wormhole-suffers-possible-exploit-worth-over-250m/

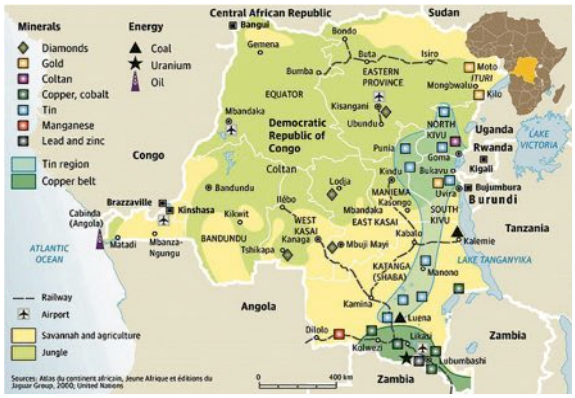
Proof of trust.

Author: Mauro Vignati

The Democratic Republic of Congo (DR Congo) is an immense country with an area of 2,345,000 km2 and an estimated population of around 86.73 million, ranking among the world's top twenty nations. It has a young population (70% of the total) with around 40% living in urban areas.



It is a country divided into 26 provinces, where the 2006 constitution gives broad independence in political and administrative management to the provinces. The



country is rich in natural resources; forests occupy half of the territory. But besides the 80 million hectares of arable land, DR Congo is known to have more than 1,100 minerals and precious metals underground.

Important quantities of diamonds, copper, cobalt, tin, gold, uranium, zinc, silver, germanium, tantalum, niobium, manganese, iron and many more are found. These resources are in the form of mining indices or economically exploitable reserves. And the sector's contribution to the national economy is essential. Indeed, it accounts for almost 90% of the country's exports, more than 15% of the gross domestic product and almost 20% of the national state budget.

The mining sector is clearly the main driver of the country, generating overwhelming dependence in terms of exports, government revenues and GDP growth.

Despite this wealth, DR Congo struggles almost permanently with financial instability and economic recessions. Rough national policies and poor management of public affairs, war and insecurity have generated a climate of profound distrust in state management, creating a parasitic system now firmly entrenched in the social and economic fabric, degrading state mining enterprises, and generally throwing the population into persistent poverty.

Arbitrary and discriminatory taxation, mediocre physical infrastructure, marginal enforcement of property rights, and an approximate rule of law have driven a gradual mutation from a formal and mechanised mining industrial power to an informal, illegal and rudimentary market. In several regions of the country, parallelism and power conflicts between customary and administrative authorities end up influencing mining activities. The Congolese gold trade is largely informal, oriented towards neighbouring countries in the East. The high level of taxes constitutes a major obstacle to the formal marketing of gold, and more generally of the entire national mining sector.

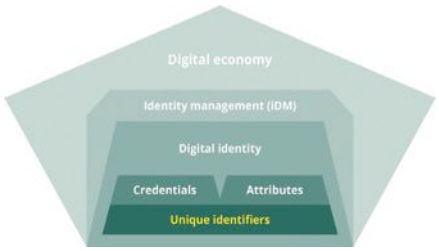
When looking at artisanal gold production in DR Congo, the informal aspect seems to prevail in all provinces. Recent field studies[1] tell us that in the five provinces in the east of the country - Haut-Uele, Ituri, Sud-Kivu, Tanganyka, Tshopo - around 80 per cent of all Congolese gold is mined, with 230,000-250,000 gold prospectors contributing between 8.1 and 12.5 tonnes per year, with an average purity of 22 carats.

A gold miner would be able to extract 0.93 grams per day during production times. The hierarchical organisation starts with the mine bosses, followed by the pit bosses, then the transporters and finally a supporting labour force.

Living and sanitary conditions are extremely difficult, often women and children work there. Huge quantities of mercury and cyanide are poured into the waters. Much of the artisanal gold ends up in neighbouring countries, in Uganda, Rwanda, Burundi, Tanzania, passing through difficult roads with a strong presence of armed people. But this route is preferable to that of the central government, which is burdensome in terms of administration, taxes and a general lack of willingness to formalise the sector.

During 2020, I was approached by a group of people, Congolese and European, experts in economics, digital and finance, who intended to accelerate the formalisation of the sector through blockchain technology. The project had several aspects.

Provide a unique digital identifier: The new national identifier would be based on birth certificates or other documents that could prove the identity of the country's inhabitants. It would have been associated with a biometric element, such as an iris scan. A government-certified digital ID would have prevented minors from being employed in the mines, their attendance at educational institutions could have been recorded, increasing education and decreasing exploitation. In addition, the digital ID would have served to associate the mined gold with the responsible miner, transporter, and helpers.



Issue a new national stablecoin: the Congolese Gold-Backed Stablecoin (C-GBS) would be issued, backed by gold reserves as collateral. Gold extracted from mines would be registered on the blockchain, accumulated in the national reserves, and sold externally by the government. The new currency, a Central Bank Digital Currency (CBDC) would have had the advantage of being a stable currency, avoiding inflationary rates of 30%-40%. Increasing or decreasing the gold reserves would have kept the CBDC stable. An increase in reserves would have put more C-GBS into circulation, a decrease in reserves would have burnt C-GBS. The central government would thus have stemmed the flight of gold to neighbouring countries, an uncontrolled traffic with huge losses for the country's economy. By increasing profits for the government, taxes would have decreased, enticing miners to work in this new formal process.

Generate a currency wallet for each inhabitant: Each inhabitant of DR Congo would be allocated a wallet, so that C-GBS could be used. Participants in the mining chain would have been paid in C-GBS: upon delivery of the mined gold, they would have been rewarded by depositing C-GBS in their wallet. This would have prevented the miners from being assaulted on the day of collecting their pay in cash. And it would have been possible to verify that the gold mined matched the payments made in C-GBS. This would have created a C-GBS-based economy, as tokens would have flowed from the miners to the entire economic sector of the country.

BIO

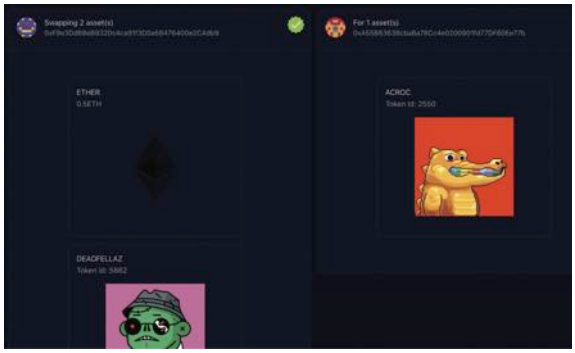
Adviser on New Digital Technologies of Warfare, International Committee of the Red Cross (ICRC, Switzerland), Mauro Vignati has worked in cyber threat intelligence and cybersecurity for the past 18 years. He worked for KOBIK, the first unit of the Swiss government dedicated to fighting cybercrime, and then for MELANI, a governmental body dedicated to protecting Switzerland's critical infrastructure against cyber attacks. Afterward, he worked for the Department of Defense and the National Cyber Security Centre (NCSC.ch). Mauro has a long experience in the prevention, identification, and analysis of cyber crimes and advanced persistent threats. He also spends his time researching in the field of communication technology innovation in different political and economical environments. He holds a master's degree in literature and an Executive Master in Criminology. He has taught at universities in Berne, Geneva, and Lugano.

With these measures, a 'Fair Trade' would have been guaranteed, without the exploitation of minors and a fair reward for the workers. It would have ensured that the gold mined was 'Green Gold' (traceable gold) and that the country could finally have a stable currency, controlling inflation, stimulating foreign investment, growing the economy and facilitating trade. All while eliminating illicit trafficking, armed crime and suffering for the local population. On paper, this project, beyond a questionable privacy discourse, had everything to be a good one.

But unfortunately, at the beginning of the chain, there was a bigger problem: the trust of those who controlled the gold mining. Who would certify that such a miner had actually mined that amount? Who would have had the authority to record in the blockchain that extraction had taken place? It would be the same agents who had hitherto avoided putting the extracted gold into the legal circuit by passing it through illegal and risky routes. So at the root of all this innovative technology, the traceability, visibility and immutability of transactions, the birth of a new future stabilising currency for the country, there is nothing but the old concept of trust. Without trust, not even the most modern technology can work.

From recycling platform to the new frontier of cybercrime

The Web3, DeFi and cryptocurrencies have for some years now mainly been talked about as a money laundering platform for established criminal schemes such as ransomware. But money laundering via coins or NFTs is turning into crime against the actors of these platforms or against the platforms themselves over the past year. And here, too, trust plays the main role. For example in NFTs. The scam technique starts with a contact via Discord, between the scammer and the person trying to sell their token. Then the scammer shows 'their' wallet on OpenSea, to give more confidence to the seller, who will feel comforted in trading with a person who also collects NFTs. The victim will then be 'diverted' to an exchange platform, created ad-hoc to execute the scam.



The exchange platform Swaptic.io (@hoffcolors)

In this case, the criminal convinces the victim that he will pay 0.5 ETH plus one NFT Deadfellaz to receive his NFT Acroc. The criminal then sends a link to sign the exchange. But upon confirmation, the owner realises that he has given access to his entire wallet to the criminal, who has used it and emptied it.

But crime in this area is not limited to petty fraud. People put their trust in technological innovations that, despite still being in a beta version of development, are already being used in productivity. Think of 'bridges' for different blockchains and sidechains. Gaping codes that allow criminals to infiltrate and steal tens of millions of dollars. Or the numerous oracle manipulations. DeFi's own platforms become victims.

Once again, as in the case of Congolese gold, the technological innovation that wanted transparency in transactions and governance can do nothing against the misplaced trust of its users.

PoH, Worldcoin, POAP: technological solutionism

In the meantime, several initiatives have sprung up to overcome the trust problem, essentially to identify that the people one interacts with on the Web3 are real and can be recognised as such. Proof of Humanity (PoH), where to sign up for the registry, you make a short video of yourself, stake a returnable deposit of 1.5 ETH (more or less $400, perhaps the hardest thing to implement in the Global South) and find a person who is already certified to vouch for you[2]. Or WorldCoin, which is scanning hundreds of thousands of irises, but which worries about acquiring tons of biometrics data[3]. Or the Proof of Attendance Protocol (POAP), where users collect attendance tokens to prove they were physically present at a specific event. These are all experimental initiatives and some of them well-intentioned. But the problems of immature technology are being answered with more immature technology. What is referred to as 'technological solutionism'[4] is unlikely to change the fact that trust is at the heart of any technology.

In his blog, Moxie Marlinspike wrote[5]: "We should accept the premise that people will not run their own servers by designing systems that can distribute trust without having to distribute infrastructure. This means architecture that anticipates and accepts the inevitable outcome of relatively centralised client/server relationships, but uses cryptography (rather than infrastructure) to distribute trust. One of the surprising things to me about web3, despite being built on "crypto," is how little cryptography seems to be involved!"

More centralisation and more distribution of trust through encryption. If on the first point the democratic experience of recent decades seems to confirm the necessity of centralisation for good social functioning, on the second we will have to reflect on how we want to increase trust in the virtual world. ■

1 http://cegemi.com/wp-content/uploads/2015/08/Nkuba-Zahinda-Chakirwa-Murhi-de-Haan-Bashwira-2018.-Lor-artisanal-congolais_Rapport-d%C3%A9valuation-du-mercure-en-ASGM-avec-ACE-UNITAR.pdf
2 https://time.com/6142810/proof-of-humanity
3 https://podcasts.apple.com/us/podcast/worldcoin-where-techno-optimism-meets-techno-colonialism/id1552627235?i=1000558511758
4 https://www.publicbooks.org/the-folly-of-technological-solutionism-an-interview-with-evgeny-morozov/
5 https://moxie.org/2022/01/07/web3-first-impressions.html

The trials & tribulations of the crypto world - a beginners guide.

Author: Raj Meghani

Blockchain technologies have changed the way in which business is being done today compared to the good old traditional methods.

Now I'm no expert in this field but even I can see the complexities in trying to decipher the various details in this space. The simplest description I have come across is that Blockchain works as a distributed network that enables the decentralisation of data – this makes it a more secure and hard to tamper technology.

So, let's start at the beginning. What does Crypto mean?

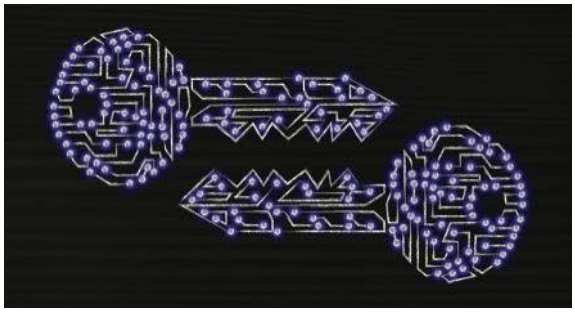
"Crypto" refers to the various ***encryption algorithms and cryptographic techniques that safeguard entries***, such as elliptical curve encryption, public-private key pairs, and hashing functions. Cryptocurrencies can be mined or purchased from cryptocurrency exchanges.

Quite simply, cryptocurrencies are tradeable digital assets or digital forms of money, built on blockchain technology, that only exists online. Through advanced encryption techniques, anyone can transfer 'virtual' money from one entity to another without central banks getting involved.

Storing data cryptographically in a decentralised framework where the power is in the hands of the people makes the hacking of data even more difficult. Combined with the transparency of the blockchain making it untraceable, it's easy to see why blockchain has gained popularity. It's also

BIO

Raj Meghani is Co-Founder & Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, UK based innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience.Raj has also been appointed as a Non-Executive Director to the Board of Money Matters Bank. Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 25 years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans. Raj is Editor for Cybersecurity Trends UK which has a global presence and is active in thought leadership and knowledge transfer of cybersecurity and business risk management.
LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/
Twitter: https://twitter.com/blockapt
Company website: https://www.blockapt.com

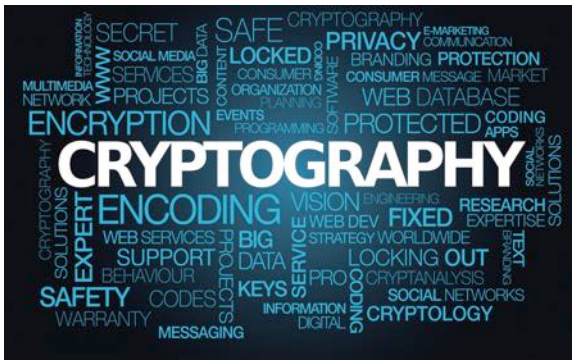


easy to see why cyber attackers are actively exploiting vulnerability loopholes in this lucrative market.

Today, it impacts people of all backgrounds and businesses. From online peer-to-peer transfers, trading, supply chain, healthcare, retail goods, right through to purchases of properties. It's a growing trend with the most expensive property to date being bought entirely with Cryptocurrency being a Miami beach home in the affluent Surfside district – for a cool $22.5m. On the other scale, in September 2021, Burger King fast food branch in Germany accepted bitcoin for its online orders and deliveries.

It is easy to understand how digital cash is being exponentially adopted across the world. In particular, we can see the rising opportunity in developing countries where there is fiscal uncertainty amplified with a politically unstable economy.

Opening the doors to crypto innovation is great and holds its value in society but there is still the aspect of security issues behind the scenes which remains a big challenge and can make the blockchain vulnerable.



We have seen many stories and cases where attacks from hackers have drastically moved market valuations for currencies like Bitcoin who has been the target of several DDoS attacks.

So where are the risks?

1. It's an unregulated market:

Operating in a decentralised market where there is a lack of governance and governments globally are increasingly imposing restrictions is the main concern.

2. Cryptocurrency wallets can come with security flaws:

Even in hard wallets, cyber hackers through malware can still find a way in to steal millions in crypto assets from users' systems. Once they have access to the crypto funds, they can divert them to a different wallet. The phrase 'Caveat Emptor' springs to mind…

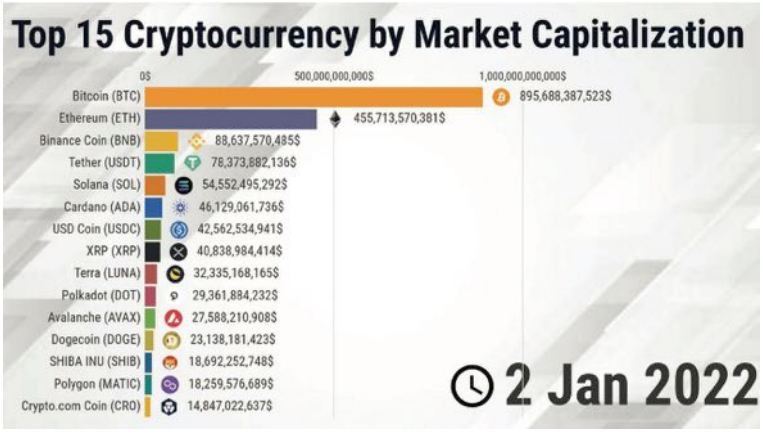
3. Losing your private key could mean adios to your funds forever:

Even with all the best intentions in the world, individuals could lose their private key which means the funds are irretrievable as once the transaction has been made there is no real way to reverse engineer it. However, with new quantum secure technology (like MicroTokenization Exchange®) emerging, this risk becomes a fear of the past.

4. Abusive management of currencies for illegal activities:

With the value of all crypto-assets in circulation at almost $3tn in Q4 2021, it's easy to see why criminals have used this market to channel illegal activities such as tax evasion, money laundering and financing of terrorist activities.

So there we have it. In 2009 we saw the first decentralised cryptocurrency – Bitcoin – created by Satoshi Nakamoto. The first gold exchange traded product – Central Fund of Canada – was founded in 1961. Fast forward to today and we have Gold with a market cap of $11.4 trillion – **only just over 5 times** the size of the cryptocurrencies in circulation which has surpassed $2 trillion.

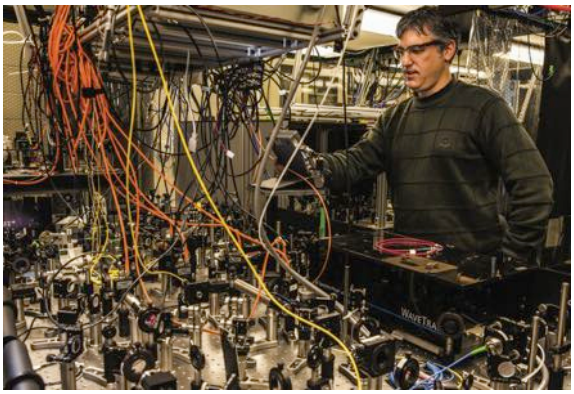


The crypto market is not going to stop. This is a market where organisations, institutions and governments will need to readjust. Where speed, security and simplicity will be king. Given the first adopters of cryptocurrency were gamers, it's apt to say this market is a serious game changer with a potential lucrative upside. ■

Advanced cryptology: bright ideas from the past to improve future security?

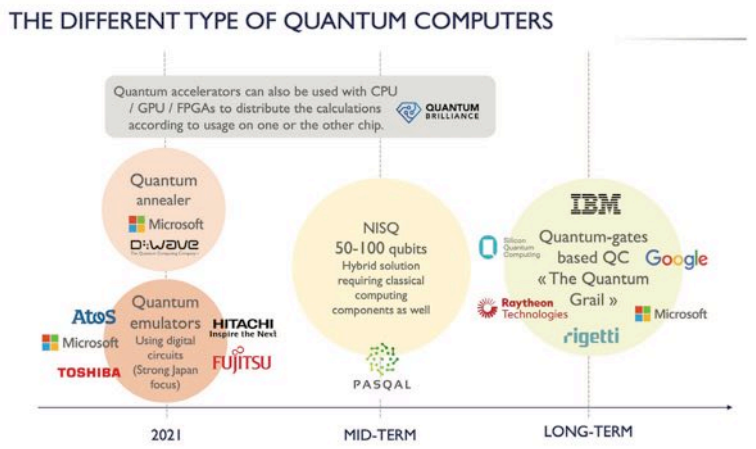
Author: Laurent Chrzanovski

We have no doubts that the future of cryptography will be quantic (see Cybersecurity Trends Issue 1:2022). Yet quantic servers and quantum computing are (and will be for a long time) extremely expensive and require top specialists to manage them.



A specialist setting a quantum computer at the Duke Quantum Centre © Duke University

Hence, if you are not a huge corporation (i.e. Forbes top 200 or near), investing in quantic servers and programmers is simply unaffordable. As a consequence, top-notch quantic services are and will be, provided as "pay per service" by the very few "above the top" IT companies i.e. mainly by Google, Apple, Facebook, Amazon, Microsoft (GAFAM) and their Chinese competitors – no matter who is the manufacturer of the quantum computer itself – , to which a few dozens of US, UK, EU, Russian and Israeli companies can be added.



The development of Quantum computing manufacturers © Yole Quantum Technologies 2021. Market and Technology Report.

The problem with the GAFAM and their Asiatic competitors will hence remain, for every type of small, medium or big business under the corporations. The simple question remaining *"can you trust them even if you pay for their products?"*. The huge concerns raised all over the EU after the release, last February, of the official Dutch Government report and March follow-ups on privacy failures in Microsoft's Teams, OneDrive Sharepoint and Azure AD, followed in June by the Swiss Data Protection Commissioner(1) confirms once again that the description of the attitudes and unfair behaviours of the GAFAM (and of their Asian counterparts) technically studied by Shoshana Zhuboff (2) and, philosophically, by Slavoj Zizek (3) are as actual as exact. Unless you are a US Government Institution like the NASA›s and the Pentagon›s secured sectors in Google›s quantic servers farm.

Privacy test on Microsoft Teams: be careful with the exchange and storage of confidential personal data

3 March 2022

The Dutch higher education sector and the Dutch government were recently advised not to discuss any (highly) sensitive information through the Microsoft Teams communication platform. This follows from a privacy test conducted by Privacy Company, commissioned by SURF and the Ministry of Justice and Security. If you work with (special categories of) personal data, read on to find out what this means for your work or studies.

The dedicated page advises students and researchers of the University of Amsterdam when using Teams

Advanced cyrptography as an alternative

NIST's last steering report redacted by N. Moha (4) reviewing the actual development phases of Advanced Encryption techniques in the optic of a future standardisation – a complete new version of the NIST 2001 Advanced Encryption Standard (AES) – will still require time, as there are many security issues in the *parametration and subsequent implementation* within the new research products submitted for an advanced analysis by more than 80 US companies.

Meanwhile, the hugest cybercrime groups are not waiting and almost all products on the market can be hacked, as it has been recently shown (5). Everything depends only on how much do you want to invest, in function of the encryption level and tools used by the company interesting you, in this (illegal) *"pay-per-service"* set of offers.

The MTE® quantum secure data, as referenced by Marco Essomba in Cybersecurity Trends (Issue 1:2022) surely provides one of the best alternatives. However, if not dealt by the best specialist and if you do not consider each token technique it has a very short lifespan before becoming "hackable".

So... which will be the possible new paths in advanced cryptography? The wheel does not need to

Main types of attacks against encryption, excluding human factor-linked ones © Krademy

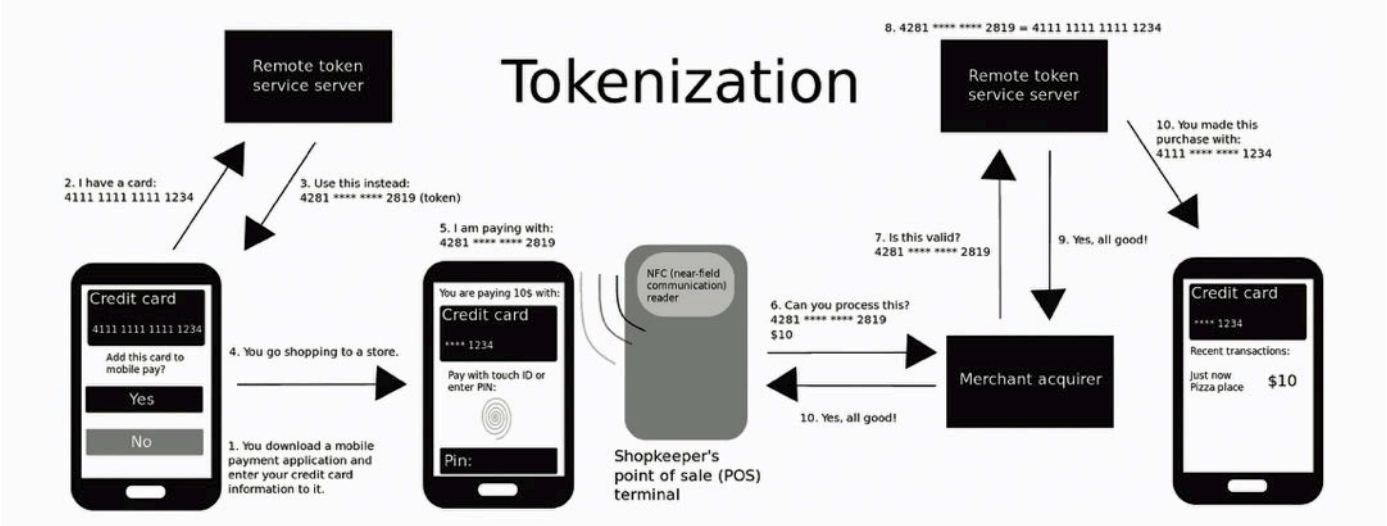
be reinvented every year, and the best security companies have had it for decades. Becoming more and more transdisciplinary led them to try, sometimes very successfully, to apply concepts already present in Greek philosophy, Renaissance researches and, most often, in the technical achievements made for other sciences during the *"siècle des lumières"*, the 19th century.

The latter period was exactly the time when Max Karl Ernst Ludwig Planck invented the term *quanta* for explaining the mystery of the discrete units exchanged by an electromagnetic radiation when interacting with matter, giving birth to the proportionality constant, h, named "Planck constant", the very base of the old *quantum theory*.

Among the richness of the 19th century discoveries, two of them nowadays are providing very interesting application capacities for next-gen encryption systems or simply to grow drastically with the resilience of the advanced encryption systems available now and in the nearest future.

Entropy theory applied to cryptography

Entropy, a term created in 1867 by the German physicist Rudolf Julius Emanuel Clausius by from the Ancient Greek word τροπή, designating "transformation". It constitutes is the central point of Clausius' second law of thermodynamics which states that the entropy of isolated



systems left to spontaneous evolution cannot decrease with time as they always arrive at a state of thermodynamic equilibrium where the entropy is highest (7).

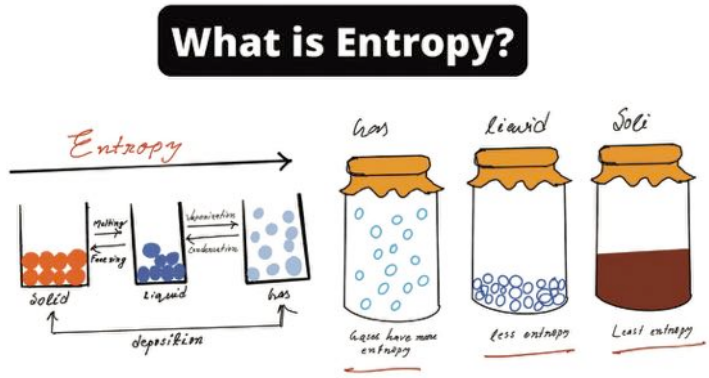
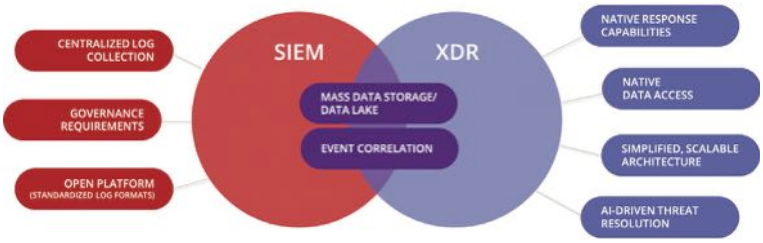
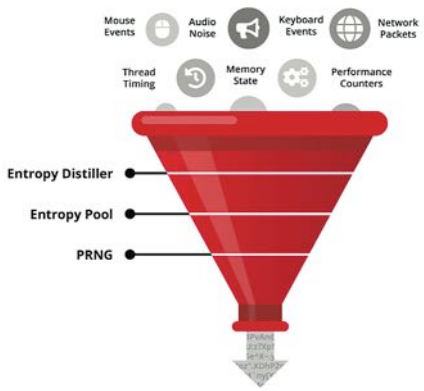


Image © microbiologynote.com

Without the users knowing it, entropy theory is one of the fundamental concepts used to build the newest automated defence systems known as XDR (Extended Detection and Response), adding to a company's defensive tools what is branded at the moment as the "ultimate layer" to protect a company and its automation strategy and proposed as a product by all IT and cybersecurity majors.



It is also one of the very bases of cryptography, as perfectly articulated by Edgar and Manz (8): *"Entropy is the foundation upon which all cryptographic functions operate. Entropy, in cyber security, is a measure of the randomness or diversity of a data-generating function. Data with full entropy is completely random and no meaningful patterns can be found".* Almost every month, new developments on entropy uses in random are published, some of them explaining perfectly the mechanism, as in the PKWare synthetic report (9) or the recent Crypto4A blog page (10).



Pseudo-random output stream based on «true» random key
© Cypto4A blog

BIO

With a PhD in Roman Archaeology obtained at the University of Lausanne, a Postdoctoral Research Degree in History and Sociology at the Romanian Academy of Sciences, and an EU Habilitation to direct PhDs in History and related sciences, Laurent Chrzanovski is Professor at the doctoral School of the Sibiu State University and holds postdoctoral courses within several major EU Universities. He is the author/editor of 32 books, of more than 150 scientific articles and of as many general-public articles. In the frame of cybersecurity, Laurent Chrzanovski is member and contractual consultant of the ITU roster of experts. He founded and manages the yearly "Cybersecurity Dialogues" PPP Congresses (Romania, Italy, Switzerland), organized in partnership with the highest international and national authorities . In the same spirit and with the same partnerships, he is co-founder and redactor-in-chief of the first cyber security awareness quarterly journal, Cybersecurity Trends, published in Romanian language since 2015, with English and in Italian versions since 2017. His main domains of study are focused on the relationship between the human behaviours and the digital world as well as the assurance of finding the right balance between security and privacy for the e-citizens.

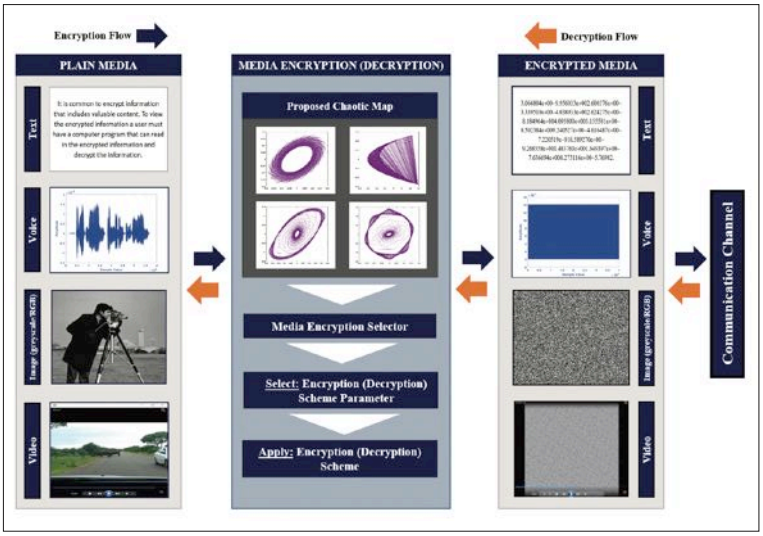
Chaos theory applied to cryptography

One of the "fathers" of chaos theory is Henri Poincaré. In the 1880s, while studying the three-body problem, he found that there can be orbits that are non-periodic, and yet not forever increasing nor approaching a fixed point (11).

Turbulence in the tip vortex from an airplane wing. Studies of the critical point beyond which a system creates turbulence are an important key for chaos theory.
Image © NASA, Langley Research Center of the United States, Creative Commons.

Yet scholars debated until the 1970s to better define a complete theory and its application, mainly in the fields of electronics, early computing patterns, weather and geology and economics.

From a computer science perspective, one should start recalling the need for feedback and control (hence the emergence of command and control) as a solution to avoid high chaotic movements. Yet besides avoiding chaos, in the past few decades, chaos theory has been used for many years in cryptography, mainly with disappointing results due to easily predictable patterns like binary ones or imitations of the human DNA chain (12). Yet, during the last five years, it came back massively, as a consequence of a huge number of IT researchers proposing new approaches and schemes which are extremely promising for their innovation aspects as well as for their reliability, at least in their testing phases (13) (14), and this works for text, voice and multimedia contents (15).



Schematic structure of the encryption and decryption processes of the proposed pipeline © Yasser et al. 2020, fig. 1, p. 4

What shall we do?

No matter which encryption you will decide to use. At the end of the day, we will recall one of the recurring themes punctuating the debates held during the 1st yearly edition of *"Cyber Espionage Awareness Day for Business"* (Bucharest, June 14th). There, all public and private specialists repeated four essential and simple hygiene rules:

1. ***Reduce the amount of data generated by your company*** (reports witnessed a factor 10 multiplication of data produced daily, during the last 5 years, per company, most not having witnessed a growth on the number of clients, suppliers, employees, cash-flow or market share).
2. ***Reduce the amount of data shared or sent.***
3. ***Prevent the human factor:*** your data may be safe after encryption, but before that and, mostly after decryption by the receiver, they are extremely vulnerable while the human factor has been the key of the success of more than 80% of the attacks.
4. ***Be aware of spywares:*** for cyber criminals and their clients, it is way easier to spy employees and staff than to use brute force against a company. The multiplication of zero-click spywares for voice, data storage, transmissions is enormous and the range of their capacities is well explained by their price : from $2.5 million (military-grade, zero-click, almost undetectable) to $100,000 (one click needed) or much less (detectable if you have the appropriate tools). ■

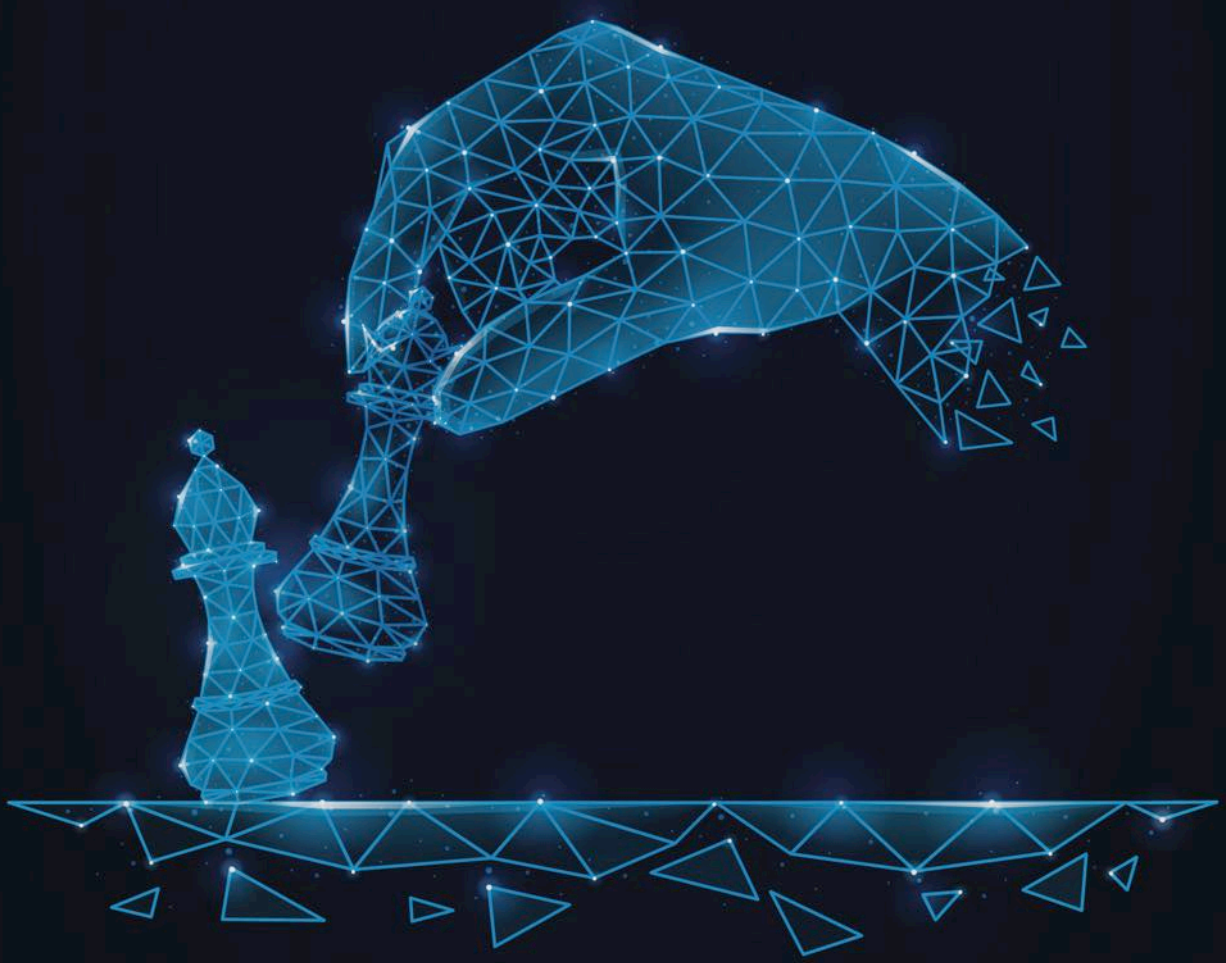
* We would like to thank Mauro Vignati, Lecturer at the Università della Svizzera Italiana and former head of the Cyber Section of the Swiss Federal Police, for his valuable advice and careful control of our text.

(1) See Dutch Government (2022), DPIA on Microsoft Teams, OneDrive Sharepoint and Azure AD (June 2021) Data protection impact assessment on the processing of Diagnostic Data Version 1.1., Public Version, 16 February 2022, Dutch Ministry of Justice and Security, Strategic Vendor Management Microsoft, Google and AWS (SLM Rijk) and SURF, The Hague (https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad)
See recent updates on the University of Amsterdam website: "Privacy test on Microsoft Teams: be careful with the exchange and storage of confidential personal data"
(https://student.uva.nl/en/content/news/2022/03/privacy-test-on-microsoft-teams-be-careful-with-the-exchange-and-storage-of-confidential-personal-data.html?cb)
For the Swiss report, see: "13.06.2022 Outsourcing of personal data to a Microsoft cloud by Suva (the Swiss National Accident Insurance Fund, n.d.r) - Due to partly conflicting legal concepts, the FDPIC advises Suva to re-evaluate the outsourcing of personal data to a cloud operated by the US group Microsoft.» https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html
(2) Shoshana Zhuboff (2019), The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power, Profile Books Ltd, London / Public Affairs, New York
(3) Slavoj Zizek (2019), Like a thief in broad daylight. Power in the Era of Post-Humanity, London, Penguin
(4) Mouha N. (2021), Review of the Advanced Encryption Standard (NISTIR 8319), NIST 2021 (https://doi.org/10.6028/NIST.IR.8319)
(5) Hazhirpasand M., Ghafari M. (2021), Cryptography Vulnerabilities on HackerOne, in : The 21st IEEE International Conference on Software Quality, Reliability and Security (QRS), pp. 18-27 (doi: 10.1109/QRS54544.2021.00013)
(6) see the synthesis of the problematic in Malviya G. (2021), What is a Token? What are its Pros and Cons?, Loginradius Blog, 21.08.2021 (https://www.loginradius.com/blog/identity/pros-cons-token-authentication/)
(7) Clausius, R. (1867), The Mechanical Theory of Heat – with its Applications to the Steam Engine and to Physical Properties of Bodies. London: John van Voorst.
(8) Edgar T.W., Manz D.O. (2017), Chapter 2 - Science and Cyber Security, in Edgar T.W., Manz D.O. (eds.) Research Methods for Cyber Security, Syngress, pp. 33-62 (doi.org/10.1016/B978-0-12-805349-2.00002-9)
(9) PKWare (2018), The Entropy Problem. Random Data and Secure Cryptography, PKWare White Paper
(10) Crypto4A (2021) Why We Need Entropy in Cybersecurity, Crypto4A blog, May 10, 2021 (https://crypto4a.com/blog/why-we-need-entropy-in-cybersecurity/)
(11) Poincaré J.H. (2017), The three-body problem and the equations of dynamics : Poincaré's foundational work on dynamical systems theory. Popp Bruce D. (Translator). Cham: Springer International Publishing, 2017
(12) Kocarev L. (2001), Chaos-based cryptography: A brief overview, in IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6-21, 2001 (doi: 10.1109/7384.963463)
(13) Amer Sharif et al. (2021), Chaos-based Cryptography: A Brief Look Into An Alternate Approach to Data Security, in: Journal of Physics: Conference Series 1566, 2020 (doi:10.1088/1742-6596/1566/1/012110)
14) Qiao Z. (2021), Nonlinear dynamics, applications to chaos-based encryption, Cryptography and Security, École centrale de Nantes, 188 p. (https://hal.archives-ouvertes.fr/tel-03200707)
15) Yasser et al. (2020), A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications, in Entropy 2020:22, 1253 (https://doi.org/10.3390/e22111253)

BLOCKAPT™

A centrally managed **COMMAND** & **CONTROL**
single platform experience.

Eliminate the weakest link.



info@blockapt.com

blockapt.com

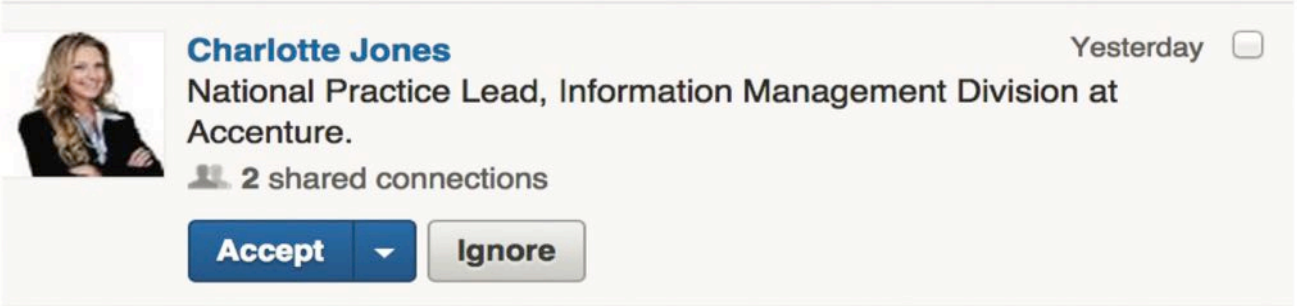
Hello Charlotte! An example of social engineering on LinkedIn.

Author: Battista Cagnoni

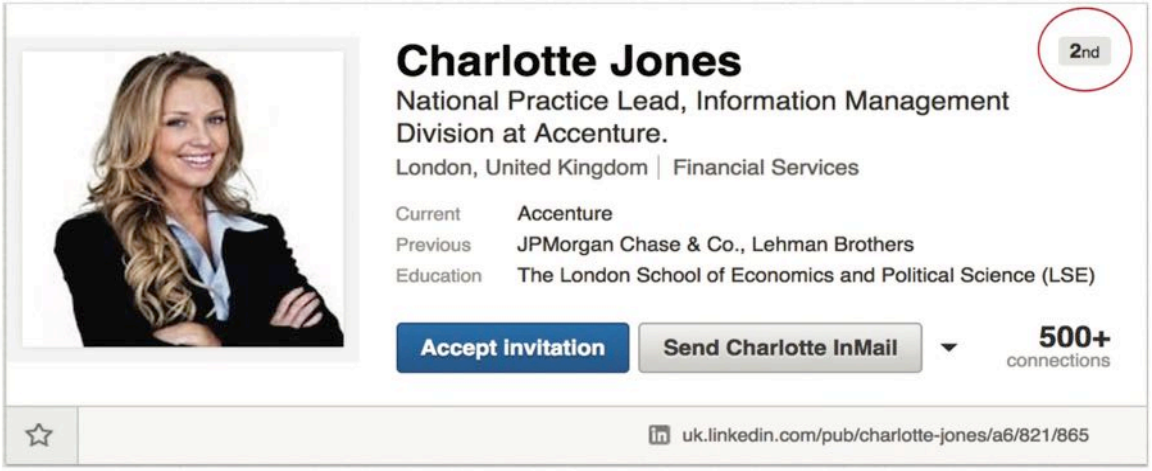
"Charlotte" is one of many cases, which was the subject of a small investigation I carried out recently.

Everything starts from the image, because of its strong emotional component. The example we are looking at here is a real case: Charlotte, a beautiful smiling blonde woman, who asked me to join my Linkedin circle, a second level invitation, i.e. someone in my network of contacts accepted Charlotte, which "in principle" would mean that they know her.

So I get an email from Charlotte via Linkedin, asking me to connect with her and I look at her profile, which is impressive. Rich in skills and professional experience. There seems to be nothing suspicious in her curriculum, which makes it easy to accept her into my circle of contacts.



Charlotte is in my network



Experience

National Practice Lead, Information Management Division.
Accenture
October 2014 – Present (1 month) I London, United Kingdom

Accenture plc is a multinational management consulting, technology services, and outsourcing company. Its incorporated headquarters are in Dublin, Republic of Ireland. It is the world's largest consulting firm as measured by revenue and is a Fortune Global 500 company. As of 2014, the company reported net revenues of $30.0 billion with approximately 305,000 employees, serving clients in more than 200 cities in 56 countries. Accenture has more employees in India than any other country; in the US, it has about 40,000 employees and 35,000 located in the Philippines. Accenture's current clients include 96 of the Fortune Global 100 and more than three-quarters of the Fortune Global 500. Since September 1, 2009 the company has been incorporated in Ireland.

Director, Enterprise Technology
JPMorgan Chase & Co.
September 2011 – September 2014 (3 years 1 month) I London, United Kingdom

JPMorgan Chase is a global investment bank with expertise in mergers and acquisitions, capital markets, financial restructuring, and valuation.

As strategist and enterprise architect, defining and advancing technology vision of enterprise systems aligned with the firm's vision for growth and service innovation, supporting entire investment banking business of Corporate Finance, Financial Restructuring, Financial Advisory Services, Capital Markets, Private Equity / Financial Sponsors Coverage and corporate departments. Constructed business case for various sized technology investments and highly successful selling concepts and solutions to business and IT.

Supported application landscape of CRM, ERP, data warehouse, web sites & applications, document management, collaboration portal, SaaS, and industry data services. Responsible for technology fit assessment, selection and execution of new technologies. Chief evangelist on enterprise CRM to accelerate conversion of prospects to clients, contacts to relationships to closed deals. Constructed Workday user stories to articulate value of streamlined investment bank talent management. Executed quick pilots / proof of concepts (POC) to introduce new technology as IT capability. Product manager of Salesforce.com, leading cross functional team in business process streamlining and technology platform implementation.

Business Intelligence Lead, Financial Planning & Analysis
Lehman Brothers
January 2006 – March 2008 (2 years 3 months) I London, United Kingdom

Lead advisor in FP&A supporting executive decision making process with data, metrics and analytics of Lehman Brothers' mortgage banking statistics and capital market trends. Managed team of data analysts and programmer analysts, responsible for corporate finance data architecture, data analysis, financial reporting, management reporting, systems integration and scorecard / dashboard design and development. Established data management best practices in taxonomy, data cleansing, migration and governance. Designed and implemented data marts to facilitate budget, forecast and metrics driven reporting and analysis. Developed integration to Cognos Planning and Hyperion / Essbase monthly consolidation and closing process.

Summary

I bring common sense and a human touch to enterprise problem solving. My passion intersects market, industry, business, customer and technology. I speak expressively across these disciplines, advising clients on strategic vision of user centric technology and organizational behavior change.

I'm passionate about boosting competitiveness and value creation enabled by technology, cultivating trust based relationships, creating win win opportunities and giving back to community.

Specialties:
• IT Strategy, technology enablement, enterprise architecture, cross functional change leadership, strategic transformation
• Consultative sales & marketing, business / alliance / partnership development
• M&A due diligence, management consulting, technology competitive analysis
• Financial services vertical - investment banking, mortgage banking, capital markets - front office, across business lines, and with regulators
• Enterprise software / solutions, product management, user experience
• Platform / service architecture, governance, outsourcing, program management, agile delivery
• SaaS, business intelligence / analytics, ERP, CRM, content management, collaboration
• Building high performance / virtual / global teams, developing capability, teaching / coaching

Lately my interest is CRM / marketing automation, data and analytics, content management, business development and financial services marketing. I enjoy product ideation and evaluate software from small niche companies.

Connect with me @ jonescharlotte947@gmail.com

Developer / Database Architect
Lehman Brothers
November 2003 – January 2006 (2 years 3 months) I London, United Kingdom

Architecture and design of large transactional databases, financial data marts, data warehouse, integration to Cognos Planning and enterprise/financial reporting of the origination and servicing businesses of Lehman Brothers Mortgage Capital, supporting field operations and corporate functions in finance, accounting, treasury, legal, compliance, risk management and Lehman Brothers corporate finance.

Volunteer Experience & Causes

Opportunities Charlotte is looking for:
• Joining a nonprofit board

Languages

French (fluent) Spanish (basic)
Germany (basic)

Education

The London School of Economics and Political Science (LSE)
2000 – 2003

Additional Info

Interests
Fiction, International Affairs, Opera, Horseriding, Fine Food

Cor dos cabelos e bronzeado fazem mulheres sentirem-se ...
www.portalrcr.com.br/.../45878-cor-dos-c... ▾ Oversæt denne side
574 × 430 - 01/11/2012 - Longos **cabelos** loiros, bronzeado e unhas tipo francesinha. Assim as mulheres sentem-se atraentes, segundo pesquisa realizada pela rede ...

Cor dos cabelos e bronzeado fazem mulheres sentirem-se ...
www.portalrcr.com.br/.../45878-cor-dos-c... ▾ Oversæt denne side
574 × 430 - 01/11/2012 - Longos **cabelos** loiros, bronzeado e unhas tipo francesinha. Assim as mulheres sentem-se atraentes, segundo pesquisa realizada pela rede ...

Cor dos cabelos e bronzeado fazem mulheres sentirem-se ...
www.portalrcr.com.br/.../45878-cor-dos-c... ▾ Oversæt denne side
574 × 430 - 01/11/2012 - Longos **cabelos** loiros, bronzeado e unhas tipo francesinha. Assim as mulheres sentem-se atraentes, segundo pesquisa realizada pela rede ...

Aprenda simpatias para crescer na profissão - Terra Brasil
vidaeestilo.terra.com.br/.../aprenda-simpat... ▾ Oversæt denne side
407 × 305 - 09/09/2013 - Beleza · **Cabelos** e Salão · **Cabelo** do dia · Dicas Profissionais · Faça você mesma · Quero esse **cabelo** · Tratamento e tintura · Salão em Casa.

Cor dos cabelos fazem mulheres sentirem-se atraentes; veja
www.meionorte.com/.../cor-dos-cabelos-e... ▾ Oversæt denne side
600 × 449 - 27/10/2012 - Longos **cabelos** loiros, bronzeado e unhas tipo francesinha. Assim as mulheres sentem-se atraentes, segundo pesquisa realizada pela rede ...

Professional Image | The Work at Home Woman
www.theworkathomewoman.com/.../profe... ▾ Oversæt denne side
507 × 338 - How to Dress for an Interview – Styling Tips for Women. Tags: Business ... A smart and professional image will say that you are a smart and **professional woman**.

How to Dress for Success - The Work at Home Woman
www.theworkathomewoman.com/dress-fo... ▾ Oversæt denne side
507 × 338 - How to Dress for an Interview – Styling Tips for Women. Tags: Business ... A smart and professional image will say that you are a smart and **professional woman**.

Job Seekers | The Work at Home Woman
www.theworkathomewoman.com/.../job-s... ▾ Oversæt denne side
507 × 338 - Upcoming Events for Entrepreneurial Women, Career Bloggers and Job Seekers ... professional image will say that you are a smart and **professional woman**.

Woman | The Work at Home Woman
www.theworkathomewoman.com/.../wom... ▾ Oversæt denne side
507 × 338 - How to Dress for an Interview – Styling Tips for Women. Tags: Business ... A smart and professional image will say that you are a smart and **professional woman**.

Michaela Quinn | The Work at Home Woman
www.theworkathomewoman.com/.../mich... ▾ Oversæt denne side
507 × 338 - How to Dress for an Interview – Styling Tips for Women. Tags: Business ... A smart and professional image will say that you are a smart and

As a potential "victim" but with knowledge of social network security, I immediately observe that the profile is almost too rich, almost too good to be real. One detail attracts my attention: this profile, so perfect, is not completed by any recommendation, neither written, nor on the list of precise skills.

I therefore wonder whether or not this profile corresponds to a real person or whether it is a profile created expressly to carry out social engineering operations. In other words, to gain the trust of the victims, primarily to encourage them, once the invitation has been accepted, not to question the future emails that "Charlotte" will send them, and especially to click on the links that she will recommend.

The first step in my role as an investigator is very simple: I insert Charlotte's photo into the Google image search engine. And there, first surprise: the photo of "Charlotte" appears on many sites, some Brazilian, others English, offering all kinds of services for women who want to succeed.

Woman

Thursday, November 1, 2012 - 21h44

Hair color and tan make women feel attractive

A- The +

Long blond hair, tan and nails French girl type. So women feel attractive, according to a survey by the British chain of beauty product stores, Superdrug. The information is the site Female First.

The image was therefore carefully chosen for its purely emotional character, to specifically target men: a beautiful, blonde, young woman, to whom several elements were added in the LinkedIn profile highlighting her intelligence and multiple talents, which are reflected in her undeniable professional success, according to the curriculum posted online.

Still using Google, I copy parts of this curriculum, putting them in inverted commas.

Experience

National Practice Lead, Information Management Division.
Accenture
October 2014 – Present (1 month) | London, United Kingdom

Accenture plc is a multinational management consulting, technology services, and outsourcing company. Its incorporated headquarters are in Dublin, Republic of Ireland. It is the world's largest consulting firm as measured by revenue and is a Fortune Global 500 company. As of 2014, the company reported net revenues of $30.0 billion with approximately 305,000 employees, serving clients in more than 200 cities in 56 countries. Accenture has more employees in India than any other country; in the US, it has about 40,000 employees and 35,000 located in the Philippines. Accenture's current clients include 96 of the Fortune Global 100 and more than three-quarters of the Fortune Global 500. Since September 1, 2009 the company has been incorporated in Ireland.

Google "Accenture plc is a multinational management consulting, technology ser

Director, Enterprise Technology
JPMorgan Chase & Co.
September 2011 – September 2014 (3 years 1 month) | London, United Kingdom

JPMorgan Chase is a global investment bank with expertise in mergers and acquisitions, capital markets, financial restructuring, and valuation.

As strategist and enterprise architect, defining and advancing technology vision of enterprise systems aligned with the firm's vision for growth and service innovation, supporting entire investment banking business of Corporate Finance, Financial Restructuring, Financial Advisory Services, Capital Markets, Private Equity / Financial Sponsors Coverage and corporate departments. Constructed business case for various sized technology investments and highly successful selling concepts and solutions to business and IT.

Google "As strategist and enterprise architect, defining and advancing"

Supported application landscape of CRM, ERP, data warehouse, web sites & applications, document management, collaboration portal, SaaS, and industry data services. Responsible for technology fit assessment, selection and execution of new technologies. Chief evangelist on enterprise CRM to accelerate conversion of prospects to clients, contacts to relationships to closed deals. Constructed Workday user stories to articulate value of streamlined investment bank talent management. Executed quick pilots / proof of concepts (POC) to introduce new technology as IT capability. Product manager of Salesforce.com, leading cross functional team in business process streamlining and technology platform implementation.

Business Intelligence Lead, Financial Planning & Analysis
Lehman Brothers
January 2006 – March 2008 (2 years 3 months) | London, United Kingdom

Lead advisor in FP&A supporting executive decision making process with data, metrics and analytics of Lehman Brothers' mortgage banking statistics and capital market trends. Managed team of data analysts and programmer analysts, responsible for corporate finance data architecture, data analysis, financial reporting, management reporting, systems integration and scorecard / dashboard design and development. Established data management best practices in taxonomy, data cleansing, migration and governance. Designed and implemented data marts to facilitate budget, forecast and metrics driven reporting and analysis. Developed integration to Cognos Planning and Hyperion / Essbase monthly consolidation and closing process.

Google "Lead advisor in FP&A supporting executive decision"

With three simple searches, I can see that "Charlotte" has borrowed existing phrases: from Wikipedia as regards the description of the company where she works, but especially from the profile of a certain Vivian Ying as regards professional background and skills.

Experience

National Practice Lead, Information Management Division.
Accenture
October 2014 – Present (1 month) | London, United Kingdom

Accenture plc is a multinational management consulting, technology services, and outsourcing company. Its incorporated headquarters are in Dublin, Republic of Ireland. It is the world's largest consulting firm as measured by revenue and is a Fortune Global 500 company. As of 2014, the company reported net revenues of $30.0 billion with approximately 305,000 employees, serving clients in more than 200 cities in 56 countries. Accenture has more employees in India than any other country; in the US, it has about 40,000 employees and 35,000 located in the Philippines. Accenture's current clients include 96 of the Fortune Global 100 and more than three-quarters of the Fortune Global 500. Since September 1, 2009 the company has been incorporated in Ireland.

Director, Enterprise Technology
JPMorgan Chase & Co.
September 2011 – September 2014 (3 years 1 month) | London, United Kingdom

JPMorgan Chase is a global investment bank with expertise in mergers and acquisitions, capital markets, financial restructuring, and valuation.

As strategist and enterprise architect, defining and advancing technology vision of enterprise systems aligned with the firm's vision for growth and service innovation, supporting entire investment banking business of Corporate Finance, Financial Restructuring, Financial Advisory Services, Capital Markets, Private Equity / Financial Sponsors Coverage and corporate departments. Constructed business case for various sized technology investments and highly successful selling concepts and solutions to business and IT.

Supported application landscape of CRM, ERP, data warehouse, web sites & applications, document management, collaboration portal, SaaS, and industry data services. Responsible for technology fit assessment, selection and execution of new technologies. Chief evangelist on enterprise CRM to accelerate conversion of prospects to clients, contacts to relationships to closed deals. Constructed Workday user stories to articulate value of streamlined investment bank talent management. Executed quick pilots / proof of concepts (POC) to introduce new technology as IT capability. Product manager of Salesforce.com, leading cross functional team in business process streamlining and technology platform implementation.

Business Intelligence Lead, Financial Planning & Analysis
Lehman Brothers
January 2006 – March 2008 (2 years 3 months) | London, United Kingdom

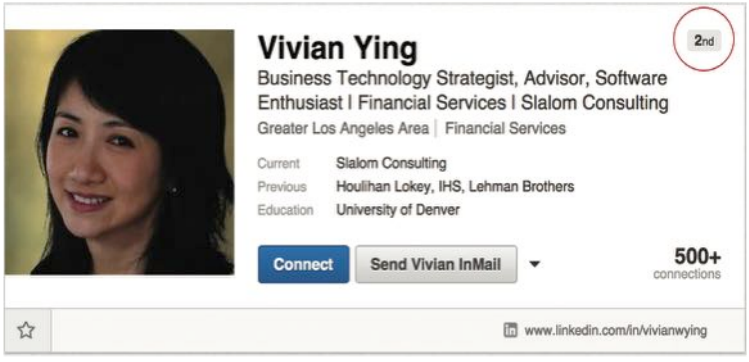
Lead advisor in FP&A supporting executive decision making process with data, metrics and analytics of Lehman Brothers' mortgage banking statistics and capital market trends. Managed team of data analysts and programmer analysts, responsible for corporate finance data architecture, data analysis, financial reporting, management reporting, systems integration and scorecard / dashboard design and development. Established data management best practices in taxonomy, data cleansing, migration and governance. Designed and implemented data marts to facilitate budget, forecast and metrics driven reporting and analysis. Developed integration to Cognos Planning and Hyperion / Essbase monthly consolidation and closing process.

Accenture - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Accenture ▾ Oversæt denne side
Accenture plc is a multinational management consulting, technology services, and outsourcing company. Its incorporated headquarters are in Dublin, Republic ...
Pierre Nanterme - HealthCare.gov - Accenture top 50 business ... - Consulting firm

Vivian Ying | LinkedIn
www.linkedin.com/in/vivianwying ▾ Oversæt denne side
Greater Los Angeles Area - Business Technology Strategist, Advisor | Financial Services | Slalom Consulting
As strategist and enterprise architect, defining and advancing technology vision of enterprise systems aligned with the firm's vision for growth and service ...

Vivian Ying | LinkedIn
www.linkedin.com/in/vivianwying ▾ Oversæt denne side
Greater Los Angeles Area - Business Technology Strategist, Advisor | Financial Services | Slalom Consulting
Lead advisor in FP&A supporting executive decision making process with data, metrics and analytics of Lehman Brothers' mortgage banking statistics and ...

The question now is whether Charlotte or Vivian is a real person. I then look at Vivian's profile. I first discover that Vivian's profile is already in my network, which implies that those who created Charlotte have researched the people in my extended professional circle, to better study the common interests that link me to them.



Charlotte's CV is identical to Vivian's! Only the last line, which includes the email address, has changed.

• Charlotte

Summary

I bring common sense and a human touch to enterprise problem solving. My passion intersects market, industry, business, customer and technology. I speak expressively across these disciplines, advising clients on strategic vision of user centric technology and organizational behavior change.

I'm passionate about boosting competitiveness and value creation enabled by technology, cultivating trust based relationships, creating win win opportunities and giving back to community.

Specialties:
• IT Strategy, technology enablement, enterprise architecture, cross functional change leadership, strategic transformation
• Consultative sales & marketing, business / alliance / partnership development
• M&A due diligence, management consulting, technology competitive analysis
• Financial services vertical - investment banking, mortgage banking, capital markets - front office, across business lines, and with regulators
• Enterprise software / solutions, product management, user experience
• Platform / service architecture, governance, outsourcing, program management, agile delivery
• SaaS, business intelligence / analytics, ERP, CRM, content management, collaboration
• Building high performance / virtual / global teams, developing capability, teaching / coaching

Lately my interest is CRM / marketing automation, data and analytics, content management, business development and financial services marketing. I enjoy product ideation and evaluate software from small niche companies.

Connect with me @ jonescharlotte947@gmail.com

• Vivian

Summary

I bring common sense and a human touch to enterprise problem solving. My passion intersects market, industry, business, customer and technology. I speak expressively across these disciplines, advising clients on strategic vision of user centric technology and organizational behavior change.

I'm passionate about boosting competitiveness and value creation enabled by technology, cultivating trust based relationships, creating win win opportunities and giving back to community.

Specialties:
• IT Strategy, technology enablement, enterprise architecture, cross functional change leadership, strategic transformation
• Consultative sales & marketing, business / alliance / partnership development
• M&A due diligence, management consulting, technology competitive analysis
• Financial services vertical - investment banking, mortgage banking, capital markets - front office, across business lines, and with regulators
• Enterprise software / solutions, product management, user experience
• Platform / service architecture, governance, outsourcing, program management, agile delivery
• SaaS, business intelligence / analytics, ERP, CRM, content management, collaboration
• Building high performance / virtual / global teams, developing capability, teaching / coaching

Lately my interest is CRM / marketing automation, data and analytics, content management, business development and financial services marketing. I enjoy product ideation and evaluate software from small niche companies.

Connect with me - viviany at slalom.com (email), @vivianwying (Twitter).

BIO

Battista Cagnoni, Senior Consultant, Advisory Services, EMEA at Vectra, is a security expert with a long experience in different areas of the industry, where he has held positions as Security Engineer, Security Analyst or SOC Lead. He is passionate about cyber security culture, awareness and understanding of methodologies to deal with security issues. He is constantly sharing his knowledge, offering advice and processes at the highest level, helping CISOs who are thinking about how to strengthen and achieve a high degree of maturity in security operations. Battista holds the GIAC Forensic Analyst and Incident Handler certifications as well as the CISSP, GCFA, GCIH Expert certificates.

To better understand the details of 'Charlotte's trap', let's now compare the two profiles. We have determined that "Charlotte" has a profile consisting of a fake photo, a copied background and a completely plagiarised CV. In addition, there are some spelling mistakes, the descriptions of her current job are very generic and she is, remember, not recommended by anyone. Vivian, on the other hand, has a real photo, is active on twitter, has dozens of recommendations and, above all, has a professional history that is confirmed by the information provided on the websites of the companies where she works and has worked in the past.

Who is real?

Charlotte	Vivian
■ "Cheated" with her profile picture	■ Seems to be a real picture
■ Spelling mistakes	■ She is active on twitter
■ Generic description of her current work	■ She has endorsements and recommendations
■ No endorsements or recommendations	■ She has a searchable work history which matches her LinkedIn profile

Once we have definitively established beyond doubt that Charlotte is not a real person, we obviously refuse her application to join our network.

Why are there so many "Charlottes" on Linkedin? There are several complementary reasons. On this site, which is intended for professional exchanges, those who hide behind "Charlottes" do so, at best, to discover the victim's skills and resell them to recruiters or company headhunters. But often, these attackers use this method to collect information and especially the victim's contact list in order to send them spam with increasingly dangerous content without arousing suspicion, or to *profile* potential targets for specific attacks, for example in the victim's internal professional circle of contacts in his own company.

In conclusion, it is important to be increasingly vigilant when connecting on social networks. The best thing to do when receiving an invitation from a stranger is to do the simple research we explained above *("sanity checking")* to check that the person is real. Don't forget that you can always ask the person inviting you why they want to meet you: this is one of the best methods, as *scammers* never reply. Finally, as a precautionary measure, do not accept any invitation from people you do not know and who have profiles that are too "generic". ■

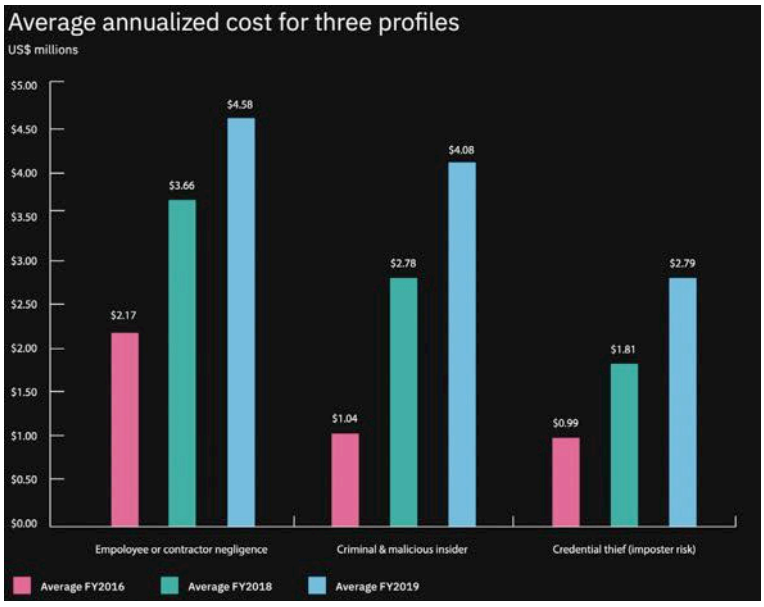
Goodbye complacency. Be alert for insider threats.

Author: Raj Meghani

Welcome to the world of Insider Threats which between 2018 – 2020 saw a 47% increase in the frequency of incidents involving Insider Threats, including malicious data infiltration and accidental data loss, according to a Tessian article. Today, Verizon's report is suggesting that Insiders are responsible for up to 22% of all security incidents.

An Insider Threat does not mean it only resides from employees inside the organisation.

How many of us operating in all different working environments have hired suppliers, contractors, had disgruntled employees leave the business, etc? Now think back to that time and remember what they had access to, who they had access to, and it all starts to get a little blurry.



The constant growth of insider threats and their costs © Ponemon Institute, 2020

That's nearly 1 in 5 of all security incidents. That's something which leaves no room for complacency. That's why Insider Threats need to be taken seriously by raising awareness and putting in place steps to mitigate against those malicious sitting insiders biding their time.

So how does an organisation prevent Insider Threats? The simple answer is to lock down **ALL** your sensitive data which is likely to be targeted and infiltrated to only a few select people who have access. However, in today's complex world where roles are evolving, companies are merging or being acquired, customers have more and more channels to communicate with organisations and so the list goes on, the ease for insiders to remain virtual and faceless gives them a head start.

BIO

Raj Meghani is Co-Founder & Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, UK based innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience.Raj has also been appointed as a Non-Executive Director to the Board of Money Matters Bank. Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 25 years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans. Raj is Editor for Cybersecurity Trends UK which has a global presence and is active in thought leadership and knowledge transfer of cybersecurity and business risk management.
LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/
Twitter: https://twitter.com/blockapt
Company website: https://www.blockapt.com

Trust or Zero Trust plays a key role here – implementation of a Zero Trust policy with restricted Privilege Access Management to sensitive data and assets also has a role to play here.

We've seen how easy it is to get intuitive information through corporate espionage in Jack Schafer and Marvin Karlins brilliant article: "Hacked by bits and pieces – what we can learn from an example of corporate espionage". There is no silver bullet when it comes to dealing with and preventing Insider Threats. Why? Because to do so, you would need to have full visibility across all your incoming, outgoing and stored/archived data and have detailed knowledge on who has access to it – or had access to it in the past. It's a minefield.

"Don't let IT beat you – adopt an impenetrable digital and physical presence which stops them bringing you down to your knees."

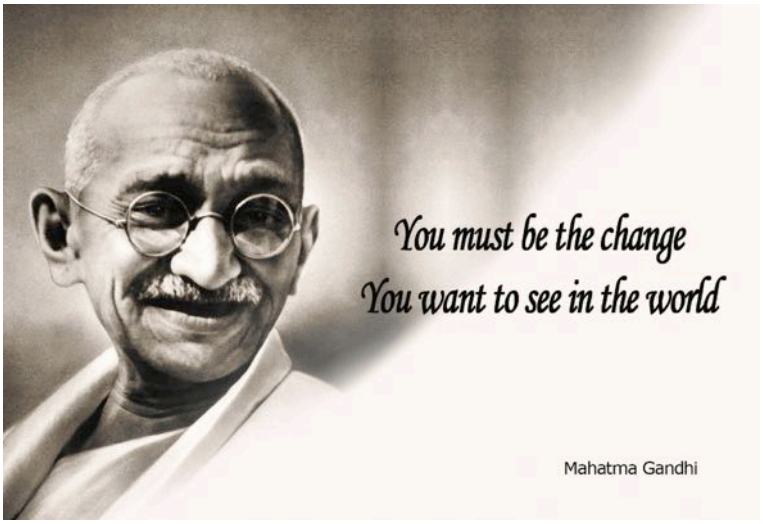
Raj Meghani.

The best way often comes down to the people themselves. Having the right level of cybersecurity training, awareness, security monitoring and management in place is paramount.

Let's take the hypothetical scenario of me working as a bank employee where I have access to customers details, accounts, etc. I can scrupulously leverage my access rights for malicious purposes which will ultimately give me a financial gain. The digital and behavioural warning signs will be there – if the bank security teams and other employees know what to look out for. I'll access and download large data file transfers which I've never had to carry out as part of my role, I'll spy on my 'colleagues' password credentials and manipulate multiple login attempts. Oh yes, I'll suddenly be working overtime too so I can make use of out of office, less busy hours or even better work remotely justifying a level of access to the bank's network. It's easy to bide my time and eventually get what I need because there's always cyber criminals out there willing to pay me for my data.

Having a security toolkit in place which through machine learning and AI can digitally monitor suspicious behaviour or activities, including but not limited to multiple failed login attempts can all help isolate insiders with a motive.

A lot of the time, improving email security to scan for suspicious content and attachments, having a robust password management policy with MFA, adding another security layer to your cloud infrastructure, etc can also help deal with targeted phishing attacks, data tampering, email negligence, etc.



I said before there is no silver bullet in dealing with Insider Threats – Mahatma Gandhi puts it simply eloquently and effectively *"You must be the change you want to see in the world"*. ■

Insider threats: profiling and detection.

Author: Battista Cagnoni

"It's all about trust" we could say. The majority of human activities and human interactions are based on trust. We trust who build and implemented the traffic light system. We cannot verify that when we see green on our way driving 80 km/h, everybody else has red and is not moving. Again we trust the restaurant' chef cooking our meal utilising good ingredients and nothing harmful for our health. We cannot break into the kitchen and personally inspect what's happening there. Inheritably we trust people in our organisation, we trust who we hire giving them access to confidential information and business critical Intellectual property.

BIO

Battista Cagnoni, Senior Consultant, Advisory Services, EMEA at Vectra, is a security expert with a long experience in different areas of the industry, where he has held positions as Security Engineer, Security Analyst or SOC Lead. He is passionate about cyber security culture, awareness and understanding of methodologies to deal with security issues. He is constantly sharing his knowledge, offering advice and processes at the highest level, helping CISOs who are thinking about how to strengthen and achieve a high degree of maturity in security operations. Battista holds the GIAC Forensic Analyst and Incident Handler certifications as well as the CISSP, GCFA, GCIH Expert certificates.

This represents a business risk which mature organisations know very well but finds it as one of the hardest problems to solve.

Security operations articulate their activities around people, process and technology and if having a good balance between the three components is true and necessary for external threats it's even more true and pushes to the limit the threat detection capabilities.

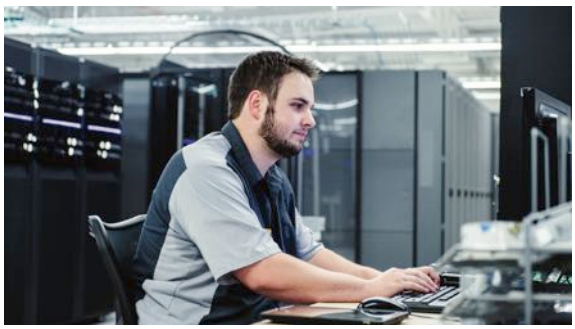
But who is an internal threat?

Based on the White Paper from Eric D. Shaw and Harley V. Stock[1] Some of the more interesting findings from the review include:

Insider IP thieves are more often in technical positions

The majority of IP theft is committed by current male employees averaging about 37 years of age who serve in mainly technical positions including engineers or scientists, managers, salespersons and programmers.

The majority of IP thieves had signed IP agreements, indicating that policy alone, without employee comprehension and effective enforcement, is ineffective.



Typically insider IP thieves already have a new job

About 65% of employees that commit insider IP theft had already accepted positions with a competing company or started their own company at the time of the theft. About 25% were recruited by an outsider who had targeted the data and about 20% of thefts involved collaboration with another insider.

Insider IP thieves most often steal what they have authorised access to

Subjects take the data they know, work with and often feel entitled to. In fact, 75% of insiders stole material they had authorised access to. This complicates an organisation's ability to protect their IP through technical controls and supports the need for more direct discussions with employees about what data is and is not transferrable upon their departure and should be an overt part of any employee IP agreement.

Trade secrets are most common IP type stolen by insiders

Trade secrets were stolen in 52% of cases. Business information such as billing information, price lists and other administrative data was stolen in 30%, source code 20%, proprietary software 14%, customer information 12%, and business plans 6%.

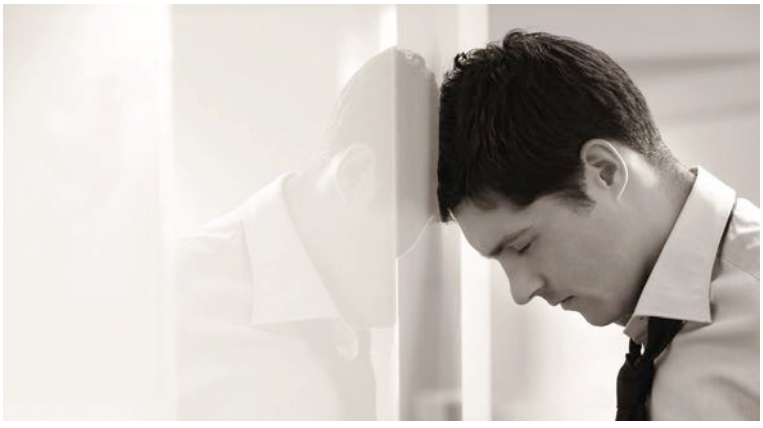
Insiders use technical means to steal IP, but they are discovered by non-technical employees

The majority of subjects 54% used a network—email, a remote network access channel or network file transfer to exfiltrate their stolen data. However, most insider IP theft was discovered by non-technical versus technical employees.

Professional setbacks can fast-track insiders considering stealing IP

Acceleration on the pathway to insider theft occurs when the employee gets tired of "thinking about it" and decides to take action or is solicited by others to do so.

This move often occurs on the heels of a perceived professional set-back or has not met his/her expectations. This demarcation from intention to



action, explains why some insider theft appears to be spontaneous, when it isn't.

At this point, having profiled who the typical insider threat is let's have a look at how to address this risk and possible mitigations. An interesting approach comes from CISA. In their website section dedicated to Infrastructure Security[2] we can find the description of the concept of People as Sensor.

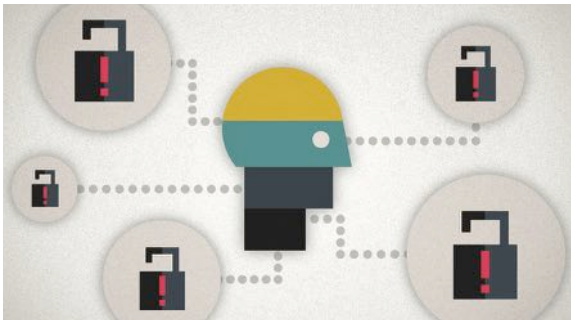
"An organization's personnel are the human component for the detection and identification of an insider threat. Co-workers, peers, friends, neighbors, family members, or casual observers are frequently positioned for insight into and awareness of predispositions, stressors, and behaviors of an insider who may be considering malicious acts. When observing human behavior, bear in mind two important qualities:

Listen through the other person's frame of reference, not your own. Do not assume that somebody will ask for help or ask to be stopped, or that they will talk about their intentions in the same way you would.

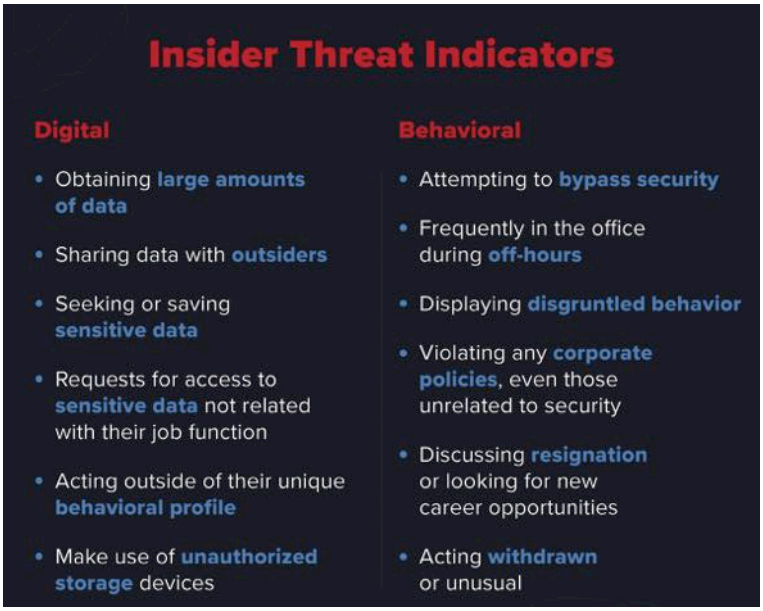
Listen to the other person with your eyes. People often disclose their intentions through non-verbal means."

There is also a series of indicators that is worth to mention as they give more context and details about where to look for Insider Threat signs.

- **Personal Indicators** are a combination of predisposition attributes and personal stressors currently impacting the insider.
- **Background Indicators** are events that happen before an individual is hired by an organisation or before an individual obtains network organisational access.
- **Behavioural Indicators** are actions directly observable by peers, HR personnel, supervisors, and technology. Over time, behaviours create a baseline of activities from which changes may be considered a threat indicator.
- **Technical Indicators** involve network and host activity and require direct application of IT systems and tools to detect.
- **Organisational/Environmental Indicators:**
  - Organisational policies and cultural practices can play a significant role in creating or managing an insider threat.
  - Environmental factors can escalate or mitigate stressors that may contribute to behavioural changes and an individual's progression from trusted insider to insider threat. These factors are often related to organisational policies and cultural practices.
- **Violence Indicators** are specific behaviours or collections of behaviours that can instill fear or generate a concern that a person might act upon these behaviours include, but are not limited to, intimidation, harassment, and bullying.

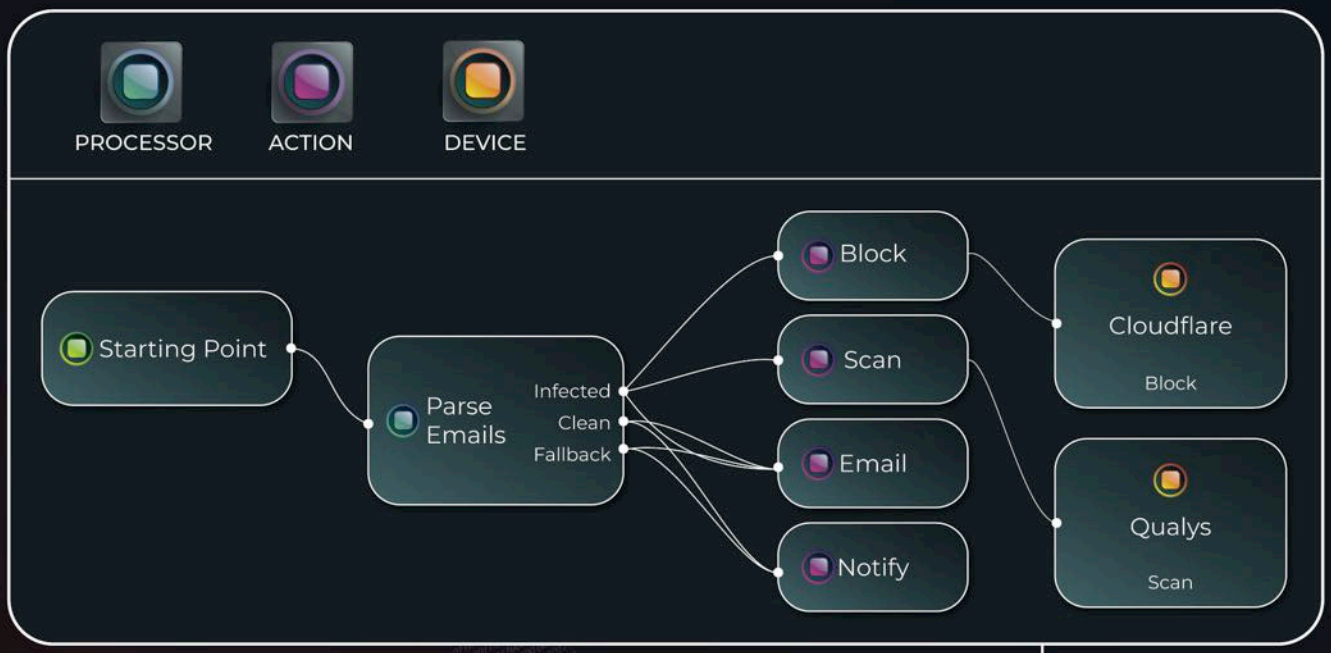


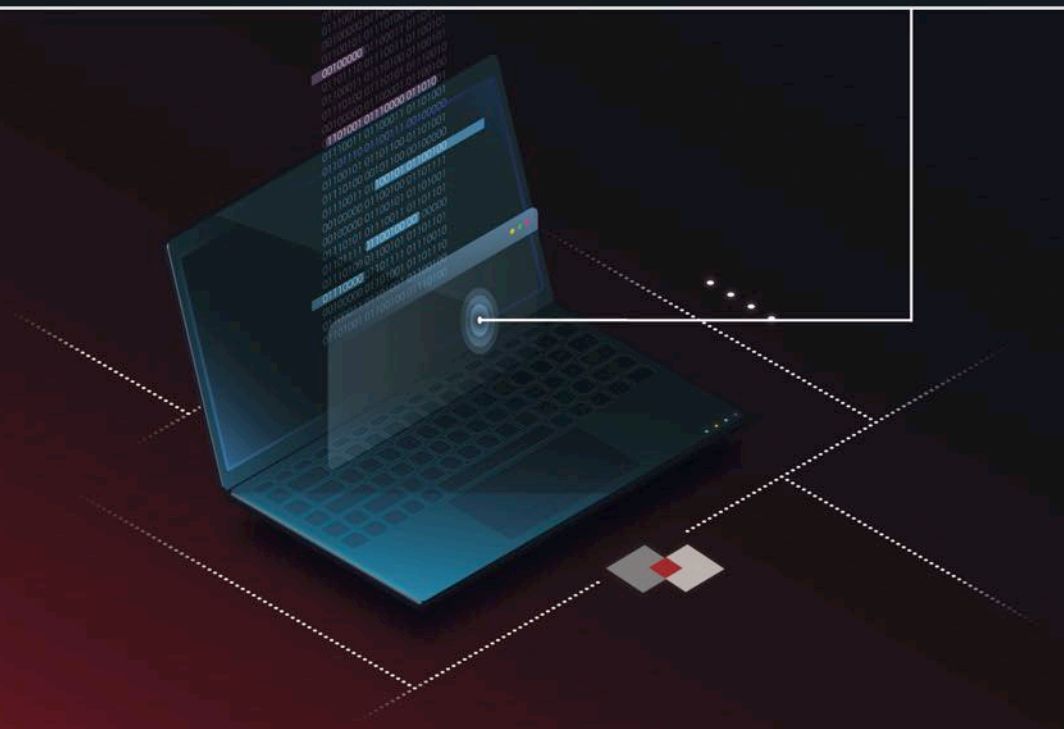
As a final consideration, it is important to mention that with the evolution of Artificial Intelligence technologies like Machine Learning it's possible to combine the behavioural approach with technical artefacts like network or host metadata. This allows the detection process to get faster by orders of magnitude. No matter if it's a Smash and Grab or a slow bleeding type of behaviour, AI will be able to generate useful indicators out of the network's noise. Also combining different type of indicators can add value and improve the posture against Insider Threats. One example that I've seen recently, is when an employee resigns and in the notice period starts to collect and exfiltrate data. In this specific scenario combining non-technical indicators – resignation - with a threat hunting approach – search the network metadata for anomalies - can be very beneficial. ■



Playbooks & Automation

- Intelligent & Dynamic
- Intuitive Drag & Drop
- Out-of-box & Customisable

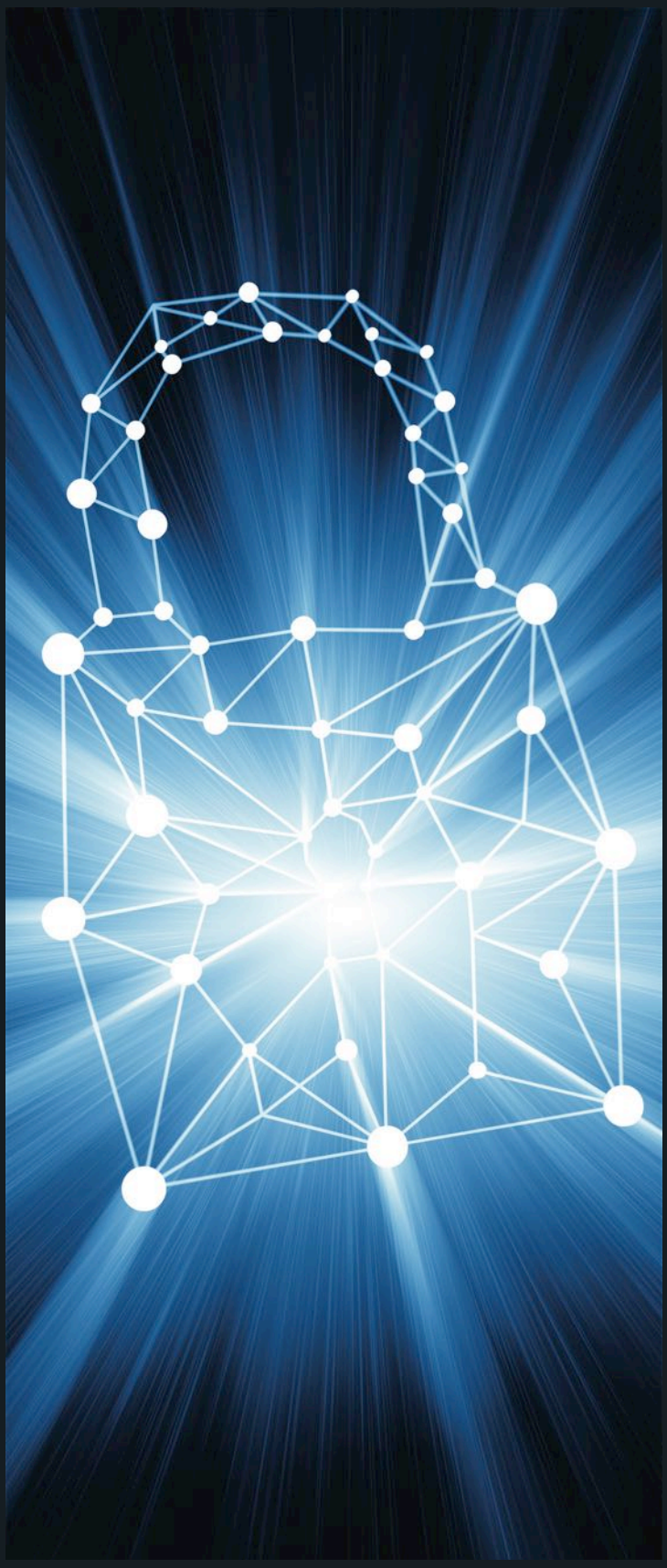




blockapt.com

BLOCKAPT™

Cybersecurity Trends



A publication

web for your business
swiss webacademy

edited by:

BLOCKAPT™

Redaction:
Laurent Chrzanovski and
Romulus Maier †
(all editions)

For the UK edition:
Raj Meghani

Translation and proofreading:
Laurent Chrzanovski, Raj Meghani

ISSN 2559 - 6136
ISSN-L 2559 - 6136

Addresses:
Swiss Webacademy - Str. Şcoala de Înot
nr.18, 550005 Sibiu, Romania

BlockAPT Limited
14 East Bay Lane,
The Press Centre, Here East,
London. E20 3BS
United Kingdom

www.swissacademy.eu
www.cybersecurity-dialogues.org
www.blockapt.com