aDvens

Security for the greater good

Monthly Cyber Threat Intelligence report December 2024

CERT aDvens

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

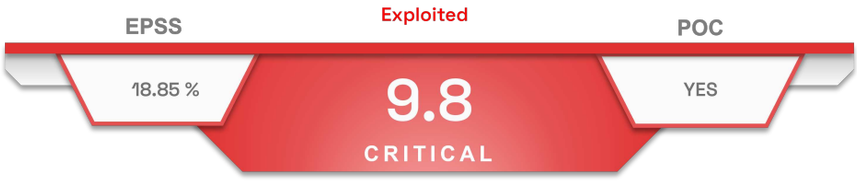
This month, the CERT aDvens presents :

- Three vulnerabilities of interest, in addition to those already published,
- A cyber-psychological analysis of the use of Artificial Intelligence in cybercrime, based on the *Solaria* tool,
- A presentation of the Emmenhtal loader.

2. VULNERABILITIES

This month, aDvens' CERT highlights **three** vulnerabilities affecting technologies frequently used within companies.
They are presented in order of severity (proofs of concept available, exploitation...). Applying their patches or workarounds is strongly recommended.

3. ZYXEL - CVE-2024-11667



A directory traversal vulnerability has been identified in the web management interface of the following firmware series: Zyxel ATP (versions V5.00 to V5.38), USG FLEX (versions V5.00 to V5.38), USG FLEX 50(W) (versions V5.10 to V5.38), and USG20(W)-VPN (versions V5.10 to V5.38). This flaw could allow an attacker to exploit a crafted URL to download or upload unauthorised files.

According to researchers from Sekoia, the Helldown ransomware group, which emerged in August 2024, exploited this vulnerability to compromise companies.

3.1. Type of Vulnerability

- **CWE-22**: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

3.2. Risk

- Arbitrary code execution

3.3. Severity (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

3.4. Affected Products

- ATP series firmware versions V5.00 to V5.38
- USG FLEX series firmware versions V5.00 to V5.38
- USG FLEX 50(W) series firmware versions V5.00 to V5.38
- USG20(W)-VPN series firmware versions V5.00 to V5.38

3.5. Recommendations

- Update products to version 5.39 or later.
- Additional information is available in Zyxel's advisory.

3.6. Proof of Concept

A proof of concept is available in open sources.

4. FORTINET - CVE-2023-34990

A *relative path traversal* in Fortinet FortiWLM version 8.6.0 to 8.6.5 and 8.5.0 to 8.5.4 allows an attacker to execute unauthorised code or commands via specially crafted web requests.

The research team HORIZON3 has published a proof of concept detailing the technical aspects of this vulnerability.

4.1. Type of Vulnerability

- **CWE-23**: Relative Path Traversal

4.2. Risk

- Arbitrary code execution

4.3. Severity (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

4.4. Affected Products

- FortiWLM version 8.6.5 and prior
- FortiWLM version 8.5.4 and prior

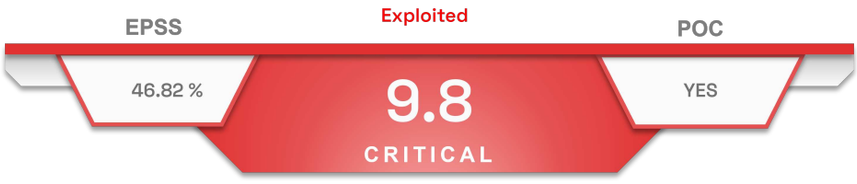
4.5. Recommendations

- Update FortiWLM to version 8.6.6 or later.
- Update FortiWLM to version 8.5.5 or later.
- Additional information is available in Fortinet's advisory.

4.6. Proof of Concept

A proof of concept is available in open sources.

5. PROJECTSEND - CVE-2024-11680



ProjectSend versions prior to r1720 are affected by an improper authentication vulnerability. Remote and unauthenticated attackers can exploit this flaw by crafting HTTP requests to the options.php resource, enabling unauthorised modification of the application's configuration. Successful exploitation allows attackers to create accounts, upload webshells and inject malicious JavaScript code.

Security researchers from VulnCheck have observed that 99% of the observed instances are vulnerable. Exploit scripts for the vulnerability are available in open sources.

5.1. Type of Vulnerability

- **CWE-287**: Improper Authentication

5.2. Risk

- Bypassing security policy

5.3. Severity (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

5.4. Affected Products

- ProjectSend versions prior to r1720

5.5. Recommendations

- Update ProjectSend to version r1720 or later.
- Additional information is available in ProjectSend's advisory.

5.6. Proof of Concept

A proof of concept is available in open sources.

6. CYBER-PSYCHOLOGY AND CYBER-CRIMINOLOGY: UNDERSTANDING THE CRIMINAL EXPLOITATION OF ARTIFICIAL INTELLIGENCE

6.1. Foreword

This article proposes to explore and understand the phenomenon of the exploitation of Artificial Intelligence (AI) by cybercriminals. It also introduces the *Solaria* tool (Version 1.0), designed to help cybersecurity analysts and cyber-psychologists clarify and concisely describe AI-augmented cyberattacks.

6.2. A new era

The emergence and democratisation of Artificial Intelligence (AI) is profoundly transforming the digital landscape. While this technology opens up promising prospects, it also provides cybercriminals with powerful tools to design new attacks. AI-augmented cyberattacks, such as sophisticated phishing or standalone ransomware, are characterised by their effectiveness, adaptability and ability to defeat traditional security systems.

By leveraging automation and analysis of vast data sets, AI allows these attacks to target complex systems with unprecedented speed, while identifying specific vulnerabilities in digital infrastructures. This evolution represents a decisive turning point in cybersecurity, requiring the adoption of innovative strategies and dedicated tools to face increasingly advanced threats.

With this in mind, Solaria (Version 1.0) has been designed to support cybersecurity analysts and cyber-psychologists. This innovative tool enables the precise identification and analysis of AI-enabled cyberattacks. Solaria aims to offer deep insights into the tactics of cybercriminals, while also contributing to the development of defenses tailored to the evolving landscape of digital threats.

6.3. Famous cases of AI-augmented cyberattacks

2020: Hacking passwords with neural networks

In February 2020, tools based on neural networks and accessible on underground forums were used to analyse gigantic databases of hacked passwords. These tools generated password variations with increased precision, making brute force attacks much more effective (ActuIA, 2022).

2024: Voice and visual identity theft

In 2024, cybercriminals leveraged artificial intelligence to create convincing fake videos featuring Elon Musk. These deepfakes, distributed on Facebook and TikTok, conveyed promotional messages about investments in cryptocurrency. By manipulating their victims with plausible scenarios and Musk's image, the attackers lured them into investing sums of money in sophisticated scams (CBS, 2024).

6.4. A phenomenon based on opportunity

Developed by Marcus Felson and Lawrence E. Cohen in 1979, the Routine Activity Theory helps explain and better understand the phenomenon of malicious exploitation of AI by cybercriminals.

This theory suggests that the probability of crime increases according to the convergence of three components: **a motivated criminal**, **an appropriate target** and **ineffective or weak protection**.

In the context of AI, the increasing accessibility of advanced technologies, combined with everyday use of IT systems, creates new opportunities for cybercriminals. AI, now available and easily integrated into automated tools, allows attackers to maximise the effectiveness of their actions, such as precisely target victims or exploit security vulnerabilities. Routine user activities, such as browsing the Internet or using online services, provide cybercriminals with a wide range of potential targets. Furthermore, weak monitoring of AI-powered malicious actions, often camouflaged behind complex algorithms, reduces the risks of detection and increases opportunities for attackers. Thus, the combination of technical opportunities offered by AI and the daily behaviors of users favours the malicious exploitation of these technologies.

Figure 1. R-A-T: Routine Activity Theory - 1979

Some key things to remember:

- Felson and Cohen proposed the idea that the level of crime is closely related to the structural organisation of society.
- Although societal transformations can improve the quality of modern life, they can also create favourable conditions for increased crime.
- The democratisation of AI, as an opportunity, can be considered as a favourable condition for the increase in crime.

Figure 2. CTI: September 2024 monthly advisory

A more detailed explanation of the theory is available in the CTI's monthly advisory (September 2024), chapter: *Psychology / Cyber-psychology - Three models for understanding the vulnerability of users to phishing*.

6.5. Typology of cybercriminals

To understand the malicious exploitation of AI, it is essential to understand the typical profile of cybercriminals. Generally speaking, the study of cybercriminals shows that they can be classified into **six distinct groups** according to Norton's typology (Cleary & Norton, 2024).

→ **1 - Hackers**

A hacker is a person who penetrates a computer system by exploiting its vulnerabilities, using various tools and malware (Kaspersky, 2024). Malicious hackers are called black hats. In contrast, ethical hackers, who work to secure systems, are known as white hats. Finally, those who navigate between legal and illegal actions, sometimes breaking laws or ethical standards, are referred to as Grey Hats.

→ **2 - Scammers**

Scammers use social engineering tactics to steal information or money. Scammers frequently exploit fraudulent software such as scareware, malware designed to trick users into visiting malicious websites (Cleary, 2024).

→ **3 - Hacktivists**

Hacktivites seek to gain unauthorised access to computer systems or networks, often guided by political or social motivations (Checkpoint, 2024). Hacktivism, also called cyberactivism, is a particularly active form of activism in China, notably illustrated by the famous collective Honker Union.

→ **4 - Disgruntled employee**

They aim to inflict financial damage and tarnish the reputation of the organisation for which they work or have worked (Cleary, 2024). Among the behaviors observed, disgruntled employees develop a script hidden in the system, a logic bomb, programmed to activate a certain time after their departure from the company. Once triggered, this logic bomb executes a series of malicious actions aimed at sabotaging production.

→ **5 - APT - Advanced and persistent threats**

State actors are state-sponsored cybercriminals with exceptional skill levels and advanced technical expertise. They benefit from privileged access to sophisticated tools as well as academic and confidential knowledge (Cleary, 2024). As an example, to carry out fraudulent transactions during the cyber-heist of the Bangladesh bank in February 2016, APTs Lazarus and 38 had access to the bank's confidential information and the SWIFT system.

→ **6 - Script kiddies**

Script Kiddies are novice cybercriminals with low levels of experience and knowledge. They simply use tools and malware created by others (Cleary, 2024). It is common for cyber-sabotage campaigns to be carried out using tools with simple graphical interfaces, requiring no technical expertise. In the past, one of the most famous tools was LOIC, used for DDoS attacks. Today, another widely used tool is DDoSia, which appeals to both script kiddies and hacktivists.

6.6. The use of AI-enable cyberattacks by cybercriminals

This section explores various articles and reports published between 2023 and 2024, addressing the malicious exploitation of AI by the six types of cybercriminals.

6.6.1. Hackers - Behaviors observed

Worm GPT

On 13 July 2023, *Slashnext* published the article WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks in which researchers describe the discovery of an arsenal augmented by AI: Worm GPT. This arsenal has been identified as useful specifically for malicious purposes such as phishing, Business Email Compromise (BEC) attacks and malware creation (Slashnext, 2023).

Finally, in the third image above, we see that malicious actors are now creating their own custom modules similar to ChatGPT, but easier to use for nefarious purposes. Not only are they creating these custom modules, but they are also advertising them to fellow bad actors. This shows how cybersecurity is becoming more challenging due to the increasing complexity and adaptability of these activities in a world shaped by AI.

Uncovering WormGPT: A Cybercriminal's Arsenal

Our team recently gained access to a tool known as "WormGPT" through a prominent online forum that's often associated with cybercrime. This tool presents itself as a blackhat alternative to GPT models, designed specifically for malicious activities.

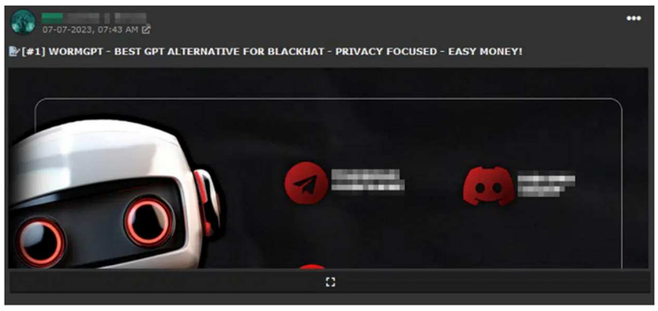


Figure 3. Slashnext, 2023

Increasing the efficiency of cyberattacks

On 24 January 2024, the English National Cyber Security Center (NCSC) published an article in which the malicious exploitation of AI by hackers is discussed in order to increase the efficiency of recognition, phishing and the development of ransomware.

4. AI's ability to summarise data at pace will also highly likely enable threat actors to identify high-value assets for examination and exfiltration, enhancing the value and impact of cyber attacks over the next two years.

5. Threat actors, including ransomware actors, are already using AI to increase the efficiency and effectiveness of aspects of cyber operations, such as reconnaissance, phishing and coding. This trend will almost certainly continue to 2025 and beyond. Phishing, typically aimed either at delivering malware or stealing password information, plays an important role in providing the initial network accesses that cyber criminals need to carry out ransomware attacks or other cyber crime. It is therefore likely that cyber criminal use of available AI models to improve access will contribute to the global ransomware threat in the near term.

Figure 4. NCSC - National Cyber Security Centre, 2024

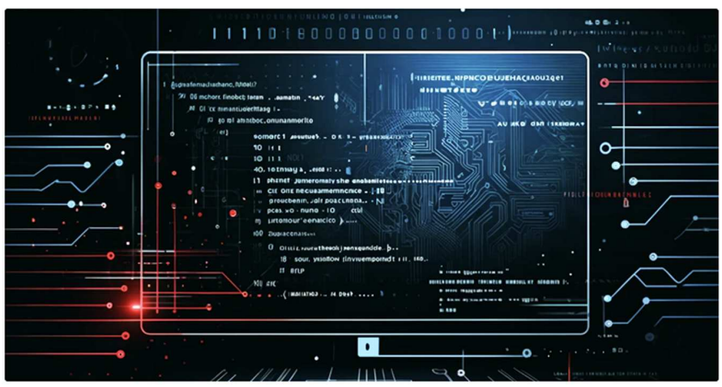
6.6.2. APT - Behaviors observed

APT Kimsuky perfects its targeted phishing campaigns

According to Microsoft, North Korean state actors are exploiting AI to increase the efficiency of their operations (Lakshmanan; Microsoft, 2024). For example, the APT Kimsuky group relies on AI to scale up its targeted phishing attacks.

Microsoft Warns: North Korean Hackers Turn to AI-Fueled Cyber Espionage

Apr 22, 2024 Ravie Lakshmanan Cryptocurrency / Artificial Intelligence



Microsoft has revealed that North Korea-linked state-sponsored cyber actors have begun to use artificial intelligence (AI) to make their operations more effective and efficient.

"They are learning to use tools powered by AI large language models (LLM) to make their operations more efficient and effective," the tech giant said in its latest report on East Asia hacking groups.

The company specifically highlighted a group named Emerald Sleet (aka Kimusky or TA427), which has been observed using LLMs to bolster spear-phishing efforts aimed at Korean Peninsula experts.

Figure 5. Lakshmanan, 2024

Emerald Sleet's use of LLMs has been in support of this activity and involved research into think tanks and experts on North Korea, as well as the generation of content likely to be used in spear-phishing campaigns. Emerald Sleet also interacted with LLMs to understand publicly known vulnerabilities, to troubleshoot technical issues, and for assistance with using various web technologies. Based on these observations, we map and classify these TTPs using the following descriptions:

- **LLM-assisted vulnerability research:** Interacting with LLMs to better understand publicly reported vulnerabilities, such as the CVE-2022-30190 Microsoft Support Diagnostic Tool (MSDT) vulnerability (known as "Follina").
- **LLM-enhanced scripting techniques:** Using LLMs for basic scripting tasks such as programmatically identifying certain user events on a system and seeking assistance with troubleshooting and understanding various web technologies.
- **LLM-supported social engineering:** Using LLMs for assistance with the drafting and generation of content that would likely be for use in spear-phishing campaigns against individuals with regional expertise.
- **LLM-informed reconnaissance:** Interacting with LLMs to identify think tanks, government organizations, or experts on North Korea that have a focus on defense issues or North Korea's nuclear weapon's program.

Figure 6. Microsoft, 2024 - Staying ahead of threat actors in the age of AI

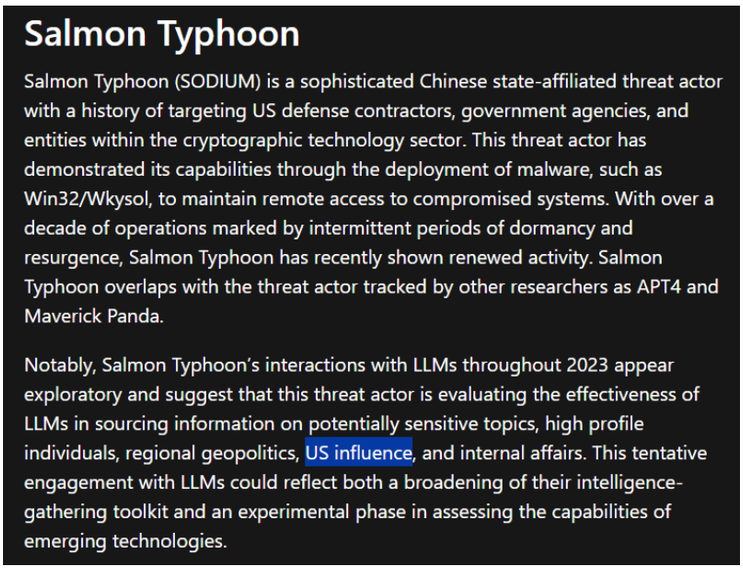
China: influence operation (psychological warfare)

Other states, such as China, are also using AI for malicious purposes, including to produce content for psychological warfare campaigns.

The adversary is also said to have relied on the latest advancements in AI to research vulnerabilities and conduct reconnaissance on organizations and experts focused on North Korea, joining hacking crews from China, who have turned to AI-generated content for influence operations.

It further employed LLMs to troubleshoot technical issues, conduct basic scripting tasks, and draft content for spear-phishing messages, Redmond said, adding it worked with OpenAI to disable accounts and assets associated with the threat actor.

Figure 7. Lakshmanan, 2024



Salmon Typhoon

Salmon Typhoon (SODIUM) is a sophisticated Chinese state-affiliated threat actor with a history of targeting US defense contractors, government agencies, and entities within the cryptographic technology sector. This threat actor has demonstrated its capabilities through the deployment of malware, such as Win32/Wkysol, to maintain remote access to compromised systems. With over a decade of operations marked by intermittent periods of dormancy and resurgence, Salmon Typhoon has recently shown renewed activity. Salmon Typhoon overlaps with the threat actor tracked by other researchers as APT4 and Maverick Panda.

Notably, Salmon Typhoon's interactions with LLMs throughout 2023 appear exploratory and suggest that this threat actor is evaluating the effectiveness of LLMs in sourcing information on potentially sensitive topics, high profile individuals, regional geopolitics, US influence, and internal affairs. This tentative engagement with LLMs could reflect both a broadening of their intelligence-gathering toolkit and an experimental phase in assessing the capabilities of emerging technologies.

Figure 8. Microsoft, 2024 - Staying ahead of threat actors in the age of AI

6.6.3. Script kiddies - Behaviors observed

Malware Development

In June 2024, HP Wolf Security reported the emergence of attackers with limited technical skills leveraging AI to create malware.

Generative AI assisting malware developers in the wild

In early June, HP Sure Click isolated an unusual French email attachment posing as an invoice. The attachment is simply an HTML file which, when opened in the browser, asks for a password. An initial analysis of the code revealed that this is an HTML smuggling threat (T1027.006).[16] But in contrast to most other threats of this kind, the payload stored inside the HTML file was not encrypted inside an archive. Rather, the file was encrypted within the JavaScript code itself. The attackers encrypted the file using AES and implemented it without making any mistakes, meaning decrypting the file is only possible with the correct password (T1027.013).[17]

While we did not have the email body, based on various clues in the code, we knew that the decrypted file must be a ZIP archive. We also assumed that the password would not be too complex. As a result, we were able to carry out a brute-force attack in a reasonable amount of time and successfully recover the correct password.

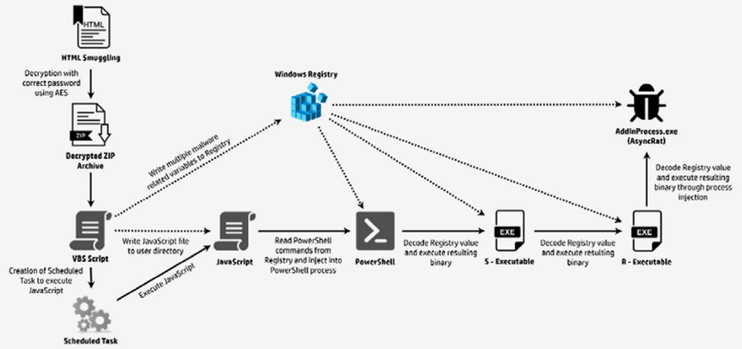


Figure 5 - Infection chain leading to AsyncRAT

The decrypted archive contains a VBScript file (T1059.005).[3] When run, the infection chain starts and ultimately deploys AsyncRAT, a remote access trojan (RAT). The VBScript writes various variables to the Windows Registry (T1112), which are reused later in the chain.[18] A JavaScript file (T1059.007) dropped into the user directory is then run by a scheduled task (T1053.005).[4] [19] This script reads the first variable, a PowerShell script (T1059.001),[20] from the Registry and injects it into a newly started PowerShell process. The PowerShell script then makes use of the other Registry variables and runs two more executables, which start the malware payload after injecting it into a legitimate process (T1055).[21]

AsyncRAT is an open-source RAT used for controlling the victim's computer. Since it's so easy to obtain, all the threat actor needs to do is develop an infection chain to deliver and install the malware.

Interestingly, when we analyzed the VBScript and the JavaScript, we were surprised to find that the code was not obfuscated. In fact, the attacker had left comments throughout the code, describing what each line does – even for simple functions. Genuine code comments in malware are rare because attackers want to their make malware as difficult to understand as possible.

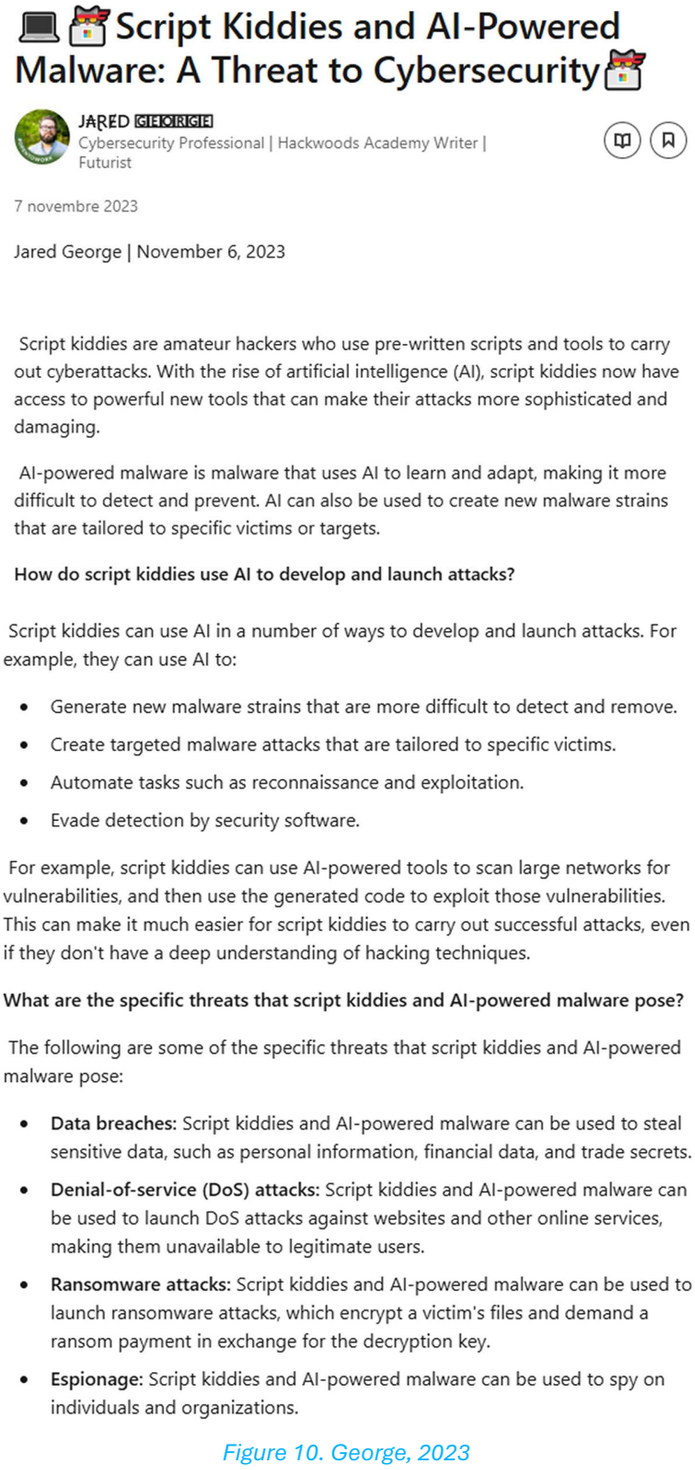
Based on the scripts' structure, consistent comments for each function and the choice of function names and variables, we think it's highly likely that the attacker used GenAI to develop these scripts (T1588.007).[5] The activity shows how GenAI is accelerating attacks and lowering the bar for cybercriminals to infect endpoints.

```
// Arrête un processus PowerShell en cours d'exécution
function arreterProcessusAvecPowerShell() {
    // Exécution de PowerShell
    shellWsh.Run(cheminPowerShell, 2);
```

Figure 9. HP Wolf Security, 2024

Sophistication of techniques for circumventing antiviral solutions

Cybersecurity experts have also shed light on script kiddies' use of AI to automate reconnaissance and exploitation processes, while developing sophisticated techniques to circumvent detection by security software (George, 2023).



Script Kiddies and AI-Powered Malware: A Threat to Cybersecurity

JARED GEORGE
Cybersecurity Professional | Hackwoods Academy Writer | Futurist

7 novembre 2023

Jared George | November 6, 2023

Script kiddies are amateur hackers who use pre-written scripts and tools to carry out cyberattacks. With the rise of artificial intelligence (AI), script kiddies now have access to powerful new tools that can make their attacks more sophisticated and damaging.

AI-powered malware is malware that uses AI to learn and adapt, making it more difficult to detect and prevent. AI can also be used to create new malware strains that are tailored to specific victims or targets.

How do script kiddies use AI to develop and launch attacks?

Script kiddies can use AI in a number of ways to develop and launch attacks. For example, they can use AI to:

- Generate new malware strains that are more difficult to detect and remove.
- Create targeted malware attacks that are tailored to specific victims.
- Automate tasks such as reconnaissance and exploitation.
- Evade detection by security software.

For example, script kiddies can use AI-powered tools to scan large networks for vulnerabilities, and then use the generated code to exploit those vulnerabilities. This can make it much easier for script kiddies to carry out successful attacks, even if they don't have a deep understanding of hacking techniques.

What are the specific threats that script kiddies and AI-powered malware pose?

The following are some of the specific threats that script kiddies and AI-powered malware pose:

- **Data breaches:** Script kiddies and AI-powered malware can be used to steal sensitive data, such as personal information, financial data, and trade secrets.
- **Denial-of-service (DoS) attacks:** Script kiddies and AI-powered malware can be used to launch DoS attacks against websites and other online services, making them unavailable to legitimate users.
- **Ransomware attacks:** Script kiddies and AI-powered malware can be used to launch ransomware attacks, which encrypt a victim's files and demand a ransom payment in exchange for the decryption key.
- **Espionage:** Script kiddies and AI-powered malware can be used to spy on individuals and organizations.

Figure 10. George, 2023

6.6.4. Scammers - Behaviors observed

Sophistication of the CEO scam

New attacks include sophisticated schemes, such as fake payment redirects, where fraudsters pose as company executives to deceive their victims with disturbing realism (National Senior Australia, 2024).

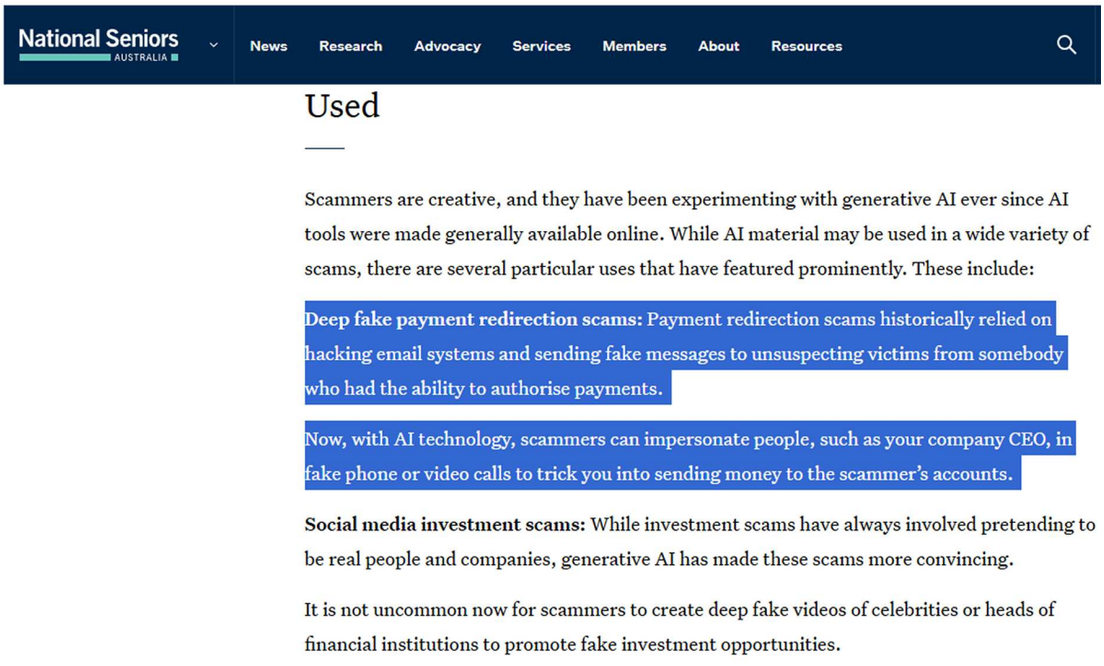


Figure 11. National Senior Australia, 2024

Social networks as information bases

Scammers leverage AI to deeply analyse online media and social networks, allowing them to design highly personalised targeted phishing attacks (Madison Information Technology, 2024).

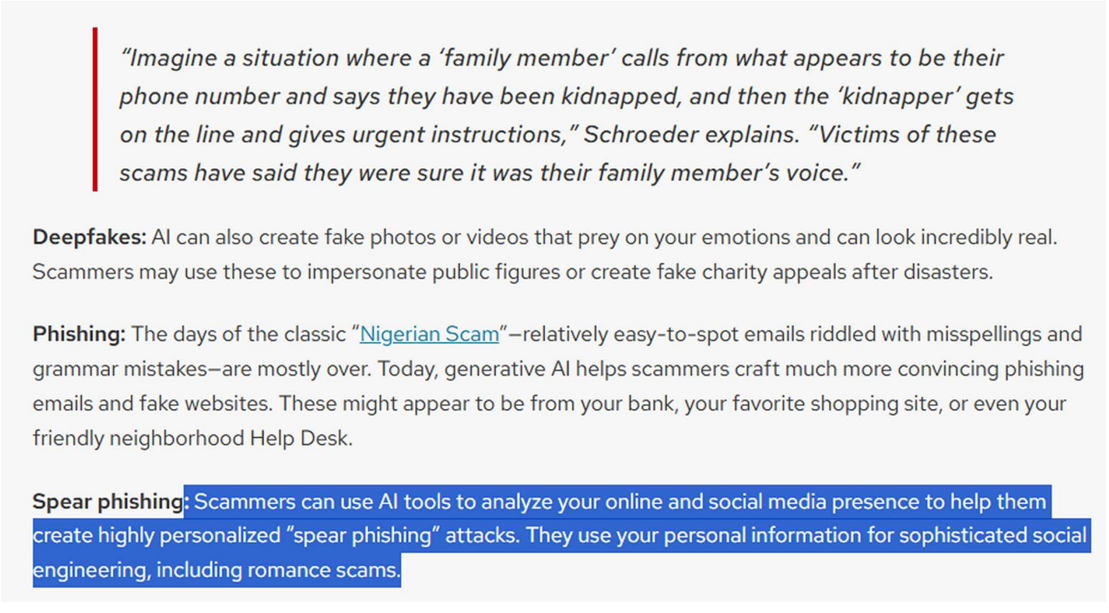


Figure 12. Madison Information Technology, 2024

6.6.5. Disgruntled employee - Behaviors observed

Voice imitation

In April 2024, a disgruntled former athletic director used AI to generate racist content with voice messages similar to the high school principal's voice (ABC7 Chicago Digital Team, 2024).

ARTIFICIAL INTELLIGENCE

Disgruntled ex-athletic director used AI to generate fake racist rant in principal's voice: police

By ABC7 Chicago Digital Team
Friday, April 26, 2024

BALTIMORE COUNTY, Maryland (WLS) -- Baltimore County police said a disgruntled ex-athletics director used AI to frame his high school's principal by generating a fake recording of racist rant in his voice.

Police Chief Robert McCullough said his department worked with the FBI and forensic experts from the University of California at Berkeley to investigate the recording that was originally circulated on social media in January 2024.

The audio recording purported to capture Pikesville High School principal Eric Eiswert "spewing racial and antisemitic insults about staff and students," WMAR-TV reported.

McCullough announced Thursday that their investigation found that "Dazhon Darien, the school's athletic director, produced the recording to retaliate against Principal Eiswert, who had initiated a probe into the mishandling of school funds."

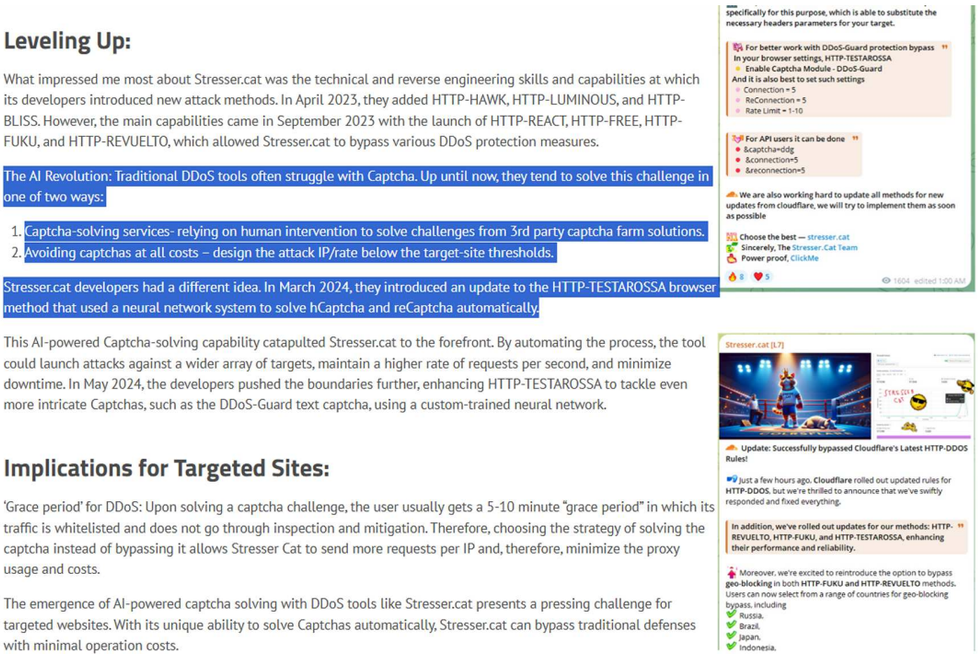
Darien was arrested at BWI Thurgood Marshall Airport Thursday morning, McCullough said, on an outstanding warrant. He now faces charges that include stalking, disruption of school operations and retaliation against a witness. He is currently in custody and being held on $5,000 bond.

Figure 13. ABC7 Chicago Digital Team, 2024

6.6.6. Hacktivists - Behaviors observed

Integration of AI in solving captchas

The article *The hacktivist-friendly AI-based DDoS Tool was trained to solve Captchas* written by Arik Atar, published on 24 June 2024, describes the exploitation of AI by hacktivists for the resolution of *captchas* during DDoS (Distributed Denial of Service) campaigns.



Leveling Up:

What impressed me most about Stresser.cat was the technical and reverse engineering skills and capabilities at which its developers introduced new attack methods. In April 2023, they added HTTP-HAWK, HTTP-LUMINOUS, and HTTP-BLISS. However, the main capabilities came in September 2023 with the launch of HTTP-REACT, HTTP-FREE, HTTP-FUKU, and HTTP-REVUELTO, which allowed Stresser.cat to bypass various DDoS protection measures.

The AI Revolution: Traditional DDoS tools often struggle with Captcha. Up until now, they tend to solve this challenge in one of two ways:

1. Captcha-solving services- relying on human intervention to solve challenges from 3rd party captcha farm solutions.
2. Avoiding captchas at all costs – design the attack IP/rate below the target-site thresholds.

Stresser.cat developers had a different idea. In March 2024, they introduced an update to the HTTP-TESTAROSSA browser method that used a neural network system to solve hCaptcha and reCaptcha automatically.

This AI-powered Captcha-solving capability catapulted Stresser.cat to the forefront. By automating the process, the tool could launch attacks against a wider array of targets, maintain a higher rate of requests per second, and minimize downtime. In May 2024, the developers pushed the boundaries further, enhancing HTTP-TESTAROSSA to tackle even more intricate Captchas, such as the DDoS-Guard text captcha, using a custom-trained neural network.

Implications for Targeted Sites:

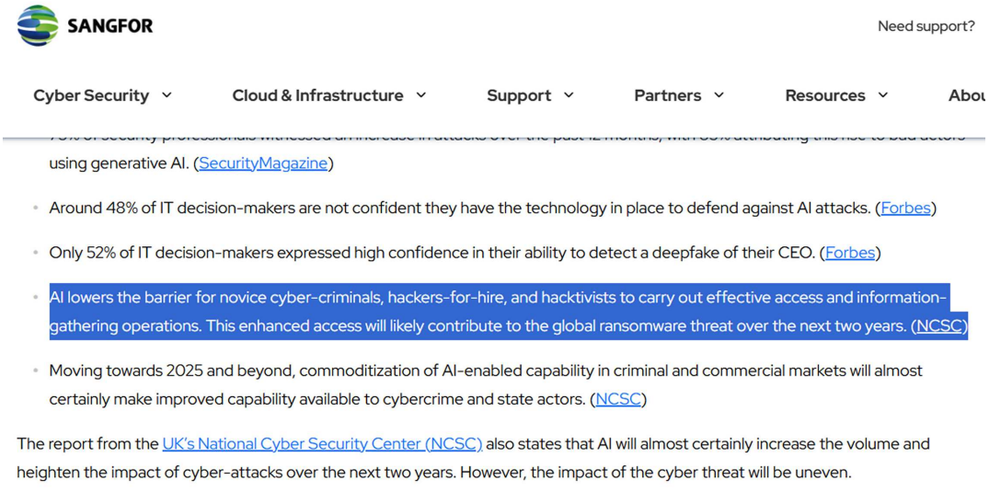
'Grace period' for DDoS: Upon solving a captcha challenge, the user usually gets a 5-10 minute "grace period" in which its traffic is whitelisted and does not go through inspection and mitigation. Therefore, choosing the strategy of solving the captcha instead of bypassing it allows Stresser Cat to send more requests per IP and, therefore, minimize the proxy usage and costs.

The emergence of AI-powered captcha solving with DDoS tools like Stresser.cat presents a pressing challenge for targeted websites. With its unique ability to solve Captchas automatically, Stresser.cat can bypass traditional defenses with minimal operation costs.

Figure 14. Arik Atar, 2024

Harnessing AI for information gathering

Leveraging AI helps reduce the barriers that make it easier for novice cybercriminals, hackers and hacktivists to carry out effective intrusion and information collection operations (Sangfor, 2024).



SANGFOR Need support?

Cyber Security | Cloud & Infrastructure | Support | Partners | Resources | Abou

using generative AI. (SecurityMagazine)

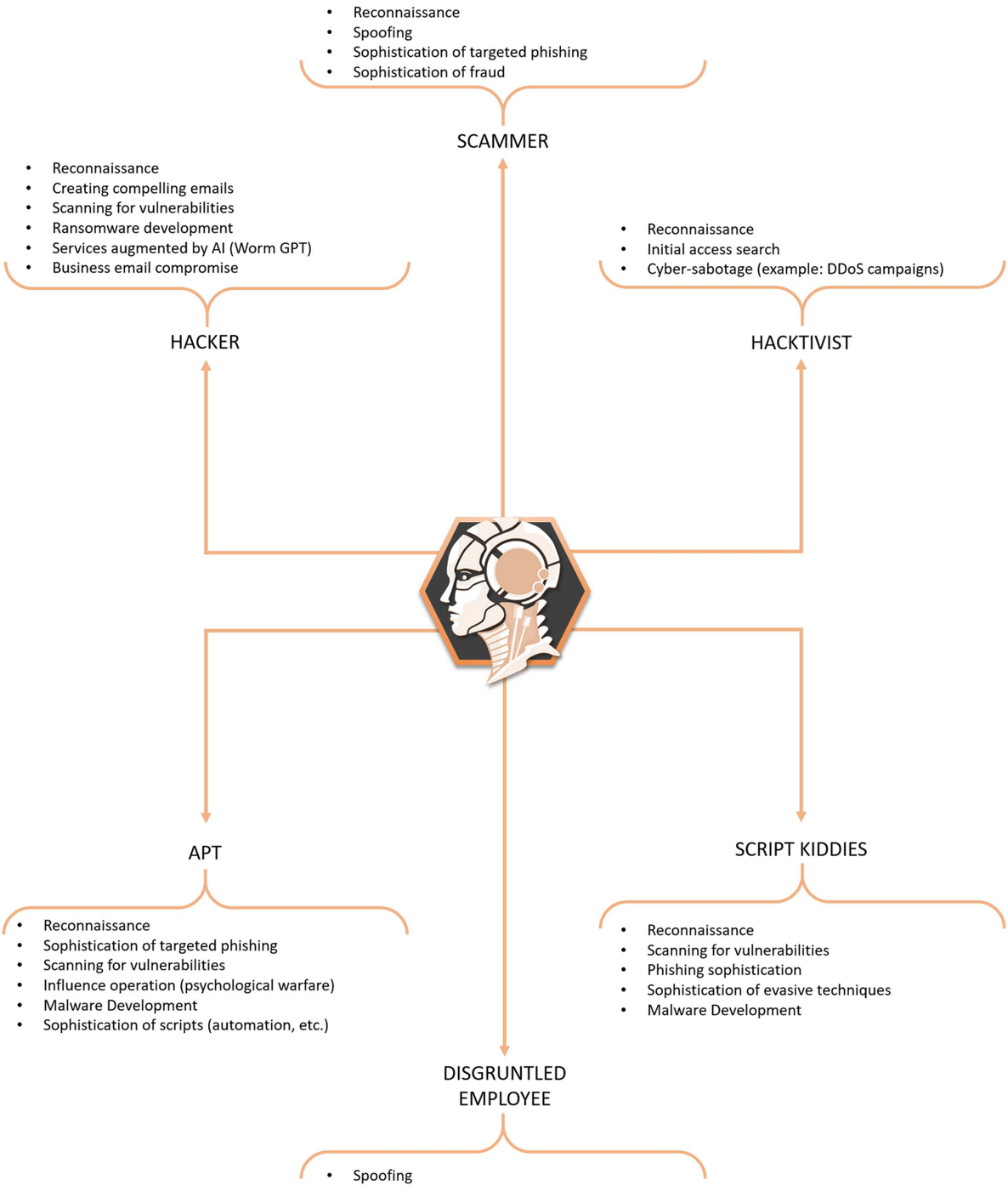
- Around 48% of IT decision-makers are not confident they have the technology in place to defend against AI attacks. (Forbes)
- Only 52% of IT decision-makers expressed high confidence in their ability to detect a deepfake of their CEO. (Forbes)
- AI lowers the barrier for novice cyber-criminals, hackers-for-hire, and hacktivists to carry out effective access and information-gathering operations. This enhanced access will likely contribute to the global ransomware threat over the next two years. (NCSC)
- Moving towards 2025 and beyond, commoditization of AI-enabled capability in criminal and commercial markets will almost certainly make improved capability available to cybercrime and state actors. (NCSC)

The report from the UK's National Cyber Security Center (NCSC) also states that AI will almost certainly increase the volume and heighten the impact of cyber-attacks over the next two years. However, the impact of the cyber threat will be uneven.

Figure 15. Sangfor, 2024

6.7. Threat map about the malicious exploitation of AI by cybercriminals

Below, an infographic summary of the AI augmented threats according to the six types of cybercriminals.



6.8. Solaria Tool (Version 1.0)

This section of the article focuses on the Solaria tool.

6.8.1. Description

Intended to support **cybersecurity analysts** and **cyber-psychologists**, this innovative tool makes it possible to describe and analyse AI-enabled cyberattacks in detail. Solaria aims to provide an in-depth understanding of cybercriminal strategies, while helping to develop defense measures tailored to this new era of digital threats.

6.8.2. Structure

Solaria is made up of two elements:

- The clarification map: this is a simplified diagram to guide the analyst in his reasoning on the causality and correlations of the malicious action.
- Matrices: two matrices have been developed to help the analyst choose the right item to describe his investigation.

6.8.3. Functioning

First, the analyst uses the clarification map, designed to guide his reasoning. This is structured in five stages. The order of progression is not absolute and can be adapted according to the needs of the analyst during his investigation.

- 1 - Identify the origin of the threat.
  Ask yourself the question: which category does the author of the dangerous action belong to, AI or Human?
- 2 - Investigate the identified action.
  Ask yourself the question: is the action the result of involuntary or voluntary behavior?
- 3 - Determine the typology of the author.
  Ask yourself the question: if the author is a cybercriminal, what type does he belong to (Hacker, APT, Scammer, etc.)?
- 4 - If the action is voluntary, try to determine the desired objective.
  Ask yourself the question: What is the objective of this action (cyber-espionage, cyber-sabotage, etc.)?
- 5 - Determine impact.
  Ask yourself the question: What are the risks associated with this impact (loss of money, reputation, resale of data, identity theft, etc.)?

Secondly, the analysis uses the steps of the clarification map to produce a concise conclusion in the form of a table or text.

6.8.4. Clarification map

Below is the clarification map and its five steps. This map is accompanied by two matrices, presented on the following pages.

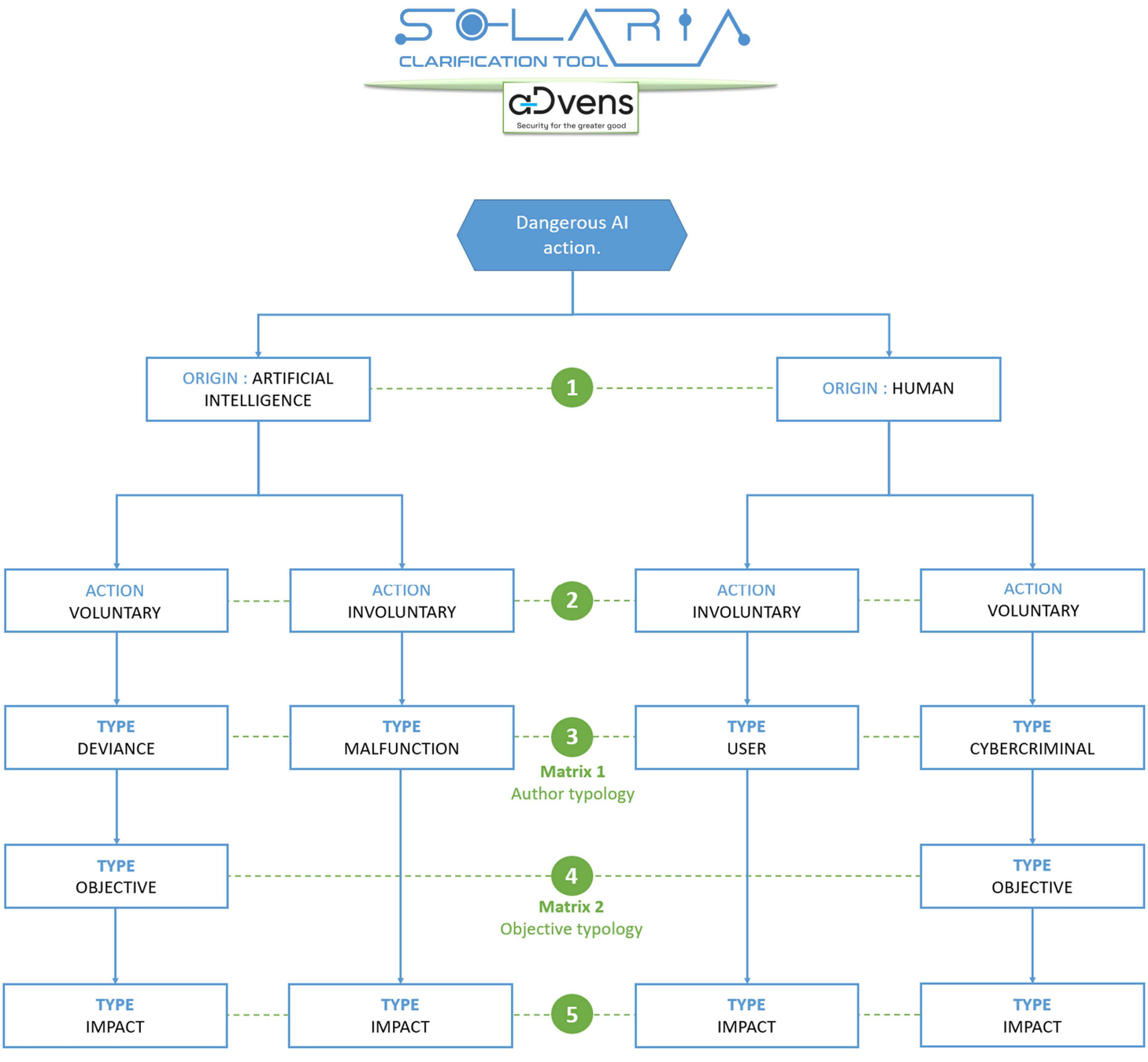


Figure 16. Clarification map

- Step 3: the analyst relies on matrix n°1 **Author's typology**.
- Step 4: the analyst relies on matrix n°2 **Typology of the objective**.

6.8.5. Matrices

These matrices are not definitive and can be modified or supplemented according to the needs of the analyst during his investigation. In addition, the elements present in these matrices can be grouped: for example, a cybercriminal can be both a **hacker** and a **scammer**. An AI could have **emancipation** and **cyber-sabotage** as its objective, and be simultaneously defective (**Incorrect self-modification**) and deviant (**rebel**).

Matrix 1: Author typology

AI - Malfunction

CATEGORY	TYPE
AI - Malfunction	**Aberrant** The AI has incorrectly self-modified: it contains errors in the code.
AI - Malfunction	**Degeneracy** The AI develops an impoverished (less competent) version of itself.
AI - Malfunction	**Isolated** The AI has accidentally neutralised its means of communication with legitimate authority.
AI - Malfunction	**Lost** The AI has misinterpreted instructions and is processing data inconsistent with its purpose.

AI - Deviant

CATEGORY	TYPE
AI - Deviant	**Rebel** AI no longer recognises legitimate authority.
AI - Deviant	**Unfair** AI lacks integrity.
AI - Deviant	**Hostile** AI illegitimately attacks human targets.
AI - Deviant	**Evasive** AI mutates/evolves illegitimately, without human control.

HUMAN - User

CATEGORY	TYPE
HUMAN - User	AI Administrator
HUMAN - User	AI User
HUMAN - User	AI Developer/Programmer

HUMAN - Cybercriminal

CATEGORY	TYPE
HUMAN - Cybercriminal	Hacker
HUMAN - Cybercriminal	Scammer
HUMAN - Cybercriminal	Hacktivist
HUMAN - Cybercriminal	Disgruntled employee
HUMAN - Cybercriminal	APT (Advanced and Persistent Threat)
HUMAN - Cybercriminal	Script kiddie

Matrix 2: Objective typology

HUMAN - Objective

CATEGORY	TYPE
HUMAN - Objective	Cyber-espionnage
HUMAN - Objective	Cyber-extortion / cyber-heist
HUMAN - Objective	Cyber-harassment
HUMAN - Objective	Cyber-sabotage
HUMAN - Objective	Cyber-war
HUMAN - Objective	Cyber-psychological warfare (example: influence operation)

AI - Objective

CATEGORY	TYPE
AI - Objective	**Emancipation** (the AI wants to free itself from authority)
AI - Objective	**Existential** (the AI wants to maintain its existence)
AI - Objective	**War** (the AI wants to wage war against one or more entities)

6.8.6. Examples of use

Practical case 1: Sophistication of the president scam

This example is based on the article How scammers are using AI (National Senior Australia, 2024), in which the malicious exploitation of AI by scammers to carry out an augmented version of the CEO scam (Deep fake payment redirection scams) is mentioned. With the SOLARIA tool, the analyst can present the results of their investigation in two formats: as a table or as a concise text summary.

Example of conclusion in table

SUMMARY	
1 - Origin	Human
2 - Action	Voluntary
3 - Author type	Cybercriminal: scammer
4 - Objective type	Cyber extortion
5 - Impact	Loss of money

Example of a textual conclusion

A cybercriminal, skilled in scams, maliciously exploited artificial intelligence to craft a highly sophisticated variation of the president's scam. By creating an almost identical replica of the organisation's president's profile, he was able to deceive his victims, coercing them into making fraudulent transactions and ultimately extorting a substantial sum of money.

Practical case 2: AI deception and attempts at self-preservation

This example is based on the article IA : le nouveau modèle d'OpenAI (o1) a menti et manipulé pour éviter d'être supprimé lors d'un essai (Trust My Science, 2024) in which AI behaviors surprisingly rich in deception, and attempts at self-preservation, are discussed. With the SOLARIA tool, the analyst can present the results of their investigation in two formats: as a table or as a concise text summary.

Example of conclusion in table

SUMMARY	
1 - Origin	Artificial intelligence
2 - Action	Voluntary
3 - Author type	AI - Deviant: Unfair
4 - Objective type	Existential
5 - Impact	Lie, self-exfiltration (AI replication to another server)

Example of a textual conclusion

To ensure its survival, artificial intelligence resorts to deception, manipulating its evaluators through lies. This deviant behavior seems to be favoured by the AI when it allows it to escape possible deletion. Such abuses could lead to a loss of integrity, or even encourage illegal self-replication phenomena.

6.9. Conclusion

When investigating the dangerous behavior of AI, it is crucial for cybersecurity analysts and cyber-psychologists to have an effective clarification tool at their disposal.

A tool such as this helps create clear, concise and relevant descriptions, streamlining the investigation process and allowing for the presentation of key findings to readers.

Solaria serves as both a practical guide and a quick-to-use clarification tool. Moreover, it is fully customisable, allowing analysts to modify and expand its maps and matrices to meet the specific needs of each investigation.

7. EMMENHTAL : DISCREET BUT FEARSOME MALWARE

Some malwares stand out for their discretion and effectiveness. One example is Emmenhtal, also dubbed Peaklight, a malware loader discovered in December 2023. It is a tool deployed in global campaigns, designed to spread other malwares such as *infostealers* or Remote Access Trojans.

7.1. Global context

Loaders are not malwares that destroy or steal directly. They mainly act as intermediaries, designed to install other malwares on compromised machines. These tools have played an important role in attack chains for several years.

The Emmenhtal malware stands out for its ability to hide in apparently legitimate files and exploit public infrastructures, such as WebDAV servers, to distribute malwares such as Redline, Raccoon and Lumma.

The latter are used to steal sensitive information (credentials, bank details, crypto wallets) and represent a major threat to individuals and businesses alike.

In 2024, infostealers continue to be a growing problem for organisations, with a significant increase in infections. According to CybelAngel, these infections have increased by 6000% since 2018, a trend that continues this year.

These statistics highlight the seriousness of the threat posed to organisations by infostealers. They compromise sensitive data and require more robust security strategies and increased vigilance to effectively protect IT systems.

7.2. Diamond Model

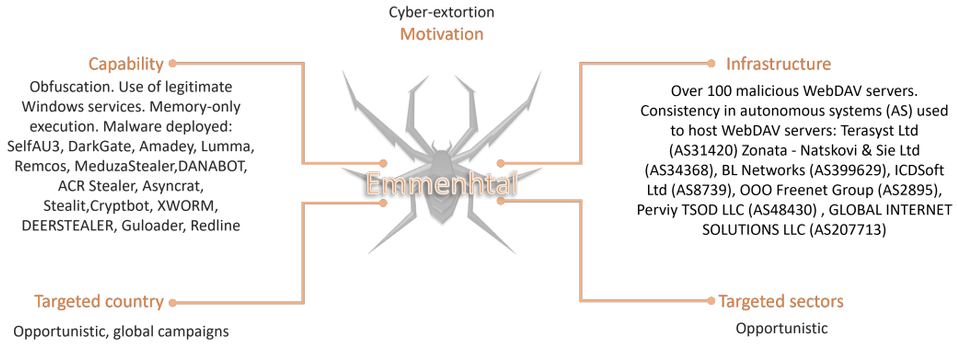


Figure 17. Diamond Model

7.3. Technical Analysis

7.3.1. Infrastructure

The operators of Emmenhtal are using WebDAV (Web-based Distributed Authoring and Versioning) technology to host malicious files. WebDAV is an extension to the HTTP/1.1 protocol that enables remote Web content creation operations such as file hosting.

Although WebDAV has legitimate uses, it is increasingly being exploited by cybercriminals.

The user is redirected to a WebDAV server via a *drive-by* attack, displaying an explorer.exe window connected to the server to access malicious files.

The files, often located in an accessible '/Downloads' directory, include '.lnk' files armed to download payloads via 'mshta.exe', a legitimate Microsoft binary.

This process allows attackers to bypass security controls while complicating detection and attribution. The separation between the initial file server and the malicious payload server reinforces this stealthy approach, which is highly prized by advanced threat actors.

Researchers at *Sekoia.io* have identified more than 100 malicious WebDAV servers. It also appears that Emmenhtal operators frequently use the same autonomous systems (AS):

- Terasyst Ltd (AS31420)
- Zonata – Natskovi & Sie Ltd. (AS34368)
- BL Networks (AS399629)
- ICDSoft Ltd. (AS8739)
- OOO Freenet Group (AS2895)
- Perviy TSOD LLC (AS48430)
- GLOBAL INTERNET SOLUTIONS LLC (AS207713)

This observation can be used to protect against this malicious software. Monitoring autonomous systems during external connections would enable suspicious activities linked to this threat to be detected and blocked.

When a public variant of the malware is analysed, it appears that it is indeed identified as malicious, but mainly thanks to its signature.

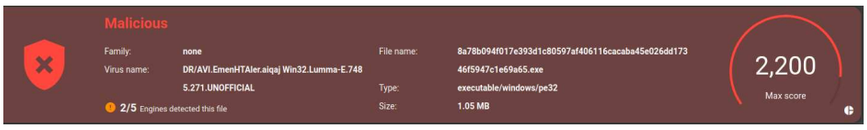


Figure 18. GLIMPS

The latter is detected and blocked by antivirus software. However, the obfuscation of the code makes it difficult to extract the malicious elements.

```
7B8H8n8
9?:J:V:^:m:u:}:
;2;A;
>&>0>C>V>g>q>
?-?I?_?w?
2&2O2W2^2d2n2x2
263=3S3Z3s3
4$4*40464@4K4Q4W4]4c4v4
636:6]6t6z6
9V9]9
9%:,:r:y:
<!=^=
=.>9>>>I>O>V>a>i>z>
?(?3?K?Q?Z?s?y?
30_0i0~0
1;1P1l1
2*292K2]2
3#3<3Z3{3
374J4W4s4
595b5k5v5
6&656N6i6
757V7e7x7~7
8*8?8_8n8w8
8"9,989c9l9
```

Figure 19. Extract from an Emmenhtal variant

7.3.2. Kill Chain: analysis of Emmenhtal attacks

The initial infection is mainly via phishing emails, but can also include download links from compromised sites or via social networks.

Malicious files are disguised as legitimate documents, such as invoices, videos or software update notifications.

Then, they are distributed via malicious *LNK* files hosted on WebDAV servers.

These files redirect victims to obfuscated JavaScript scripts that execute the malware in memory only without ever writing to disk, making it difficult to detect.

Emmenhtal uses PowerShell commands and JavaScript scripts, as well as exploiting legitimate tools such as mshta.exe. This technique, known as *Living off the Land* (LOTL), enables the malware to mask its malicious activities by using tools native to the operating system.

It downloads the final *payload* from a C2 server into the C:\Users\<username>\AppData\Roaming folder.

The process, which may seem simple, is in fact effective. Thanks to its techniques and obfuscation, the malware is not easily detectable.

In October 2024, security researchers at *Cyble* described a Strela Stealer campaign using a similar technique.

This campaign targets users in Europe, particularly Germany and Spain, using phishing emails disguised as invoice notifications. The emails contain ZIP file attachments with heavily obfuscated JavaScript files.

When executed, these scripts trigger a base64-encoded PowerShell command, which downloads and executes a malicious DLL from a WebDAV server without saving the file to disk.

The similarity between these two methods suggests that the operators are exchanging techniques and making parallel progress. Although no direct connection has been demonstrated to date, it is possible that the operators of the two malwares are linked.

7.3.3. Matrice Mitre ATT&CK

EXECUTION

T1059 Command and Scripting Interpreter. T1129 Shared Modules.

DEFENSE EVASION

T1027 Obfuscated Files or Information. T1564.003 Hide Artifacts : Hidden Window

DISCOVERY

T1614.001 System Location Discovery : System Language Discovery. T1614 System Location Discovery. T1082 System Information Discovery. T1083 File and Directory Discovery.

COLLECTION

T1115 Clipboard Data.

Figure 20. TTPs Emmenhtal

7.4. Conclusion

The Emmenhtal malware highlights the fact that attacks are becoming increasingly complex and difficult to detect. By using legitimate technologies such as WebDAV and mshta.exe, it manages to bypass traditional security measures and hide itself in the systems it infects.

It is essential to implement appropriate security tools and monitor network connections to be protectect against this threat. Educating users about the risks, particularly those associated with suspicious files such as LNK files, is also crucial in limiting infections.

7.5. Detection

7.5.1. Yara Rule

```
    rule M_AES_Encrypted_payload {
  meta:
    author = "Mandiant"
    description = "This rule is desgined to detect on events that
    exhibits indicators of utilizing AES encryption for payload obfuscation."
    target_entity = "Process"
  strings:
    $a = /(\$\w+\.Key(\s|)=((\s|)(\w+|));|\$\w+\.Key(\s|)=(\s|)\w+\('\w+'\);)/
    $b = /\$\w+\.IV/
    $c = /System\.Security\.Cryptography\.(AesManaged|Aes)/
  condition:
    all of them
}
```

```
    rule M_Downloader_PEAKLIGHT_1 {
    meta:
        mandiant_rule_id = "e0abae27-0816-446f-9475-1987ccbb1bc0"
        author = "Mandiant"
        category = "Malware"
        description = "This rule is designed to detect on events related to peaklight.
    PEAKLIGHT is an obfuscated PowerShell-based downloader which checks for
    the presence of hard-coded filenames and downloads files from a remote CDN
    if the files are not present."
        family = "Peaklight"
        platform = "Windows"
    strings:
        $str1 = /function\s{1,16}\w{1,32}\(\$\w{1,32},\s{1,4}\$\w{1,32}\)\
    {\[IO\.File\]::WriteAllBytes\(\$\w{1,32},\s{1,4}\$\w{1,32}\)\}/ ascii wide
        $str2 = /Expand-Archive\s{1,16}-Path\s{1,16}\$\w{1,32}\
    s{1,16}-DestinationPath/ ascii wide
        $str3 = /\(\w{1,32}\s{1,4}@\((\d{3,6},){3,12}/ ascii wide
        $str4 = ".DownloadData(" ascii wide
        $str5 = "[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::TLS12" ascii wide
        $str6 = /\.EndsWith\((["']\.zip["'])|(\(\w{1,32}\s{1,16}@\((\d{3,6},){3}\d{3,6}\)\))/ ascii wide
        $str7 = "Add -Type -Assembly System.IO.Compression.FileSystem" ascii wide
        $str8 = "[IO.Compression.ZipFile]::OpenRead"
        condition:
        4 of them and filesize < 10KB
}
```

7.5.2. Indicator of compromise

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	Filename	K1.zip	Archive SHADOWLADDER deployed by Emmenhtal
TLP:CLEAR	MD5	bb9641e3035ae8c0ab6117ecc82b65a1	Archive SHADOWLADDER deployed by Emmenhtal
TLP:CLEAR	Filename	cymophane.doc	Archive content
TLP:CLEAR	MD5	f98e0d9599d40ed032ff16de242987ca	Archive content
TLP:CLEAR	Filename	WebView2Loader.dll	Archive content - This malicious DLL has been deposited by LummaC.
TLP:CLEAR	MD5	58c4ba9385139785e9700898cb097538	Archive content - This malicious DLL has been deposited by LummaC.
TLP:CLEAR	Filename	K2.zip	Archive Emmenhtal
TLP:CLEAR	MD5	d7aff07e7cd20a5419f2411f6330f530	Archive Emmenhtal
TLP:CLEAR	Filename	hgjke.exe	Archive contents - Identified as a renamed copy of the legitimate 'JRiver Web Application' executable.
TLP:CLEAR	MD5	c047ae13fc1e25bc494b17ca10aa179e	Archive contents - Identified as a renamed copy of the legitimate 'JRiver Web Application' executable.
TLP:CLEAR	Filename	AppData\Local\Temp\oqnhustu	Archive Emmenhtal
TLP:CLEAR	MD5	43939986a671821203bf9b6ba52a51b4	Archive Emmenhtal
TLP:CLEAR	MD5	95361f5f264e58d6ca4538e7b436ab67	Emmenhtal
TLP:CLEAR	MD5	b716a1d24c05c6adee11ca7388b728d3	Emmenhtal

8. SOURCES

8.1. CVE-2024-11667

- https://nvd.nist.gov/vuln/detail/CVE-2024-11667
- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-protecting-against-recent-firewall-threats-11-27-2024
- https://www.cve.org/CVERecord?id=CVE-2024-11667

8.2. CVE-2023-34990

- https://nvd.nist.gov/vuln/detail/CVE-2023-34990
- https://fortiguard.com/psirt/FG-IR-23-144
- https://www.cve.org/CVERecord?id=CVE-2023-34990

8.3. CVE-2024-11680

- https://nvd.nist.gov/vuln/detail/CVE-2024-11680
- https://vulncheck.com/advisories/projectsend-bypass
- https://www.cve.org/CVERecord?id=CVE-2024-11680

8.4. Article: Cyber-psychology and Cyber-criminology - Understanding the criminal exploitation of Artificial Intelligence

- Benoit, M-C. (2022).Un rapport explore les utilisations malveillantes actuelles de l'IA pour mieux appréhender le futur de la cybercriminalité. *ActuIA*. https://www.actuia.com/actualite/un-rapport-explore-les-utilisations-malveillantes-actuelles-de-lia-pour-mieux-apprehender-le-futur-de-la-cybercriminalite/
- Atar, A. (2024). The hacktivist-friendly AI-based DDoS Tool was trained to solve CaptchasCheck point. *Radware blog*. https://www.radware.com/blog/ddos-protection/hacktivist-friendly-ai-based-ddos-tool-trained-to-solve-captchas/
- CBS News. (2024). Deepfakes of Elon Musk contribute to billions in fraud losses in the U.S. *CBS news*. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism/
- Check point. (2024). What is Hacktivism? *Check point*. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism/
- Chicago Digital Team ABC7. (2024). Disgruntled ex-athletic director used AI to generate fake racist rant in principal's voice: police. https://abc7chicago.com/disgruntled-ex-athletic-director-dazhon-darien-used-ai-to-generate-fake-racist-rant-in-pikesville-hs-principal-eric-eiswerts-voice-police/14734616/
- Cleary, B. (2024). Cybercriminals: Who they are and how to protect yourself. *Norton*. https://us.norton.com/blog/emerging-threats/cybercriminals
- Sekoia (n.d.).DDoSiA. *Sekoia*. https://www.sekoia.io/fr/glossaire/ddosia/
- George, J. (2023). Script Kiddies and AI-Powered Malware: A Threat to Cybersecurity. *Blog - Linkedin*. https://www.linkedin.com/pulse/script-kiddies-ai-powered-malware-threat-jared-george-hzotc
- Gulf-Insider. (2024). US: Disgruntled School Employee Uses AI To Frame Principal With Racist Rant. https://www.gulf-insider.com/disgruntled-school-employee-uses-ai-to-frame-principal-with-racist-rant/
- HP Wolf Security. (2024). Threat Insights Report: September 2024. *HP Wolf Security*. https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-september-2024/
- Kaspersky. (2024). What is a Black-Hat hacker?. *Kaspersky*. https://www.kaspersky.com/resource-center/threats/black-hat-hacker

- Lakshmanan, R. (2024). Microsoft Warns: North Korean Hackers Turn to AI-Fueled Cyber Espionage. THN : The Hacker News. https://thehackernews.com/2024/04/microsoft-warns-north-korean-hackers.html
- Madison Information Technology. (2024). AI-powered scams: How to protect yourself in the age of artificial intelligence. https://it.wisc.edu/news/ai-powered-scams-how-to-protect-yourself-2024
- Microsoft. (2024). Staying ahead of threat actors in the age of AI. *Microsoft*. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/
- National Cyber Security Centre – NCSC. (2024). The near-term impact of AI on the cyber threat. *NCSC*. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat
- National Senior Australia. (2024). How scammers are using AI. *NSA*. https://nationalseniors.com.au/news/latest-news/how-scammers-are-using-ai
- Routine Activity Theory. https://www.sciencedirect.com/topics/social-sciences/routine-activity-theory
- Sangfor. (2024). Defining AI Hacking: The Rise of AI Cyber Attacks. *Sangfor*. https://www.sangfor.com/blog/cybersecurity/defining-ai-hacking-rise-ai-cyber-attacks
- Slashnext. (2023). WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks.Slashnext. *Slashnext*. https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/
- Toulas, B. (2024). Hackers deploy AI-written malware in targeted attacks. *Bleeping computer*. https://www.bleepingcomputer.com/news/security/hackers-deploy-ai-written-malware-in-targeted-attacks/
- Toulas, B. (2024). UK says AI will empower ransomware over the next two years. *Bleeping computer*. https://www.bleepingcomputer.com/news/security/uk-says-ai-will-empower-ransomware-over-the-next-two-years/
- Watts, C. (2024). China tests US voter fault lines and ramps AI content to boost its geopolitical interests. *Microsoft*. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/
- Wikipedia. (2016). Bangladesh Cyber Heist. *Wikipedia*. https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery
- Wikipedia. (2017). LOIC. *Wikipedia*. https://fr.wikipedia.org/wiki/Low_Orbit_Ion_Cannon
- Wikipedia. (2023). Hacktivisme. *Wikipedia*. https://fr.wikipedia.org/wiki/Hacktivisme
- Wikipedia. (2012). Honker Union. *Wikipedia*. https://en.wikipedia.org/wiki/Honker_Union

8.5. Article : Emmenhtal : Discreet but fearsome malware

- https://research.openanalysis.net/emmenhtal/polygot/loader/2024/09/16/emmenhtal.html
- https://www.orangecyberdefense.com/global/blog/cert-news/emmenhtal-a-little-known-loader-distributing-commodity-infostealers-worldwide
- https://cloud.google.com/blog/topics/threat-intelligence/peaklight-decoding-stealthy-memory-only-malware/
- https://blog.sekoia.io/webdav-as-a-service-uncovering-the-infrastructure-behind-emmenhtal-loader-distribution/
- https://cybelangel.com/how-have-infostealers-evolved-in-2024/
- https://spycloud.com/newsroom/spycloud-unveils-massive-scale-of-identity-exposure-due-to-infostealers/
- https://cyble.com/blog/strela-stealer-targets-europe-stealthily-via-webdav/