N°2 - JULY/SEPTEMBER 2024

CYBER-IT

CYBER IS A MARATHON NOT A SPRINT

OSINT

The secrets of photo-based open source intelligence

INTERVIEWS

Discovering new Cyber & IT talents

EUROPOL

Behind the scenes of Operation EndGame

SHADOW IT

Revealing vulnerabilities in an organization's external attack surface

SPECIAL FEATURE

OLYMPIC GAMES

WHAT ARE THE PRIMARY RISKS FOR THE UPCOMING EVENT ?

@arnaud_leroy

EDITORIAL

First and foremost, many thanks for all your feedback and encouragement after the first issue.
Your comments and support inspired me to start this second edition.

This new issue will focus on the biggest sporting event of the coming years: the Paris 2024 Olympic Games !

The stakes related to an event of this magnitude highlight the challenges of maintaining IT infrastructures and security. I would like to extend a special thanks to Lieutenant Colonel Lambert for his contribution to the special report.

Additionally, I am pleased to present a demonstration of an OSINT research based on an element from a photo, presented in the form of a little challenge.

I will revisit the disruption of several domains and servers by Europol during Operation EndGame, which took place in recent weeks.

The continuation of interviews with IT and cybersecurity professionals, who pleasantly answered my questions, will also be featured.
I will conclude this issue with a brief overview of what Shadow IT is and the risks associated with it.

I hope that reading this second edition will be as interesting to you as the first edition, and that it will be well received.

Arnaud Leroy

SOMMAIRE

Paris 2024 Olympic Games
A Major Challenge for Cybersecurity

Games and security : a tumultuous pair

The Paris 2024 Summer Olympic and Paralympic Games loom as France's most monumental event since the 1900 World's Fair.

The numbers are staggering: a budget of 7 billion Euros, an audience of 4 billion viewers, and an expected 12 million spectators. However, let's hope cyberattacks don't reach record highs.

Previous Olympic Games have shown that the threat is real. During the Tokyo 2020 Games, for instance, cyberattacks attempted to disrupt the event, although most were thwarted thanks to robust security measures. Paris 2024 aims to leverage these experiences to further improve its defenses.

Can these Games be an exception?

results, broadcasting images, and managing accreditations for athletes, teams, and officials. All of this, places information systems at the heart of the Games' operations.

The Olympics are one of the most targeted events in the world. This is a technology director worst nightmare, according to Bruno Marie-Rose, Paris 2024's Technology Director.

The Olympics, as a global gathering, are often an arena for political games. The exclusion of Russia from the Tokyo 2022 Olympics and political statements by certain athletes are striking examples.

This political facet exposes them to potential threats from state actors as well as cybercriminals.

The Paris 2024 Games are expected to be the target of billions of cyberattacks, “eight to ten times more than the Tokyo games »

Bruno Marie-Rose
(Technology Director - Paris 2024 Games)

France, gold medal in security ?

How to encounter an invisible enemy ? Are prevention, training and communication sufficient to minimize the risks during these games?

The History of the Olympic Games is marked by a multitude of incidents and attacks, Highlighting the Inherent Risks of hosting an event of such magnitude.

The tragic assassination of participants during the Munich Games in 1972 remains engraved in our memories, poignantly reminding us of the Games' vulnerability to external threats. Moreover, instances of cyberattacks have been reported in previous editions, underlining the imperative need to strengthen digital security in preparation for Paris 2024.

To counter these threats, robust technical measures are crucial. It is essential to implement protection mechanisms against DDoS attacks and malware to ensure the uninterrupted availability of networks. At the same time, the importance of public awareness should not be underestimated.

Training programs on digital and physical security for staff and athletes are of critical importance. Additionally, clear and precise communication with the public is necessary to anticipate potential crises and ensure the safety and well-being of all participants.

The Olympic Games Organizing Committee is getting prepared to counter cyberattacks, drawing on lessons from previous editions. Each edition is unique, with changing contexts, evolving threats, and an increasing number of attacks.

To face increasingly sophisticated and frequent cyberattacks, French authorities are implementing enhanced measures. ANSSI (France' National Cybersecurity Agency) has entered into a cooperation agreement with the Japanese NISC (National Center of Incident Readiness and Strategy for Cybersecurity), enabling strengthened exchanges and sharing of experiences in cybersecurity for major sporting events. Simultaneously, ANSSI is intensifying its communication campaigns to raise public awareness about the importance of digital hygiene.

The cyber threat looming over the Paris 2024 Olympic and Paralympic Games, in line with previous editions, is primarily related to state-sponsored disruptions. Attackers might attempt to target certain systems to gain unauthorized access to venues or to trigger the evacuation of spectators, gathering them outside secured areas and thereby facilitating terrorist attacks.

Concrete Measures and Implementation

Aware of the threat of cyberattacks for more than three years prior to the event, the 2024 Olympic Games Organizing Committee focuses on international collaboration among governments, companies, and involved organizations to ensure security.

For the Paris 2024 Olympic Games, several security measures are implemented to protect the event against various threats, including cyberattacks and physical attacks.

The measures can be categorized into five main areas:

- **Cybersecurity**
- **Physical Security**
- **Raising awareness**
- **Advanced Technologies**
- **Coordination**

Cybersecurity

A substantial budget of over 17 million Euros is allocated to cybersecurity for the Paris 2024 Olympic Games, including a series of detailed preventive and defensive measures against cyber threats.

This budget covers a variety of initiatives aimed at ensuring maximum protection for the event. Among these initiatives are full-scale simulations conducted to prepare security teams for a diversity of attack scenarios, executing realistic exercises that simulate potential cyberattacks, including DDoS attacks, network intrusions, and phishing attempts. These simulations aim to strengthen rapid and effective incident response capabilities.

In parallel, software development integrates extremely stringent security protocols. This includes rigorous code audits to detect and correct vulnerabilities before deployment, as well as the implementation of a system for regular updates to address new threats. Simultaneously, the network infrastructure and servers are designed with high levels of isolation and robust security barriers.

The network architecture is segmented to protect different levels of the network, and separation techniques are employed to ensure the impermeability of network layers and servers, thereby preventing intrusions and safeguarding sensitive data.

Regular security audits are conducted to identify potential vulnerabilities and proactively apply necessary fixes. Security Operations Centers (SOCs) are also established to monitor network activities in real time, allowing for immediate detection and rapid response to security incidents. This continuous monitoring is crucial to ensure any anomaly is quickly detected and addressed, minimizing the risk of intrusion.

International cooperation is an essential pillar of this defense strategy. A partnership agreement with Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) facilitates the exchange of valuable information and experiences in cybersecurity. These exchanges enhance the defense capabilities of both nations, providing insights into best practices and the latest security innovations.

Furthermore, collaborations with other cybersecurity agencies worldwide reinforce cyber defenses, ensuring a coordinated and integrated approach to counter global threats. These partnerships allow for diverse expertise and better anticipation of potential attacks, contributing to the overall security of the Paris 2024 Olympic Games.

NISC
National center of Incident readiness and Strategy for Cybersecurity
内閣
サイバー
セキュリティ
センター

Physical Security

For the Paris 2024 Olympic Games, a comprehensive set of physical security measures has been implemented to ensure the protection of all participants, spectators, and staff. Surveillance is intensified through the installation of high-resolution surveillance cameras strategically placed in and around the Games venues. These cameras enable continuous and detailed monitoring of activities, helping to quickly identify any suspicious behavior or potential threats.

In addition, security drones are deployed for aerial surveillance, providing an overall view of the sites and the ability to detect incidents on a larger scale and in real time.

Access controls are rigorously reinforced. The use of identification badges and biometric technologies, such as facial recognition and fingerprint scanning, ensures that only authorized personnel can enter critical areas. Barriers and checkpoints are set up at all strategic entry points, where thorough identity checks and access authorizations are conducted. These measures aim to prevent any unauthorized intrusion and ensure that access to the facilities is strictly reserved for accredited personnel.

Security arrangements are significantly reinforced for the event, requiring more personnel. An increased presence of police and security forces ensures public order and a rapid response to incidents. These forces are complemented by private security agents, specially trained to enhance surveillance and intervene when necessary. Together, they patrol the Games sites, monitor the crowds, and are ready to react quickly in case of emergencies.

Preventing terrorist attacks is a crucial aspect of the Olympic Games security.

The Vigipirate plan, a French national security alert system, is reinforced with specific measures adapted to the Games. This includes increased patrols, stricter controls, and heightened vigilance in all areas related to the Games.

Additionally, close collaboration with intelligence services is in place to identify and neutralize potential threats before they materialize. This partnership provides access to up-to-date intelligence information, facilitating a proactive response to identified threats.

These coordinated efforts, including advanced technologies, enhanced human presence, and proactive prevention strategies, aim to create an extremely secure environment for the Paris 2024 Olympic Games.

This comprehensive approach ensures not only the physical safety of participants and spectators but also a quick and effective response to any eventuality, thereby ensuring the success and security of this major event.

Expecting the unexpected! We are already seeing attackers trying to target individuals with login attempts. We remain vigilant and cautious

Bruno Marie-Rose
(Technology Director - Paris 2024 Games)

Raising Awareness

For Paris 2024 Olympic Games, raising awareness and training are fundamental elements of the security strategy, aiming to comprehensively prepare all parties involved to face various potential challenges, whether related to cybersecurity or physical security.

Awareness campaigns are carefully designed to reach a wide audience, including not only spectators, athletes, and on-site staff but also external stakeholders such as the Game's partners.

They provide detailed information on best practices in cybersecurity, from identifying potential threats to secure management of personal data and vigilance against phishing attempts. These campaigns are not limited to the digital sphere, they also address physical security measures, such as emergency evacuation procedures, gathering points/safety zones, and incident reporting protocols.
Specific trainings are meticulously tailored to the needs and responsibilities of each group involved in the event. For the staff and volunteers responsible for organizing and managing the Games, these trainings include an in-depth immersion in security protocols, crowd management, emergency procedures, and crisis intervention coordination.

Practical simulations are integrated into these trainings, allowing participants to apply their knowledge and skills in real-world scenarios, thereby improving their preparedness and responsiveness in emergency situations.

For athletes and delegations, specific awareness sessions are organized to inform them of potential cybersecurity and physical security risks.
These sessions provide practical advice on protecting personal information, securing electronic devices, and steps to take in case of a threat or security incident.
They also raise awareness about procedures for reporting suspicious behavior or potentially dangerous activities, thus encouraging active participation in collective security. By comprehensively integrating awareness and training at all levels of the Olympic Games organization, Paris 2024 aims to create a secure and resilient environment for all participants and spectators. These initiatives reinforce the culture of safety, promoting collective vigilance and effective responsiveness to emerging threats, thus contributing to the success and safety of this major international event.
To complement these initiatives, additional resources are allocated to the creation of interactive educational materials, including educational videos, infographics, and practical guides.
These resources make information on cybersecurity and physical security more accessible and engaging, promoting better understanding and more effective adoption of best practices.

Additionally, each French elementary school pupil received a commemorative 2 Euro coin.
This initiative helps to engage young generations with the Paris Games.

Commemorative 2 Euros coin
(gifted to French elementary school students)

Advanced Technologies

The use of artificial intelligence (AI) allows networks to be constantly monitored to detect anomalies that may indicate cyberattacks. AI systems are programmed to analyze huge volumes of data in real time, identifying suspicious patterns and unusual behaviors that could signal an imminent threat.

Thanks to these capabilities, security teams can quickly respond to neutralize attacks before they cause significant damage.

Artificial intelligence is also employed for crowd management. AI applications analyze the flow of people using real-time data from surveillance cameras and sensors to understand crowd movements and anticipate potentially dangerous situations.

For example, if a crowd begins to form in a critical area, AI can alert security officials to take preventive measures, such as redirecting the flow of people or deploying additional personnel. This technology helps maintain order and ensure the safety of spectators by preventing overcrowding and panic situations.

In parallel, blockchain technology is implemented to secure the ticketing for the Olympic Games. Blockchain ensures the authenticity of tickets by making each one unique and tamper-proof. Every ticket is recorded in a decentralized digital ledger, preventing any unauthorized duplication or modification.

This innovative ticket management method significantly reduces the risk of fraud and ensures that spectators can access events with complete confidence.

Furthermore, the transparency provided by blockchain means that each ticketcan be tracked from its creation to usage creation to usage, offering complete traceability and further enhancing security.

The implementation of these advanced technologies requires sophisticated infrastructure and close coordination among various security systems. Dedicated teams work continuously to develop, test, and improve these systems to ensure they operate seamlessly during the Games.

This proactive and technological approach to security contributes to creating a safe and reliable environment for the Paris 2024 Olympic Games, ensuring the protection of data and the physical safety of participants and spectators.

Coordination and Communication

A unified command center will be established to coordinate safety efforts among the various agencies and services involved. This center will play a crucial role in the management of safety operations, ensuring smooth communication and rapid response to incidents.

Advanced communication systems will facilitate real-time transmission of information, enabling effective coordination and immediate reaction to potential threats. This centralized setup is essential to ensure that all stakeholders are synchronized and can act cohesively and swiftly in case of emergencies.

Simultaneously, international collaboration will be strengthened to exchange crucial information on threats and best security practices.

Partnerships with other countries will enable the sharing of data and strategies, thereby enhancing collective defense capabilities.

This cooperation will also include mutual logistical and technical support, where countries assist each other in bolstering their incident response capabilities.

By combining resources and international expertise, the Games' organizers will be able to anticipate and neutralize potential threats more effectively, ensuring the security of the event on a global scale.

The worst-case scenario would be attacks that would cause interruption or disruption of the competitions.

One of my counterparts at the 2018 PyeongChang Winter Olympics witnessed some systems shutting down just before the opening ceremony. I do not want this to happen!

Bruno Marie-Rose
(Technology Director - Paris 2024 Games)

Over 10 Years of Cyber Attacks Targeting the Olympic Games

After enduring 4 billion cyber-attacks during the Tokyo Games in 2021 and half a billion in Rio in 2016, what will be the impact in 2024, and what measures can we take to prevent the risks ?

In 2008, during the Beijing Games, several deceptive sites were set up to sell fake tickets. However, it was the attack during the opening ceremony of the London 2012 Games that brought cybersecurity to the forefront of concerns for the organizers.

LONDON 2012

The London Games marked a turning point in the attention cybercriminals paid to the Olympics. On the day of the opening ceremony alone, over 212 million cyberattacks were detected, including several coordinated attacks that disrupted services on the electrical infrastructure.

SOCHI 2014

In 2014, during the Winter Olympics in Sochi, no significant cybersecurity incidents were reported. Was this due to Russia's tight state-controlled communication, a lack of interest from cybercriminals, or fear of retaliation? This question remains unanswered...

RIO 2016

During the Rio Games, the data was alarming, with a total of cyberattacks reaching half a billion, equating to a frequency of 400 attacks per second. Large-scale and repeated DDoS attacks targeted Olympic partners' websites, starting several months before the event's opening ceremony.

PYEONG-CHANG 2018

In 2018, the problem became publicly amplified during the opening ceremony of the PyeongChang Games. Difficulties arose: some spectator could not print their tickets, due to Wi-Fi issues on site, screen outages, malfunctioning access sensors, and a dysfunctional official Olympics app affecting access to ticketing, events schedules, hotel information, and access maps. The consequences were quickly felt.

TOKYO 2020 (2021)

Even with the Tokyo 2021 Olympics taking place behind closed doors after being postponed for a year due to the global pandemic, the organization was targeted with 4.4 billion cyberattacks. The Nippon Telegraph and Telephone Corporation reported that these attacks exploited various methods, including phishing emails and the creation of fake websites resembling the official Olympic platforms.

BEIJING 2022

In 2022, during the Winter Olympics in Beijing, it was the official Covid-19 tracking app, My2022, that sparked controversy due to fears of cyber espionage. A subsequent reverse-engineering analysis of the app revealed that athletes' communications were being collected, analyzed, and stored on Chinese servers.

Paris, a Favorable Ground for Attackers?

Les hostilités semblent déjà déclarées du côté des attaquants, en tout cas ça semble en prendre le chemin quand on voit les vols de données concernant les jeux de Paris.

Hostilities appear to have already been declared on the attackers' side, or at least they seem to be heading that way when we consider the data breaches concerning the Paris Games.

Recently, several security incidents related to the Paris 2024 Olympic Games have been reported, highlighting potential vulnerabilities. One of the most notable incidents involves the theft of a laptop and USB drives containing information about the Games. An employee of the Paris City Hall boarded a train stationed on platform 18 of Paris Gare du Nord. As the train was delayed and he prepared to switch trains, he discovered that his bag was missing.

He later reported that he had placed the bag in the luggage compartment above his seat. A few dozen minutes later, around 7:30 p.m., he went to the station's police station to report the theft and file a complaint.

Paris prosecutor's office later clarified that the stolen USB drive only contained "notes related to traffic circulation in Paris during the Olympic Games" and not sensitive information about security measures. It was simply "ordinary maps of Paris."

Are these reassurances genuine, or a facade to calm future spectators? The question becomes more pressing considering this is not the only incident reported in the media...

Two months after this event, at around 2.00 a.m. in Sceaux (South of Paris metropolitan area), a house owner is awakened by the sound of breaking glass. He discovers that he has been the victim of a burglary. The next thing he knew, three laptops were missing and the burglars manage to escape with their loot.
When the police arrive on the scene, the victim explains that he works for Thalès and one of the stolen laptops is for professional use.

The victim states that this laptop also contains "sensitive information related to territorial surveillance and security for the Olympic Games."

Should these events alarm us, or are they mere coincidences?

The safety and security of our employees, clients, and operations are critical issues for the group, and we enforce very strict security procedures, including strong authentication systems and encryption.

Statement from Thales Group

Meeting with Lieutenant Colonel Sophie LAMBERT from COMCYBER-MI

Who better to discuss the risks associated with the Olympics than the Head of the Cyber Anticipation and Crisis Management Department of the French Ministry of the Interior's cyberspace command ?

We are witnessing a significant increase in cybercriminal activities, echoing previous large-scale international sporting events.

Sophie LAMBERT

What is the COMCYBER-MI ?

The French Ministry of the Interior's Cyber Command (COMCYBER-MI) plays a central role in protecting the Paris 2024 Olympics against cyber threats.

Our missions include :

- Continuously monitoring cyberspace to detect and neutralize potential threats.
- Coordinating with national and international partners to exchange information on cyber threats.
- Implementing protocols for rapid dissemination of any detection or suspicion of cyber-attacks to minimize impact on the Games.
- Training and raising awareness among involved parties on cybersecurity best practices.

Our Cyber Threat Analysis and Aggregation Center centralizes and analyzes critical data to identify cybercriminals, analyze their modus operandi, characterize cyber threats, and anticipate crises. We produce specific alerts and analyses to inform our partners in the event of cyber-attacks or emerging threats.

We are positioned at the National Strategic Command Center (CNCS) for the Paris Games at Beauvau (where the French Ministry of Interior is located) alongside our partners, including ANSSI (France' National Cybersecurity Agency).

Who is Sophie LAMBERT ?

I am Lieutenant Colonel Sophie Lambert, head of the Department of Anticipation and Crisis Management within the Cyber Command of the Ministry of the Interior.

Our role is to develop the most comprehensive threat assessment possible in cybersecurity, and thereby adapt our operational response to counter cyber threats and effectively combat cybercrime.

Cybersecurity is a shared responsibility. As we approach the Paris 2024 Olympics, I want to emphasize the importance of everyone's vigilance. Together, we can confront cyber challenges, ensure the security of this global event, and demonstrate our cyber resilience to deter our adversaries.

I also encourage you not to leave cyber incidents go unanswered. Filing a complaint is an essential step to protect yourself, your loved ones, and contribute to everyone's safety. Threats are constantly evolving, and it's essential to remain vigilant, stay informed, get training, and implement appropriate protection measures. Do not underestimate the importance of a strong genuine cybersecurity culture.

According to you, what are the most important or notable risks for these games ?

This global event, which will attract millions of visitors and spectators, represents not only an exceptional sporting moment but also a potential target for various threats, particularly in the digital realm.

Paris 2024 Olympics present a prime opportunity for cybercriminals driven by profit, sabotage, hacktivism, or espionage. The most significant risks include :

- DDoS attacks aiming to disrupt online services.
- Ransomware, paralyzing computer systems until a ransom is paid.
- Mass or targeted scams exploiting the event's popularity.
- Website defacements, often used to spread propaganda messages.
- Theft and massive dissemination of sensitive data, compromising confidentiality and integrity of information.

International conflicts and the political and social context in France could also intensify cyberattacks, aiming to disrupt the event and spread propaganda messages. This high-profile event would benefit cybercriminals aiming to disrupt the Paris 2024 Olympics, destabilize French interests, and actually convey propaganda messages. The Paris Games also serve as a recruiting platform for them.

As we approach the 2024 Olympic and Paralympic Games, we observe a significant increase in cybercriminal activities, echoing previous international sporting events.

For the year 2023, French police and gendarmerie services recorded 278,770 digital incidents, compared to 255,320 in 2022. This represents a 40% increase in cyber-related offenses over the past five years, with an average annual increase of 8%.

COMCYBER-MI Unit Badge

Since January 2024, we have tripled our detections of DDoS attacks, data thefts, and website defacements. Some hackers may already be infiltrated into critical systems, ready to strike at the right moment. Between 2022 and 2023, cyberattacks increased by 30% according to ANSSI (France' National Cybersecurity Agency).

There are several possible explanations for this increase: the expansion of digital usage, an increase in potential attack surfaces, but also the improvement of incidents reporting. However, there is still a significant dark figure in cybercrime, as only 0.4% of offenses are reported, highlighting massive underreporting of attacks.

If we focus solely on the organization of the Olympic Games today, it represents an attractive target for cybercriminals. We are likely to see an increase in cyber attack attempts targeting the Games infrastructure, participants, and spectators.

Ransomware attacks and theft/distribution of sensitive data are our main concerns due to their potential for significant disruption. We are also monitoring scams targeting spectators, website defacements, and risks related to the supply chain. The consequences of these attacks could be disastrous:

- Disruption of sports event broadcasts.
- Suspension of authorized personnel access to secure areas.
- Disruption of public transportation and visitors' management systems.
- Disruption of Olympic venue infrastructures.
- Event-related scams such as typosquatting

To ensure the security of the Games, several measures have been implemented.

What measures have been implemented to secure these games ?

The creation of the CNCS dedicated to major sporting events like the Games, operating 24/7.
The integration of advanced technological solutions for detecting and preventing cyberattacks.
Regular simulations and exercises to test and improve our response capabilities.

Close collaboration with the Olympic Games organizers, public authorities, national (public and private) and international partners for a comprehensive and coordinated security approach. We are well aware of the increased risks due to the overexposure and attack surface that the Olympics represent.

Photos in open source research

How to find information from photos

OSINT: What is it?

OSINT (Open Source INTelligence), consists of collecting and analyzing data from publicly accessible sources. This can include websites, social networks, public records, etc. The goal is to transform this data into useful information for decision-making.

Open source data is legally accessible to the public. It can be free or require purchase or official procedures (such as a press article or a business registration document). It is important to know how to identify and collect this data legally and efficiently.

OSINT Sub-families

SOCMINT : Intelligence from social networks.

IMINT : image-based intelligence.

SIGINT : Intelligence based on electronic signals.

HUMINT : Intelligence from human sources.

GEOINT : Intelligence from geospatial imagery.

MASINT : Intelligence from measurements and signatures.

The Intelligence Cycle

The intelligence cycle consists of four phases: identification of needs, data collection, analysis, and dissemination, with sometimes a fifth decision-making phase.

Identification of Needs

This involves defining the issues and identifying useful information by asking specific questions to guide the research.

Data collection

This phase involves determining the scope of sources, collecting reliable and relevant data, and documenting each research details to avoid oversight.

Analysis

This phase transforms data into information by interpreting and contextualizing it, eliminating false positives, and establishing timelines if necessary.

Dissemination and Decision-making

Dissemination should be tailored to each stakeholder's role and lead to a decision, which can redirect needs and initiate a new research cycle if necessary.

To begin the analysis of an image, it is recommended to observe it carefully to identify significant elements. These can then be isolated for specific research purposes.

Examining EXIF data is essential, as well as reviewing file properties such as creation dates and file names.

Next, performing a reverse image search can be useful, potentially by isolating a part of the image. If a location is identified, using cartographic visualization tools such as Google Street View and Photosphere is necessary.
Depending on the location, it may be necessary to search based on the address or local land registry information.

Finally, if the image was posted by an internet user, a search using their username may provide additional information.

Here is an example flowchart illustrating the types of information that can be extracted from a simple photo.

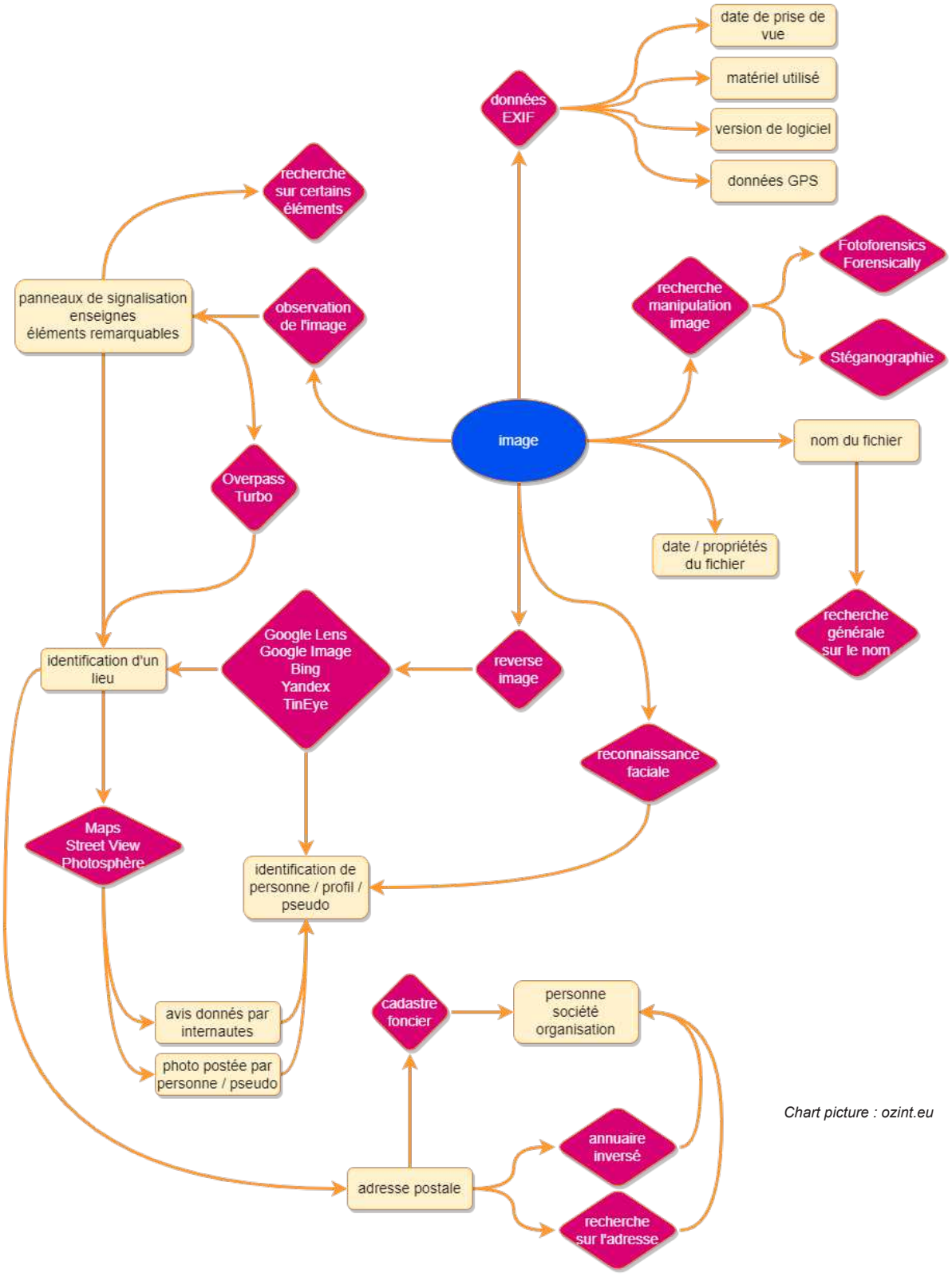


Chart picture : ozint.eu

Concrete scenario : Carrots, Rabbits, and Statues

Here is an example of an OSINT challenge imagined by Ozint.eu
(with Julien Metayer's consent for the distribution of this content)

With the image provided only, can we answer the following three questions ?

1. How many carrots and rabbits is this statue greeting in June 2022 ?

Before his current company, the creator of the artwork had another commercial structure that is now closed.

2. In which city was this structure domiciled ?

In this city, the war memorial was created by a famous sculptor who proposed his own vision of the original man in the 1930s.

3. What is the name of the historical site located 18 km from this artwork ?

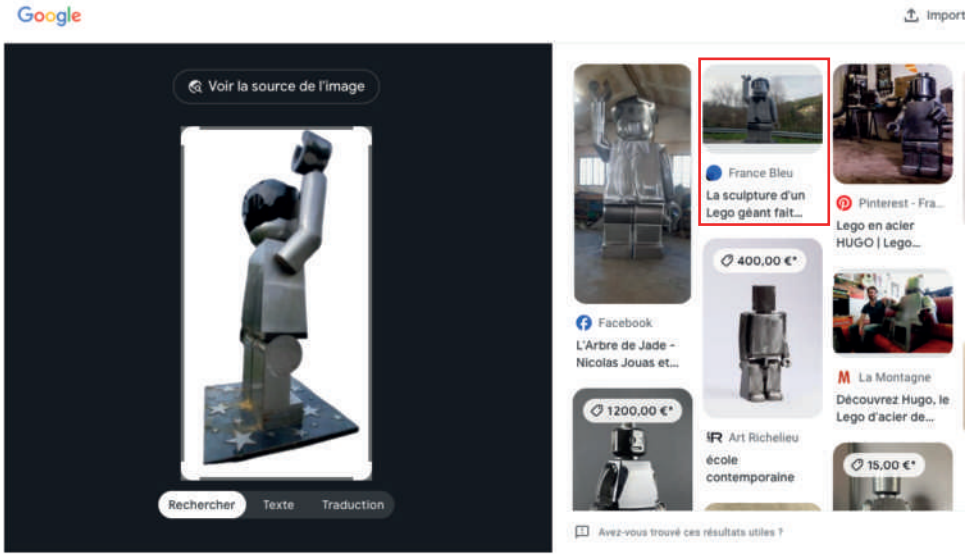


Figure 1 - Google Lens

A reverse search on Google Lens *(Figure 1)* allows us to bring up an image that appears to closely resemble the photo provided.

We see a picture of an article from France Bleu *(Figure 2)* that seems to be about the statue we are looking for.

Upon reading the article, we gather essential information: the city where the statue is located is **"Lodève"** and the name of the artist who created is **Nicolas Jouas** *(Figure 3)*

Figure 2 - Picture from France Bleu article (French media)

Du haut de ses quatre mètres, la sculpture du Lego® géant salue les automobilistes depuis le bord de la route. © Radio France - Sophie Pouzeratte

Les automobilistes ont eu la surprise de voir apparaître cette monumentale figurine Lego® mi-décembre à la sortie de Lodève. Avec ses **quatre mètres de haut**, et son air avenant, la sculpture fait sensation, et les curieux sont nombreux à s'arrêter pour prendre des photos.

C'est dans l'atelier Takavenir que l'artiste Nicolas Jouas et son collectif ont imaginé et créé la sculpture. **L'atelier est spécialisé dans les œuvres d'arts en métal**, et voulait fabriquer une création taille XXL. "*Techniquement c'était plus pratique de réaliser un Lego_™_*, explique Nicolas, *il suffisait de prendre une figurine et d'adapter ses dimensions à une œuvre de très grande taille*".

Figure 3 - France Bleu article (French media)

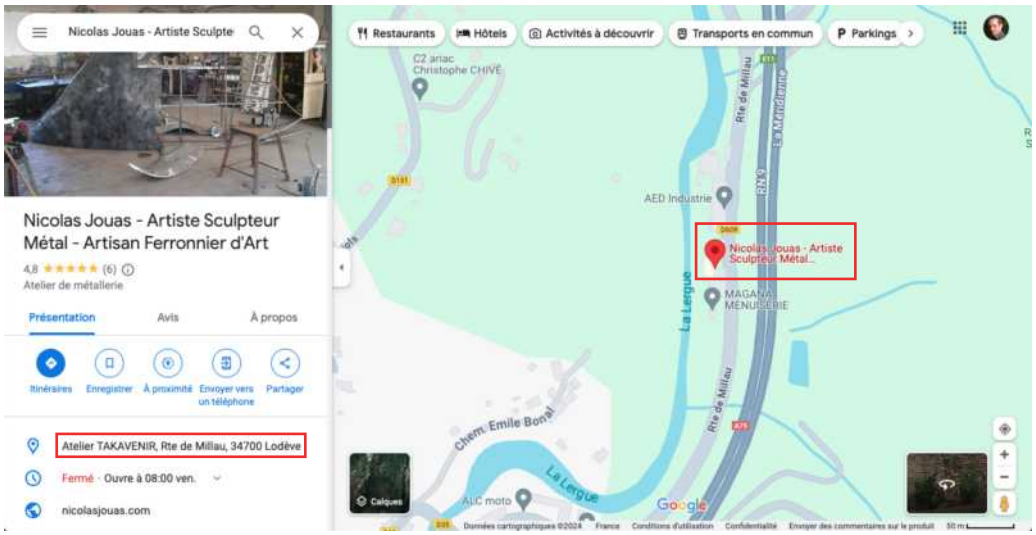


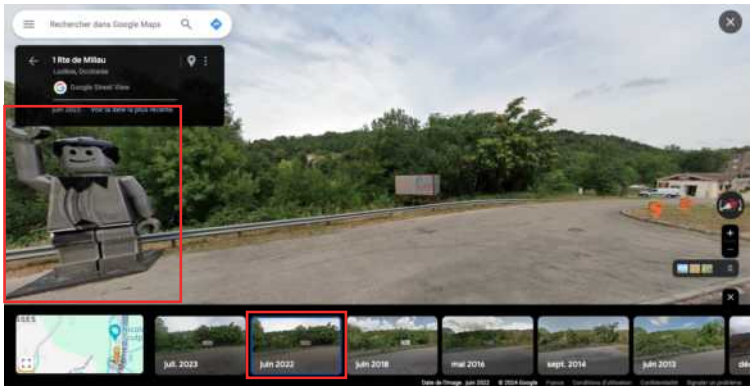
Figure 4 - Google street view

If we search for the artist's name on Google Street View *(Figure 4)* we indeed find the name of the city of "Lodève" mentioned in the previous article, as well as the presence of his workshop. In street view mode, we can clearly see the workshop, but there is no sign of the Lego statue...

Upon closer look, we notice that the photo was taken in July 2023. Let's change the photo's shooting date and check in June 2022 if we can find something that looks like our statue.

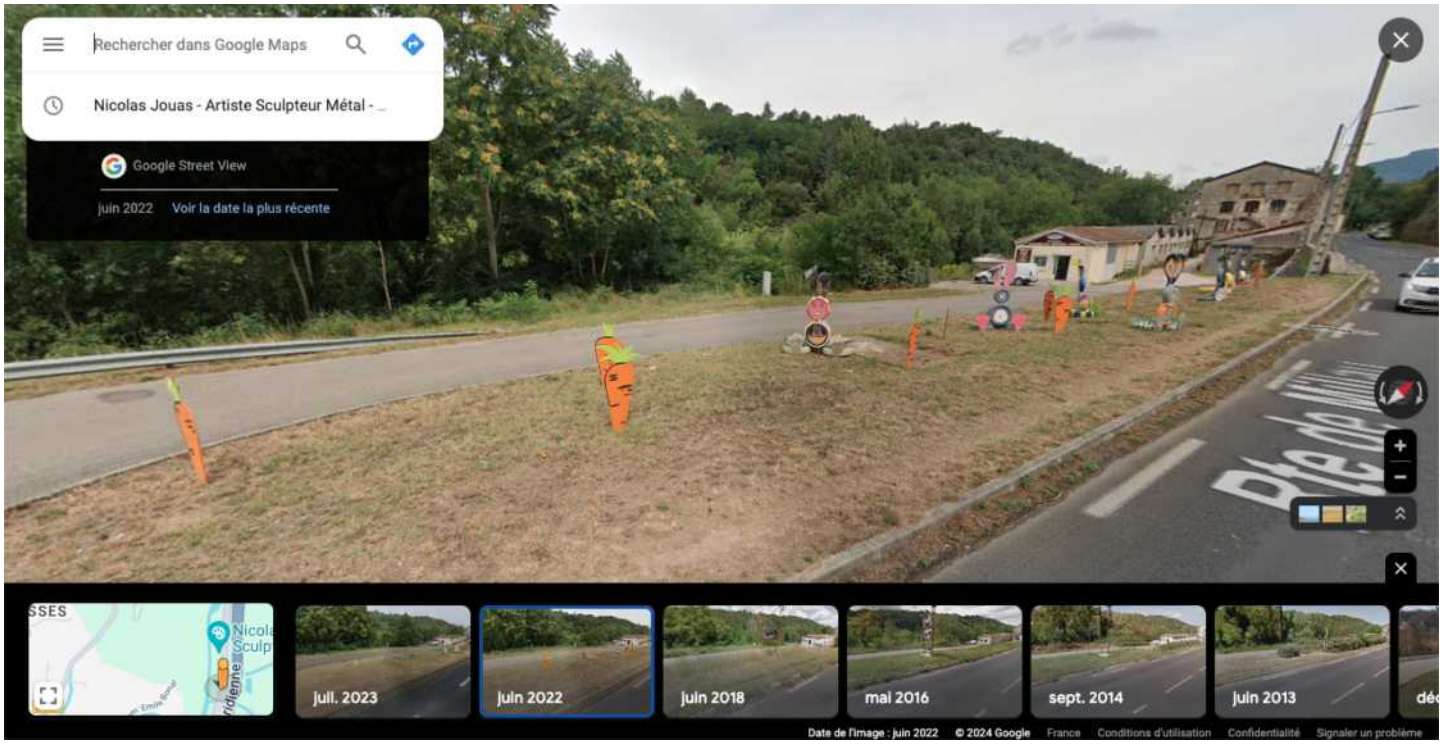
BINGO !

Juillet 2023



Juin 2022

If we turn the camera around, we can see a number of rabbits and carrots planted in the grass in front of our Lego statue: 9 carrots and 7 rabbits in total. **The answer to the 1st question is 16!**



It is mentioned in the challenge's summary that before leading the Takavenir workshop, Nicolas Jouas was responsible for another structure that is supposedly closed today.

In such cases, the most obvious thing to do is to conduct a search on the French website societe.com, which provides a significant amount of information that could be useful to progress in our search.

To get started, the easiest approach is to search for the name of the Takavenir workshop to ensure that we are dealing with our artist and not a namesake.

The result obtained is as expected, and we find Nicolas Jouas, as shown in the screenshot *(Figure 5)*.

We can now check on this website to find more information about companies associated with Nicolas.

Figure 5 - Takeavenir company profile on societe.com website

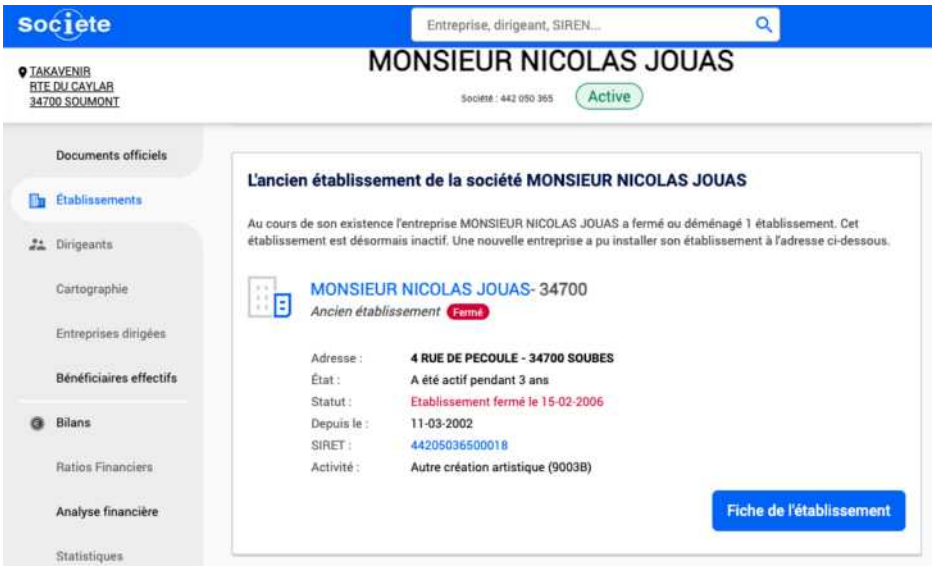


Figure 6 - Nicolas Jouas' profile on societe.com website

By searching further on the page dedicated to the sculptor artist, we found a secondary establishment that is now closed, which is interesting!

This establishment was located in the city of Soubes.

Therefore, the answer to the second question is Soubes!

In the city of Soubes, the war memorial was created by a renowned sculptor who proposed his vision of the “original man” in the 1930s.

Our next mission is to gather information about this famous war memorial, which will serve as our starting point to answer the third question of this challenge: What is the name of the historical site located 18 kilometers (11.2 miles) from this artwork?

A Google search provides us the first crucial information for the next steps: the sculptor of Soubes’ war memorial is Paul Dardé *(Figure 7)*.

Among Paul Dardé's work, we find the sculpture we are looking for *(Figure 8)*.

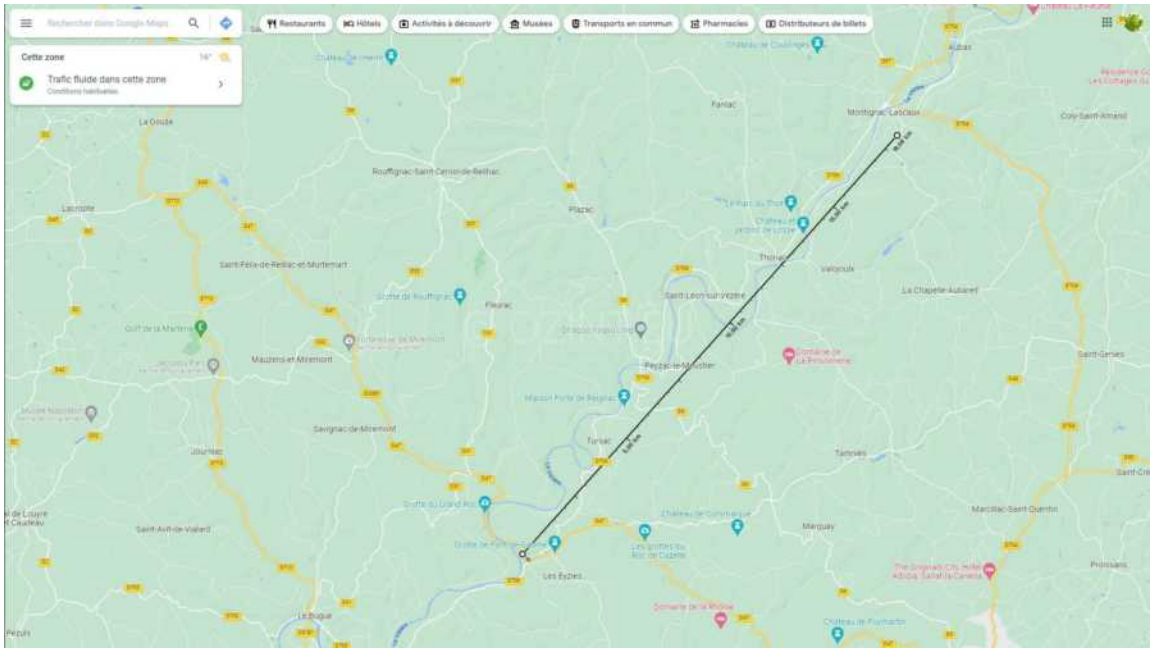
Figure 7 - Google search

Autres sculptures [modifier | modifier le code]

- *L'Homme-Chèvre*, ornant anciennement le parc du Château de Vizille.
- *Stèle à la mémoire des officiers de médecine* à Béziers, Hérault.
- *Les Pleureuses*, localisation inconnue. Plateau des Glières, Haute-Savoie.
- *La Douleur*, dit aussi *Tête Aux Serpents*, *Tête de Prostituée* ou *Remords*, 1913, gypse, Paris, musée d'Orsay.
- *Laocoon*, 1919, domaine de Montplaisir, Lodève, Hérault.
- *Faune Guettant Une Nymphe*, 1924, Musée de Lodève, Hérault[11, 12].
- *L'Homme Primitif*, 1931, Les Eyzies-de-Tayac-Sireuil, musée national de Préhistoire ; cette œuvre de trois mètres de haut et de cinq tonnes a été sculptée dans un seul bloc ; elle représente un homme de Néandertal et non pas un homme de Cro-Magnon, ainsi surnommé localement à cause de la proximité de l'abri de Cro-Magnon[13], distant de moins d'un kilomètre.

Figure 8 - Wikipedia webpage - information about Paul Dardé’s “L’Homme Primitif” sculpture

Using Google's distance measurements, we can find a world-famous historical site: the Lascaux Cave.
Therefore, the answer to the third question is Lascaux!



Interviews with the movers and shakers of today's cyber and IT space

We know them through their daily online publications, but who are they ?

Here is the continuation of the interviews that started in the first issue of CYBER-IT Magazine. I once again had the privilege to discuss with professionals in the industry who agreed to participate to these Q&A sessions. Time is precious for everyone, and each moment dedicated to answer my questions is truly valuable! To all of them, Thank You!
The interviews published in the magazine tend to be longer than those posted on LinkedIn (due to Linkedin's character limit policy).

PIERRE PENALBA
Police Chief Emeritus

Hi Pierre, can you explain who you are, in your own words ?

"A dinosaur of cybersecurity because I started programming in 1983 on a ZX81... But above all, a technology enthusiast."

Can you explain a bit about your background ?

"I first completed my high school diploma, then went on to earn a degree in software engineering. I've worn many hats over the years, starting as a police inspector and then becoming an IT correspondent. Later, I became the head of the first cybercrime unit outside of Paris.

I also have the pleasure of being an author of books on cybersecurity and the darknet. Since I don't like to get bored, I also have the privilege of being a speaker and trainer in cybersecurity, as well as a lecturer at an engineering school. "

What are your daily tasks ?

"Currently, I mainly do consulting, pentesting, and training. Additionally, there are periods of teaching."

What does a typical day look like for you ?

"I start by checking the news, dark web forums, and other sources. Then, whenever possible, I take specialized MOOCs on cybersecurity, forensics, etc. In the afternoon, I work on analysis missions, OSINT, etc. My day ends with 2 hours of exercise and quality time with my family until 10.00-11.00 p.m.

I continue with a few hours navigating the complexities of cybersecurity. As you can see, I sleep very little. I think I would need multiple lives 😅"

What do you like about your job ?

"What I appreciate is learning, discovering, investigating, training, and also teaching.

There are some things I don't particularly enjoy, like people who think they know everything, invoicing... oh yes, and also realizing that I forgot to sleep 😅"

Thank you, do you have a final word ?

"Don't worry about AI!
They are tools; humans can learn, comprehend, and always benefit from their chaotic and non-logical capabilities!"

KARIM LAMOURI
Co-founder and President of Hackers Without Borders

Hello Karim, it's a pleasure to share this moment with you. In a few words, who are you ?

"Hi Arnaud, the pleasure is truly mutual! I see myself as just an ordinary person, coming from the suburbs of Paris. Some people are lucky to start from zero, but I started from about -30... I was born to a Moroccan military father who served in the French army and an exceptional mother, notable for her amazing knowledge! I grew up in a family of five, including myself.

Cyber is a way to bring people together, I got into it out of passion, but it's just one facet of who I am; it doesn't fundamentally define me. I often tell myself that I want to live every moment as if I were in the terminal phase of life; I try to live fully and seize every opportunity ! "

What is your background ?

"I will be original and tell you that... I am self-taught. Passion, the time I dedicate to learning and networking, have allowed me to acquire skills that make me employable, especially during incidents or complex situations"

I assume you can't say much, but what are your missions ?

"Indeed, I remain as discreet as possible about my daily missions. What I can tell you is that I strive to be as precise and rigorous as possible in the tasks entrusted to me. For example, I provide consulting to various states, especially abroad. I also manage our NGO "Hackers Without Borders," which I've been involved in since my youth. I believe in including "The Other one" in my choices and my life. A healthy society relies on mutual aid and living together harmoniously. My passion is Humanity with a capital H; it's too important.

I have also recently become the director of the Effor Cyberlab training center in Reims/Nancy, Limoges, and soon Paris."

What do you like and/or don't like about cyber ?

"I love everything about cyber, but I want to emphasize a very important point to me: in France, we have a problem with unity and mutual support! By that, I mean that we have a country of geniuses, with people who are capable to get things moving, great talents, but the big downside is that we are unable to agree and unite !

Certainly, we cannot achieve unanimity and please everyone (even God Himself did not achieve unanimity, so how could we ourselves ?), but sharing with others is the driving force. Ego is simply something horrible."

Thank you, a few words about Hackers Without Borders to conclude ?

"With pleasure !

Hackers Without Borders (HWB) is an NGO created in 2022 following an evening discussion with Florent Curtet, after the cyberattack on the Red Cross in Switzerland which occurred in January 2022. We decided to bring cybersecurity specialists together to establish our association. Florent and I continued to refine our project by including Clément Domingo and Pierre-Marie Léoutre. And that's how Hackers Without Borders was born! Today, we continue our journey, and we are proud to say that profit is not the focus of the association; in fact, we do not have a bank account linked to HWB.

Last but not least, thank you for the time we spent together Arnaud, and I am looking forward to meeting you again soon."

JONATHAN SPEDALE
Investigator and fraud analyst

Hello Jonathan, thank you for taking the time to respond. So, who are you ?

"Hello Arnaud, I'm Jonathan Spedale, a net rogue hunter !"

And what has been your career path ?

"Formerly an artist, after an injury, I stumbled into the world of cryptocurrencies at a time when fraud, which is very prevalent now, was being kept underground and not in vogue. This allowed me to initially self-educate myself and then collaborate with law enforcement on detecting fake documents. It opened doors to various fields: combating payment fraud, investments, insurance, and eventually joining one of the hardest-hit sectors, e-commerce. As a passionate and curious individual, I've evolved in these diverse sectors out of interest and thirst for knowledge, now I am offering my services in fraud testing.
This service has proven its worth: how to combat what we can't see, explain, or understand ?"

Okay! What exactly do your daily missions entail ?

"Currently, I have several types of contracts: path testing, cyber watch/monitoring for companies wanting to assess their exposure to fraud threats, implementing or modifying processes after fraud detection, setting up pre-payment scoring rules to mitigate fraudulent payment attempts - it's quite varied."

Generally, what does a typical day look like for you ?

"No two days are alike for me, just like my offices. I work on-site or remotely, depending on the client's preference.

I listen to their needs, monitor, inform, and advise them, implement procedures or tools for specific issues: constantly improve evolving fraud prevention strategies, monitoring key indicators to reduce risk, alerting on new fraud pockets, enhancing existing fraud detection tools and systems, handling orders on hold, investigating suspected or confirmed frauds, processing daily data reports for analysis of suspicious or fraudulent behaviors, recording and tracking unpaid bills, initiating and monitoring debt recovery procedures.

Overall, I provide internal training on operational processing and research methods."

What do you like and/or don't like about your job ?

"I enjoy the diversity of encounters and, above all, the ingenuity I have to combat every day, an imaginary chess game that gives me daily adrenaline and leaves me smiling with amusement."

Perfect, thank you! Any final words ?

"Stop taking yourselves too seriously in an industry that's evolving every day; anyone can become a has-been tomorrow. Since we're often called in after the breach, there's no need to act like a know-it-all …just take action!"

CYBER MOUSTACHE

YOHANN BAUZIL
Cybersecurity Manager

Hi Yohann, thanks for stepping in front of the microphone this time. Tell us, who are you ?

🎙 "I'm 40 years old and live in Toulouse.

In real life, I'm the Director of Security at a NewSpace startup - @look up space.

On LinkedIn, I'm a cyberstaaar finder and a fighter for equality through cyber influence with robindescyberbois. 🎯"

And what about your background ?

🎙"Completely classic :

- Engineering school with an internship because I wasn't keen on working right after my DUT (technology degree).
- 9 years in the space and IT security sector as a consultant.

With the planets well aligned, I became the CISO of a NewSpace startup, an Airbus subsidiary, for 5 years.

- Then, a misstep, but eventually landed a great role in an amazing NewSpace startup. 🔥🔥"

What can you tell us about your multiple daily tasks ?

🎙"Being in a startup, sometimes one person has many roles, but it's a great exercise of controlled schizophrenia. 🙃
Let's put it this way: I strive to guarantee all aspects of security in my company, from the physical to the digital. I also support our users and our business to find digital solutions that meet their needs."

What does a typical day look like for you ?

🎙"Days are often pretty long:
- I try to limit meetings, but it's not uncommon to have 4 meetings a day because there are so many different topics to address.
- I handle all my emails, daily (sometimes late in the day), and at worst, every week! Never block a user or the business; otherwise, they will bypass you...
- I support my amazing team (who is much more productive than me) to bring tangible improvements and solutions every day."

What do you like and/or don't like about your job ?

🎙"Likes: The diversity of my mission. These conceptual positions only exist in startups. No day is like the other!

What I don't like: These are roles where you can only succeed through excessive commitment. I've been playing the lottery for 3 years; I think it's time to win !😅"

Thanks, Yohann. Do you have any final words ?

🎙"- "Expand your network without limits": we become strong through others. 💪

- "Find a mentor who inspires you": our jobs are too complicated, get some help. 🤝

- "Work on your personal branding": Heaven helps those who help themselves." 👊"

Look Up SPACE

PIERRE PIVETEAU
CEO of Cyberveille

Hello Pierre, many people know you, but tell us more about yourself !

"Well, I am Pierre PIVETEAU, born in the last century (ha ha!), and I am present on various social media networks, I also go by the pseudonym “Cyber Veille”. Cyber Veille started as a small internal 4 pages publication, written in French first and then in English for a NATO headquarters where I used to work.
Later, the idea of putting it on the internet took off, and here I am! At the same time, my desire not to stay away from the civilian world (in terms of cybersecurity) led me to apply to CESIN (Club des Experts de la Sécurité de l’Information et du Numérique - Club of Experts in Information and Digital Security), where I had the privilege of being admitted as a member. I also joined a non-profit organization, the OCOI (Observatoire de Cyber sécurité de l’Océan Indien - Indian Ocean Cyber Security Observatory), whose goal is to promote IT security and data protection in the Indian Ocean region."

What is your background ?

"I have been a military officer for almost 35 years now, coming from the Signal Corps. I've always been immersed in the world of security and the culture of secrecy right from the beginning of my career. Back then, we didn’t talk much about information security but rather SECOM (Communication Security). Naturally, I shifted towards information security at first and then towards cybersecurity with the advent of computers in communication systems. My academic background was initially military, and over time I attended numerous courses through various organizations ANSSI, Sysdream, CF2I, for example."

Can you tell us about your multiple daily tasks ?

"JI don't think my daily routine is very different from other CISOs. Between meetings with management, providing information security support to project managers in the form of working groups, dealing with little issues inherent to an institution like mine, and educating and raising awareness about cyber risks to the people I work with. The only difference is my expertise in certain subjects directly related to Defense."

Can you describe a typical day for you ?

"I don’t have a typical day as my areas of action are very varied, and sometimes it’s international news that sets the pace! However, I do have a small ritual: both in my role as ISSO and as Cyberveille, I start every morning with a quick press review and feed my cyber watch.
I set aside some articles that might be interesting for my daily work and sort what can feed my "general public" monitoring. I post on various networks based on the interest it might generate and write my newsletter every day so that it's ready to be sent at 9.00.a.m."

What do you like/don’t’ like about your job ?

"I think the first thing I like is being proactive, knowing that, at my very small level, I too can make a contribution. Every day, I tell myself that the help, expertise, and awareness I provide about the dangers of the digital world, serves to move things forward. I am lucky enough not to have a job, but to living out a choice I made long before I turned 18, which is to be a soldier. I don't know if that’s the case for many professions.

What I don’t like? Whether it’s online or in real life, eternally negative people. People who criticize or denigrate without adding the slightest bit of value. Pessimists, who will always see the glass as half-empty and who, no matter what you do, can only see the bad side of things. These toxic people are the ones I try to stay away from."

Thank you, Pierre. Do you have any final words ?

"Well, the first thing that comes to mind is to thank you for your invitation. It’s never easy to talk about yourself without it turning into “my life, my work!” 😂

I wish "Cyber IT" all the best, and I hope you won't stop any time soon. Thank you, Arnaud!"

MATTHIEU BILLAUX
Technical director, Consulting and R&D

Hello Matthieu, can you tell me a bit about yourself ?

"Hi, I'm Matthieu, approaching my forties. I am currently the technical director of a consulting and R&D business in offensive security.
I am also the French ambassador for Hack The Box. I am known as euz in various online communities. I love security in all its forms, and I'm also an avid video game player."

Can you tell us about your background ?

"My journey started quite standard but took a less conventional path later. I began with computers at a very young age, playing with one before I could even read. My passion for it was sparked early on. We had internet at home when I was about 8-10 years old and ADSL when I was 12. It was a different era.
In terms of education, I completed my high school diploma in science with an engineering focus "by talent" (meaning I didn't study much as I was too busy playing or developing video games). This was followed by two years of educational wandering: starting an English literature degree and then law school. I eventually decided to buckle down and joined the French Navy, where I served as a non-commissioned officer in IT for 10 years. I discovered cybersecurity during this job and quickly decided to make it my career. Since this was not possible for me in the military at the time, I left after 10 years and started my career in the private sector. Eight years and several jobs later, here I am as a technical director.

What are your daily tasks ?

"I work on many fronts: sales, pre-sales, team management, developing our methodologies, and also completing a quota of missions as an auditor. I also spend a significant part of my time on R&D in the field, mainly focused on malware development and initial access for red team assignments."

What is a typical day like for you ?

"There's not really a typical day, but it often starts with a review of cyber news (monitoring) and checking my emails. Then I prioritize my tasks for the day, followed by several meetings to structure the activity. If I'm on an assignment, I get started on that. After lunch break, we have a brief 15-minutes team meeting to discuss everything and anything and address any sticking points, then we get back to our respective missions."

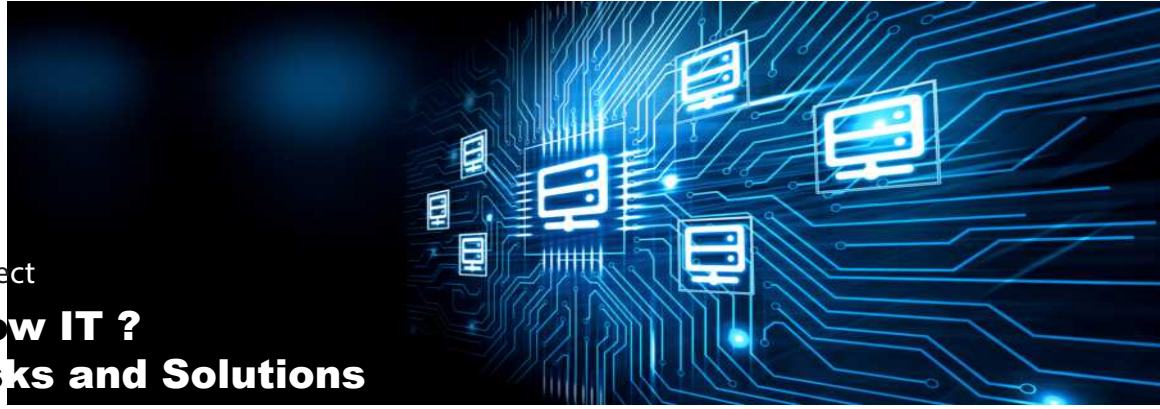
What do you like/don't like about your job ?

"New techniques are discovered every day, and it is both exhilarating and exhausting to keep up with. Days are unfortunately only 24 hours long, which is the biggest issue when you need to be present on all fronts !
But I love the creativity required to achieve our goals, especially during red team missions, which demand a truly holistic vision, and that is fantastic."

Thank you, Matthieu. Any final words ?

"Polypus Pirata Immortalis Est ! (A nod to friends who will recognize themselves)"

Crédit : Halalolo



Article from IT-Connect

What is Shadow IT ? Definition, Risks and Solutions

In this article, we will discuss a widespread phenomenon in most companies that represents a tangible risk and can expose them to cyberattacks: Shadow IT.

We will first define what Shadow IT is, then discuss the risks it poses to an organization. Finally, the last part of the article will focus on analyzing an organization's external attack surface to illustrate the importance of addressing the issues related to Shadow IT.

What is Shadow IT ?

Shadow IT, also known as Rogue IT, can be commonly translated as “ghost computing” or “parallel computing”. This term refers to the use of software and applications without the approval of the IT department. In other words, the IT department is not aware that some users are utilizing these services or applications. This means that the processes for validation and implementation have been bypassed, whether intentionally or not, by the users.

Shadow IT also includes forgotten or unreferenced systems. For example, it can involve a Proof of Concept (PoC) conducted by the IT department itself, in the form of a test environment.
These test systems may remain active well beyond the initial experimentation phase. If they are not properly isolated from the production environment or, worse yet, if they are exposed on the Internet, they can represent considerable risks. Uncontrolled test environments can become entry points for cyberattacks, exposing unsuspected vulnerabilities and compromising the overall security of the organization.

In reality, Shadow IT has become a common phenomenon due to the spread of accessible applications and services. Many modern tools are designed to be extremely user-friendly, allowing users to adopt them quickly without the need for IT department’s intervention. Cloud services, often offered as SaaS (Software as a Service) solutions, are a perfect example of this.

These solutions offer flexibility and easy access like never before, but this same ease can encourage users to bypass official procedures, creating invisible risks for the organization.

However, Shadow IT comes with a series of significant risks, particularly concerning security, compliance, and information management. Unauthorized applications and services may not meet the company's security standards, introducing vulnerabilities exploitable by cybercriminals. Additionally, the lack of centralized control over these tools can complicate data management and regulatory compliance, potentially resulting in penalties for the company. These different aspects of Shadow IT and their implications for organizations will be examined in detail in the next part of this article.

Risks Associated with Shadow IT

Security

By definition, applications deployed without IT department approval will not respect the company's security standards. In other words, they will neither be correctly configured nor secured, and it's possible that this data will not be adequately backed up. Over time, if these applications are not monitored, they can become vulnerable to one or more security flaws. These vulnerabilities can be exploited by cybercriminals, jeopardizing the company's security. This risk is particularly high and critical when it involves systems exposed on the Internet, where threats are everywhere and constantly evolving.

The lack of regular monitoring and maintenance of these applications increases the risk of exploitation by malicious actors. Necessary security updates and patches may not be applied promptly, leaving systems open to attacks. This situation is exacerbated by the fact that uninformed users may also misconfigure applications, thereby creating additional entry points for attacks.
In summary, unsupervised applications constitute a serious threat to the company's IT security and require particular attention to minimize associated risks.

It is crucial to understand that IT security relies on rigorous protocols and meticulous configurations. Unapproved and independently deployed applications bypass these essential controls, exposing the company to potential dangers. The importance of tracking and securing every application used within the organization cannot be understated.

This includes implementing regular backups, applying security updates, and ensuring all configurations adhere to the company's security standards. In the next part of this article, we will explore the measures that companies can take to identify and manage the risks associated with Shadow IT.

Data Management

Beyond the risks related to the lack of security control, such as inadequate configuration and neglected update monitoring, Shadow IT poses a real threat to data management within the organization.

Data can be stored in unsecured locations where proper security measures are not in place. This can include public repositories without authentication, unencrypted connections, or faulty permission management.

Additionally, the company can lose control over the concerned data, not knowing where it is stored or who has access to it.
Eventually, this can lead to data leaks if an unauthorized third-party gains access. Losing control over sensitive data can have severe consequences, both financially and reputationally for the company. Furthermore, this can also lead to violations of data protection regulations, exposing the organization to legal sanctions and significant financial damages.

Therefore, it is imperative for companies to take steps to identify and control Shadow IT to effectively protect their data. This involves implementing clear security policies and using advanced monitoring tools to detect any unauthorized activity.
Besides, raising employee awareness about the risks associated with Shadow IT is essential to promote a security-conscious culture within the organization.

Compliance and GDPR

There is also a close link between the concept of compliance and Shadow IT, particularly regarding GDPR. GDPR (General Data Protection Regulation) is a European Union legislation designed to protect the personal data of EU citizens. It requires strict and precise tracking of personal data processed by companies.

This means the organization must know exactly where the data is stored and who has access to it. These requirements are in direct contradiction with the issue of Shadow IT, where data can be stored on unapproved and potentially non-GDPR-compliant systems. In the event of a data breach, the company can be held liable and face severe sanctions, including substantial fines. GDPR compliance also involves demonstrating that adequate protective measures are in place, which is challenging to ensure when uncontrolled applications are used.

Beyond GDPR obligations, compliance also includes managing licenses and adhering to the terms of use for services or applications. Using unlicensed software or violating terms of use exposes the company to legal and financial risks. Shadow IT complicates this management, as applications deployed without IT department's approval often escape necessary controls to ensure compliance with licenses and terms of use.

It is crucial for companies to implement rigorous measures to detect and control Shadow IT to ensure compliance with regulations like GDPR. This can include using monitoring tools to identify unauthorized applications and training employees on the risks and legal obligations associated with unapproved software use. In the next section, we will discuss strategies that organizations can adopt to manage and mitigate the risks associated with Shadow IT while ensuring regulatory compliance.

External Attack Surface Analysis

Security

Given the risks posed by Shadow IT, it is crucial for companies to take necessary measures to protect their data. Beyond implementing strict procedures, an organization can adopt an External Attack Surface Management (EASM) tool to obtain a precise mapping of assets exposed on the Internet. These assets represent a significant risk and can be used as initial attack vectors, in the same way as phishing emails.

Using EASM offers several advantages to fight against Shadow IT:

Identification of Unauthorized Assets : The analysis performed by the EASM tool identifies all assets associated with an organization, whether authorized or not. This proactive analysis helps uncover systems, applications, and services used without the IT department approval. It reveals the elements of Shadow IT and helps understand their scope.

Continuous Monitoring : The regular discovery process of the EASM solution ensures continuous monitoring. This is crucial to minimize the time between when an asset goes online and when it is detected. Thus, the organization, through its technical team, can react quickly to minimize risks. Continuous monitoring maintains constant visibility over new assets and promptly addresses potential issues.

Risk Assessment : Each identified asset is reviewed and evaluated to determine potential risks associated with it. This assessment identifies weaknesses, such as configuration issues and vulnerabilities, similar to what a pentester would do. By knowing the specific risks associated with each asset, the organization can take appropriate corrective measures to enhance security.

By integrating an EASM solution, companies can better control and secure their IT environment while detecting and mitigating risks related to Shadow IT. External attack surface analysis becomes an indispensable tool for maintaining security and compliance while minimizing exploitable attack vectors by cybercriminals. In the next section, we will examine best practices for effectively implementing and using an EASM solution to protect the company's assets.

By identifying vulnerabilities and risks associated with each exposed system and service, the EASM tool helps you take necessary actions and make the right decisions. In the case of Shadow IT, this may involve deactivating the unauthorized systems or retaining the system provided its configuration is revised (e.g., by strengthening system security or applying hardening measures).

The EASM tool not only detects non-compliant assets but also prioritizes actions based on the risk level associated with each asset. With a clear view of vulnerabilities, the organization can develop an effective and targeted response plan. For example, critical or highly exposed systems can be addressed first to quickly mitigate major risks.

Also, using EASM enhances the overall security posture of the company by integrating robust security practices and ensuring continuous monitoring. This proactive approach helps anticipate threats and reduce potential attack surfaces, thereby intensifying protection of the organization's data and resources.

sweepatic SECURITY

In addition to external attack surface analysis, organizations can track Shadow IT through:

Employee training to inform them about the risks associated with Shadow IT, and to explain internal validation processes of the company. For example, the policy they should follow when they request access to an application or service. This applies equally to the IT department itself: no shortcuts, and they must ensure proper application of these processes.

Device and authorization management: Mobile devices and applications management tools can help deploy applications and enforce policies to grant or deny certain actions. This can also control which devices and applications have access to the organization's data.

Network & systems monitoring and auditing to detect unusual flows and events.

Dialogue between the IT department, employees, and department leaders plays a crucial role beyond technical solutions. For example, the origin of Shadow IT might be related to disputes between an employee and the IT department.

EASM screenshot

Shadow IT must be taken very seriously. We should not turn a blind eye to this inherently covert aspect of IT. On the contrary, it is crucial to highlight the services, applications, and systems used without the IT team's approval in order to make the right decisions. Proactively discovering these elements allows for identifying and managing potential risks before they become problematic.

In addition to identifying and managing unauthorized assets, it is also important to implement strategies to reduce the temptation for users to resort to Shadow IT. This can be achieved through employee training and awareness. By informing users about the risks associated with using unapproved software and explaining the policies to follow to obtain necessary tools, the organization can reduce reliance on Shadow IT.

Listening to the users' needs is also essential. Understanding why employees turn to unauthorized solutions, can allow the IT team to find and provide approved alternatives that meet their needs in the best way. Involving users in the tool selection and validation process is important so the organization can create a safer and more collaborative work environment.

In conclusion, taking Shadow IT seriously involves a proactive approach to identify and manage unauthorized assets, as well as a strategy for awareness and training to limit its occurrence.

From Florian BURNEL

About the author

FLORIAN BURNEL

System and network engineer, co-founder of IT-Connect, and Microsoft MVP in "Cloud and Datacenter Management".

I want to share my experience and discoveries through my articles. I have a broad expertise with a particular focus on Microsoft solutions and scripting.

IT-CONNECT FR

Cyber is a marathon not a sprint !

Source : Europol.europa.eu

Behind the scenes of Europol's «EndGame» operation

The largest operation ever conducted against botnets.

The international operation disrupted several malware programs.

Between May 27 and May 29, 2024, Operation Endgame, orchestrated from Europol's headquarters, targeted droppers such as IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee, and Trickbot. The actions aimed to disrupt criminal services by targeting high-value targets, dismantling illegal infrastructures, and freezing illicit revenues.

This strategy had a global impact on the dropper ecosystem. The malware whose infrastructure was destroyed during the operation days facilitated ransomware attacks and other types of malware.

Following these interventions, eight fugitives linked to these criminal activities, sought by Germany, were added to Europe's most wanted list on May 30, 2024. These individuals are accused of involvement in serious cybercrime activities.

This operation is the largest ever conducted against botnets, crucial for deploying ransomware. It was launched and led by France, Germany, and the Netherlands, with the support of Eurojust (the European union agency for Criminal Justice Cooperation), and involved Denmark, the United Kingdom, and the United States.

Armenia, Bulgaria, Lithuania, Portugal, Romania, Switzerland, and Ukraine also participated through various actions, including arrests, interrogations, searches, and the seizure or removal of servers and domains

Many private partners, both national and international, provided their support, including Bitdefender, Cryptolaemus, Sekoia, Shadowserver, Team Cymru, Prodaft, Proofpoint, NFIR, Computest, Northwave, Fox-IT, HaveIBeenPwned, Spamhaus, DIVD, abuse.ch, and Zscaler.

EndgGame key results :

4 arrests (1 in Armenia and 3 in Ukraine)

16 police searches (1 in Armenia, 1 in the Netherlands, 3 in Portugal, and 11 in Ukraine)

Over 100 servers seized or disrupted in Bulgaria, Canada, Germany, Lithuania, the Netherlands, Romania, Switzerland, the United Kingdom, the United States, and Ukraine

More than 2,000 domains placed under law enforcement control

Additionally, investigations revealed that one of the main suspects had earned at least 69 million Euros in cryptocurrency by renting out criminal infrastructure for the deployment of ransomware. Transactions involving this suspect are under constant surveillance, and legal authorization to seize these assets during future actions has already been obtained.

EUROPOL

What is a dropper and how does it work ?

Malware droppers are programs designed to install other malware on a target system. Used at the beginning of an attack, they enable cybercriminals to bypass security measures and deploy harmful programs such as viruses, ransomware, or spyware. While droppers themselves do not directly cause damage, they are essential for infecting systems with malicious software.

SystemBC provides anonymous communication between an infected system and command-and-control servers. Bumblebee, is often distributed through phishing campaigns or compromised websites, it facilitates the delivery and execution of additional payloads on compromised systems.

SmokeLoader acts as a downloader to install other malware on infected systems.
IcedID (also known as BokBot) is initially a banking Trojan, it has evolved to support various cybercrimes beyond financial data theft.

Pikabot is a trojan used to gain initial access to infected computers, enabling the deployment of ransomware, remote control, and data theft.
All these droppers are used to deploy ransomware and represent a significant threat in the infection chain.

Meeting room of Operation "Endgame"

The end of the game is not here yet

Operation Endgame is not concluding today. New initiatives will soon be announced on the Operation Endgame website. The individuals involved in these botnets, as well as other activities not yet apprehended, will be directly called to account for their actions.

Droppers operating phases

Infiltration : Droppers can penetrate systems through various channels such as email attachments, compromised websites, and they can also be associated with legitimate software.

Execution : Once executed, the dropper installs additional malware on the victim's computer. This installation often occurs without the user's knowledge or consent.

Evasion : Droppers are designed to avoid detection by security software. They may use methods such as hiding their code, executing it in memory without saving it to disk, or impersonating legitimate software processes.

Payload delivery : After deploying additional malicious software, the dropper may either remain inactive or self-delete to escape detection, allowing the payload to perform its intended malicious activities.

A command center at Europol to coordinate operations

Europol facilitated information exchange and provided analytical, cryptographic tracing, and forensic support to the investigation. To coordinate the operation, over 50 coordination meetings were held with all participating countries, as well as an operational sprint at Europol headquarters.

Over 20 law enforcement agents from Denmark, France, Germany, and the United States supported coordination from Europol's command center, with hundreds more in the field. A virtual command center also enabled real-time coordination among Armenian, French, Portuguese, and Ukrainian officers.

Europol's command center facilitated the exchange of information on seized servers, suspects, and data transfers, with local command centers established in several countries. Eurojust (the European union agency for Criminal Justice Cooperation) also contributed by setting up a coordination center for judicial cooperation, supporting the execution of European arrest warrants and investigation orders.

EUROJUST

July/September 2024

CREDITS

Editor-in-Chief : **Arnaud LEROY**
Graphic Design : **Arnaud LEROY**
English Translation : **Maëva ASTORGA**

We thank all contributors and partners for their support and collaboration on this issue.