Monthly Cyber Threat Intelligence report
September 2024

2024-10-03 I **TLP:CLEAR** I CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

Table of content

1. Executive summary

This month, the CERT aDvens presents three noteworthy vulnerabilities, in addition to those already published.

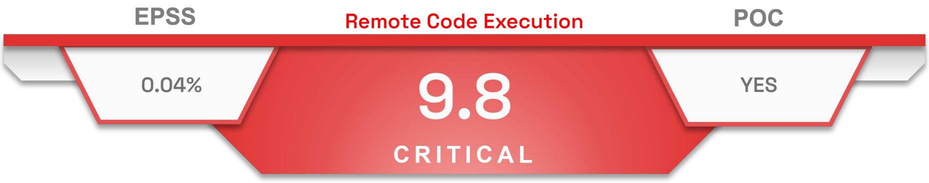
In two articles, CERT analysts present :

- three psychological and cyberpsychological models to understand user vulnerability to phishing;
- an analysis of a scam campaign targeting the retail sector.

2. Vulnerabilities

2.1. CVE-2024-40711

Security researcher Florian Hauser from *CODE WHITE Gmbh* has discovered a critical vulnerability (CVE-2024-40711) affecting Veeam Backup & Replication. This vulnerability was patched by the editor in their September 2024 advisory.



An insecure deserialisation in Veeam Backup & Replication allows an attacker to execute arbitrary code by sending a specifically crafted payload.

According to *Censys*, 2 833 Veeam Backup & Replication servers are exposed on the Internet, mainly present in Germany and France. These servers are not necessarily all vulnerable.

2.1.1. Type of vulnerability

- CWE-502: Deserialization of Untrusted Data

2.1.2. Risk

- Remote Code Execution

2.1.3. Severity (base score CVSS 3.1)

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

2.1.4. Impacted Products

- Veeam Backup & Replication versions 12.x prior to 12.1.2.172 (included)

2.1.5. Recommandations

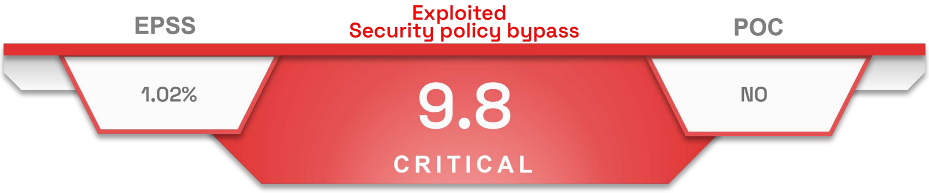
- Update Veeam Backup & Replication to the version 12.2 (build 12.2.0.334) or later.
- Additional information is available in Veeam's advisory.

2.1.6. Proof of concept

A proof of concept is available in open source.

2.2. CVE-2024-40766

On 22 August 2024, SonicWall published a security advisory concerning a critical vulnerability affecting their firewalls. On 6 September 2024, they updated their advisory to state that the vulnerability also affects SSLVPN.



EPSS

1.02%

Exploited
Security policy bypass

9.8

CRITICAL

POC

NO

An access control flaw in SonicOS and SSLVPN allows an attacker to bypass the security policy and gain access to restricted resources. Under certain specific conditions, the attacker can cause a denial of service.

The vulnerability is exploited.
It was added to the CISA's Known Exploited Vulnerabilities (KEV) catalog on 09 September, 2024.

2.2.1. Type of vulnerability

- CWE-284: Improper Access Control

2.2.2. Risk

- Security policy bypass
- Breach of data confidentiality
- Denial of service

2.2.3. Severity (base score CVSS 3.1)

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

2.2.4. Impacted Products

- SOHO (Gen 5) versions prior to 5.9.2.14-12o
- Gen6 firewalls versions prior to 6.5.4.14-109n, 6.5.4.15.116n : SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W
- Gen7 firewalls versions prior to 7.0.1-5035 : TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700

2.2.5. Recommandations

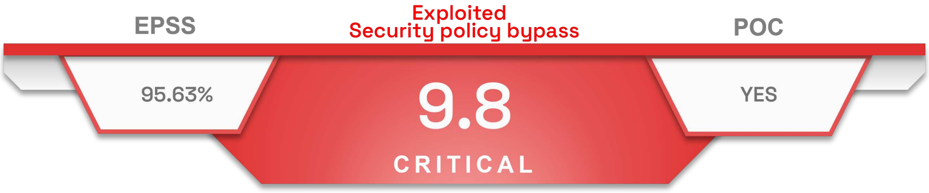
- Update SOHO products (Gen 5) to version 5.9.2.14-12o or later.
- Update Gen6 firewalls to version 6.5.4.14-109n, 6.5.4.15.116n or later.
- Update Gen7 firewalls to version 7.0.1-5035 or later.
- The editor recommends updating the SSLVPN's user passwords and enabling multi-factor authentication.
- Additional information is available in SonicWall's advisory.

2.2.6. Proof of concept

To date, no proof of concept is available in open source.

2.3. CVE-2024-6670

Security researcher Sina Kheirkhah of *Zero Day Initiative* has discovered a critical vulnerability (CVE-2024-6670) affecting Progress WhatsUp Gold. This vulnerability was patched by the editor in their August 2024 advisory.



An SQL injection vulnerability allows an unauthenticated attacker to obtain the user's encrypted password. According to Progress, this vulnerability exists when the system has only one user.

The vulnerability has been exploited.
It was added to the CISA's Known Exploited Vulnerabilities (KEV) catalog on 16 September, 2024.

2.3.1. Type of vulnerability

- **CWE-89**: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

2.3.2. Risk

- Security policy bypass

2.3.3. Severity (base score CVSS 3.1)

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

2.3.4. Impacted Products

- WhatsUp Gold versions prior to 2024.0.0

2.3.5. Recommandations

- Update WhatsUp Gold to version 2024.0.0 or later.
- Additional information is available in Progress' advisory.

2.3.6. Proof of concept

A proof of concept is available in open sources.

3. Psychology / Cyberpsychology: Three Models for understanding user's vulnerability to Phishing

3.1. Foreword

This article consists of two distinct parts. The first part examines in detail three major models used by researchers to understand users' susceptibility to phishing attempts. The first model presented is the **Opportunity and Routine Activities Theory** (1979), followed by the **Heuristic Systematic Information Processing** model (1980), and finally the **Suspicion, Cognition, and Automaticity Model** (2018).

The second part introduces a new concept, the **Psychological Attack Surface** (SAP), which is directly inspired by these three theoretical frameworks.

3.1.1. vocabulary

Below are some definitions to help with the reading.

- **Cognitive**
  The acquisition of knowledge (LeRobert, 2024).

- **Heursitic**
  Using mental shortcuts to quickly formulate judgments or decisions (Cuofano, 2024).

- **Systematic**
  Analytical, rational and in-depth evaluation of information content (Cuofano, 2024).

- **Cyberpsychology**
  Study of mental phenomena applied to cyberspace, i.e. the virtual, artificial and recreated world. Virtual reality and telepsychotherapy are two concrete examples of cyberpsychology (Bouchard, 2016).

- **Cyberspace**
  Communication space created by the global interconnection of computers (Internet) and by the data processed there; space, environment in which Internet users navigate (LeRobert, 2024).

- **Postmodernity**
  Refers to the structural upheavals in lifestyles and social organisation specific to the 20th century (Yousfi, 2013).

- **Stimulus**
  External or internal cause capable of provoking the reaction of an excitable system, of a living organism (LeRobert, 2024).

3.2. Section 1: Models

This first section highlights the three explanatory models.

3.2.1. Explanatory model 1: Routine Activity Theory

- Research field: Criminology
- Scientists: Marcus Felson and Lawrence E. Cohen
- Name: Routine Activity Theory
- Acronym: RAT
- Year: 1979

Description

Developed by Marcus Felson and Lawrence E. Cohen in 1979, Routine Activity Theory suggests that the likelihood of a crime increases with the convergence of three components: a motivated criminal, a suitable target and an ineffective and absent protection.

This convergence of the three components in space and time is favored by postmodernity, which characterises the current state of Western civilisation. Marked by the emergence of a flourishing economy after the Second World War, this period led to profound social upheavals, particularly in the areas of urbanisation and transport. However, this era of development was also accompanied by a significant increase in crime. According to Felson and Cohen, this increase is the result of new opportunities offered by economic prosperity. For example :

- The feminisation of work offered criminals a double opportunity: targeting women and homes that are often empty and unprotected.
- The automobile also offered a double opportunity: in addition to being stolen, the automobile is a means of free and rapid mobility for the criminal.

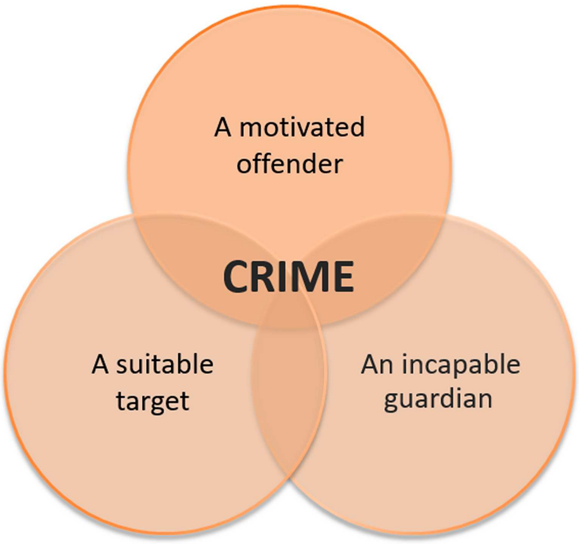


Figure 1. Routine Activity Theory.

In short, *Felson* and *Cohen* raised the idea that the level of crime would be influenced by the normal organisation of society.

Key Elements of the Routine Activity Theory

- According to the theory, having adequate protection in place helps prevent criminal acts and secure potential targets.
- The interaction between motivation, opportunity and the availability of vulnerable targets increases the likelihood of committing a crime.
- Although societal transformations can improve the quality of modern life, they can also create favorable conditions for increased crime.

Cyber context

Since its development, Routine Activity Theory has been widely applied to the study of various forms of crime, including cybercrime. Like other societal transformations, the rise of computing and the cyberspace has created new opportunities for cybercriminals.

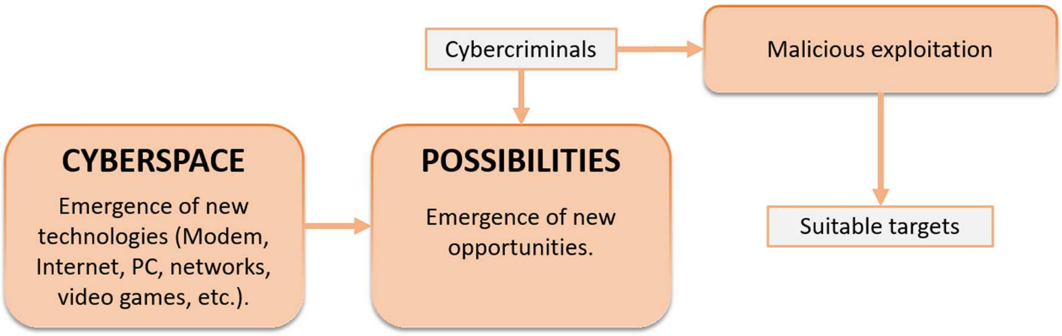

Cybercriminals
Malicious exploitation
CYBERSPACE
Emergence of new technologies (Modem, Internet, PC, networks, video games, etc.).
POSSIBILITIES
Emergence of new opportunities.
Suitable targets

Figure 2. Cyberspace: the fifth battlefield (after land, sea, sky and space).

Among the many malicious techniques, phishing is particularly popular with cybercriminals. They strive to design fraudulent emails or SMS messages aimed at exploiting the psychological vulnerabilities of users (psychological hacking or social engineering) in order to obtain a manipulated consent. Insufficient or ineffective protection would not prevent these attacks or protect vulnerable targets.

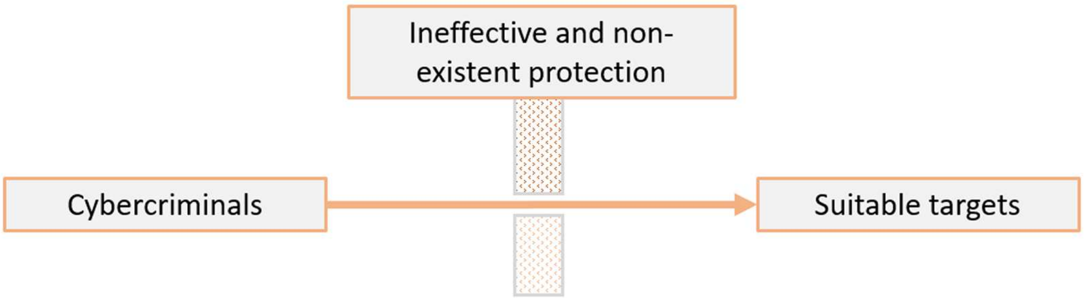


Figure 3. Ineffective and absent protection would not prevent crime.

According to the theory, an adequate protection would counter the crime and protect appropriate targets.

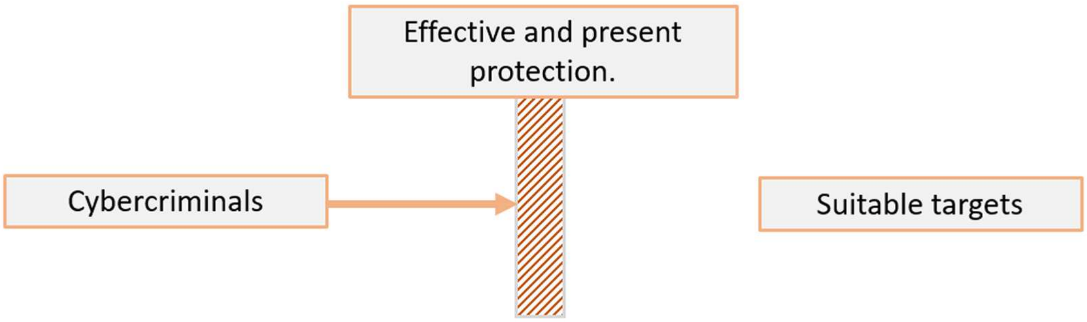


Figure 4. Adequate protection would help counter crime.

VIVA in the cyber context

The Routine Activity Theory specifies that the "appropriate target" is defined by four attributes, grouped under the acronym **VIVA**. It is these attributes that determine whether a target is deemed suitable by the criminal. Here are the four attributes:

ATTRIBUTES	EXPLANATIONS (Miró, 2014)
V - Value	The value of the target, in a real or symbolic manner.
I - Inertia	The physical obstacles of the target: weight, height, strength, etc.
V - Visibility	The attribute of exposure which solidifies the suitability of the target.
A - Accessibility	The placement of the individual, or object, that increases, or lessens, the potential risk of the intended attack.

According to the work of Liliana Ribeiro, Inês Sousa Guedes and Carla Sofia Cardoso (Which factors predict susceptibility to phishing? An empirical study), **VIVA** can be explained as follows in the context of phishing:

ATTRIBUTES	EXPLANATIONS
V - Value	Value can vary depending on the crime, but in a phishing attack, it relates to motivations such as financial gain. Therefore, individuals with higher incomes may be at a greater risk of receiving phishing emails (Graham & Triplett, 2017).
I - Inertia	Inertia applies to people or objects, which in the context of cyberspace, could be exemplified when an attachment is downloaded with a virus (Leukfeldt & Yar, 2016).
V - Visibility	Visibility might be facilitated due to the lack of physical barriers on the Internet, which in turn may attract more motivated offenders. (Yar, 2005).
A - Accessibility	Access can be limited by the potential victims by implementing various security measures, such as the use of strong passwords.

Conclusion

In the context of cybersecurity, Routine Activity Theory highlights the essential importance of appropriate protection to prevent cybercrime. By blocking the convergence of three key elements – a motivated cybercriminal, a vulnerable target and insufficient or no protection – it is possible to significantly reduce users' susceptibility to phishing attacks.

3.2.2. Model 2: The Heuristic-Systemic model of information processing

- Research fields: Cognitive psychology and Social psychology
- Scientist: Shelly Chaiken
- Name: The Heuristic-Systemic model of information processing
- Acronym: THS
- Year: 1980

Description

The Heuristic-Systemic model of information processing was developed by psychologist Shelly Chaiken in 1980 to explain how individuals receive and process persuasive messages.

According to the model, humans can process messages in two ways: systematic and heuristic.

- **Systematic**: This type of processing involves in-depth and analytical processing of information. The content and reliability of the references are analysed by the individual to determine the relevance of the arguments. This processing requires higher cognitive abilities and skills, which consequently leads to high resource consumption. Judgments developed by the individual from systematic processing tend to respond adequately to the semantic content of the message (Bhattacharjee, 2017; Chen et al., 1999).

- **Heuristic**: This type of processing involves the use of simplifying decision rules to quickly evaluate the content of the message. Its functioning is based on knowledge structures that have been learned and memorised by the receiving individual. The three indices of heuristic processing are availability (memorised knowledge), accessibility (activated knowledge from memory) and applicability (relevance of the knowledge compared to the individual's objectives). The particularity of this treatment is that it allows the individual to save resources since the cognitive effort is low. Advertisements are known to exploit processing heuristics in individuals (Bhattacharjee, 2017; Tanner, 2005).

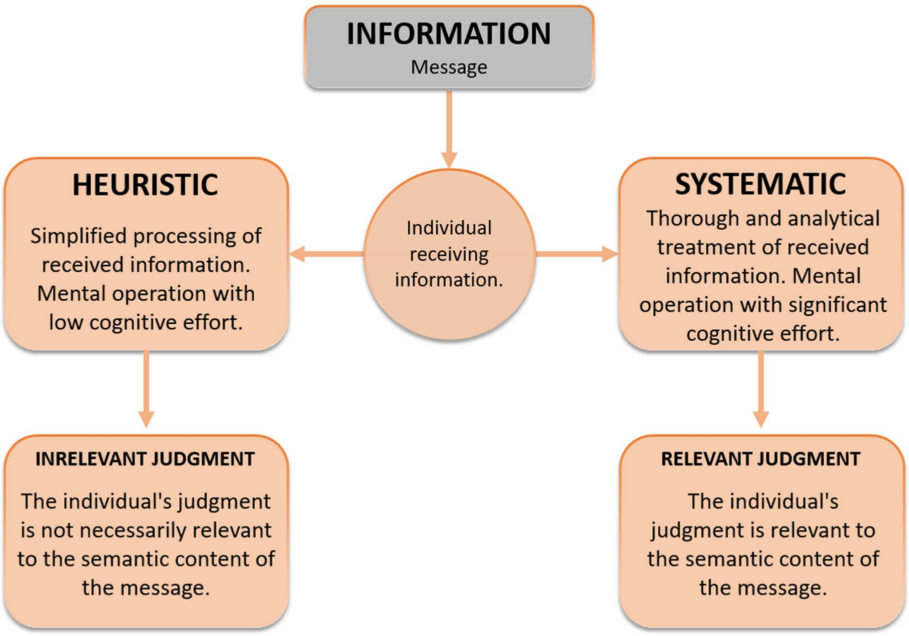

INFORMATION
Message
HEURISTIC
Simplified processing of received information. Mental operation with low cognitive effort.
Individual receiving information.
SYSTEMATIC
Thorough and analytical treatment of received information. Mental operation with significant cognitive effort.
INRELEVANT JUDGMENT
The individual's judgment is not necessarily relevant to the semantic content of the message.
RELEVANT JUDGMENT
The individual's judgment is relevant to the semantic content of the message.

Figure 5. Two types of information processing processes.

Key Elements of the Theory

- Scientific studies reveal that individuals are capable of both processes, however heuristic processing is predominant over systematic processing (Vishwanath et al., 2011).
- Systematic processing requires more cognitive effort than heuristic processing (Suri & Monroe, 2003).
- Individuals may be able to carry out one processing process independently or both simultaneously (Bhattacharjee, 2017).
- Unlike attitudes developed through systematic processing, those developed or modified using only a heuristic process will likely be less stable, less resistant to counterarguments, and will be less predictive of their future behaviors (Bhattacharjee, 2017).

Cyber context

The explanation proposed by the Heuristic-Systemic model of information processing is not limited to the physical world. Indeed, this model also applies to the cyberspace where billions of individuals interact. Thus, It provides a better understanding of how individuals receive and process persuasive messages in the cyberspace.

Several additional works by Shelly Chaiken, published in 1987 in *Social Influence The Ontario Symposium, Volume 5* revealed the importance of different factors that can influence the individual to favor heuristic processing. These factors are authority (director, CEO, manager, etc.), time and/or social pressure, and personal abilities.

This work echoes the numerous research studies on the exploitation of cognitive biases during social engineering. Depending on the type of fraud, attackers may craft phishing emails to exploit certain cognitive biases. This psychological vulnerability is particularly emergent during heuristic processing.

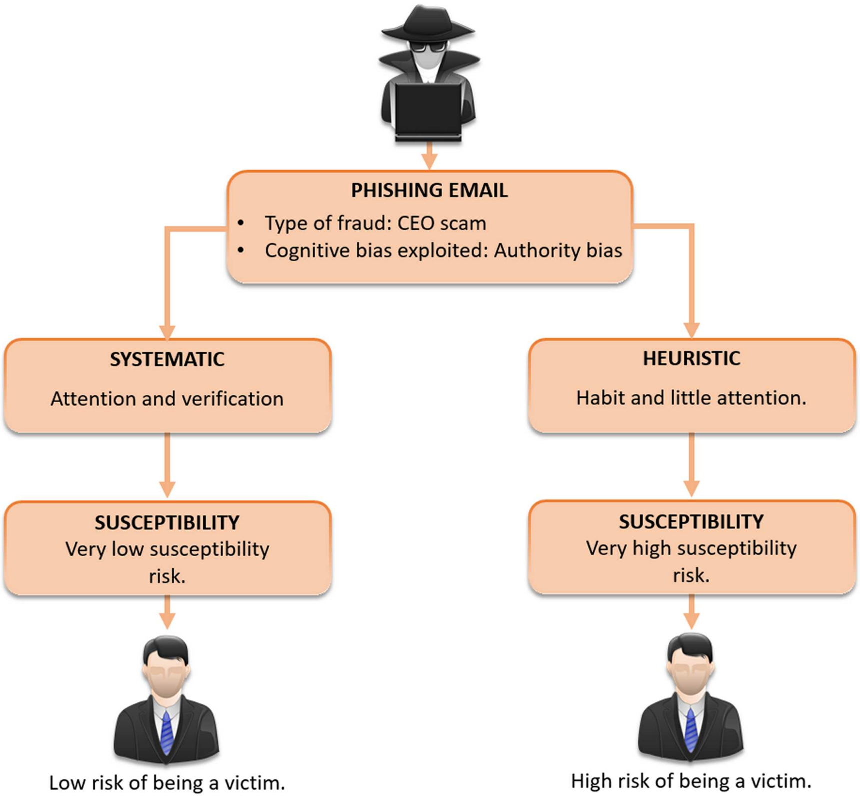

PHISHING EMAIL
• Type of fraud: CEO scam
• Cognitive bias exploited: Authority bias
SYSTEMATIC
Attention and verification
HEURISTIC
Habit and little attention.
SUSCEPTIBILITY
Very low susceptibility risk.
SUSCEPTIBILITY
Very high susceptibility risk.
Low risk of being a victim.
High risk of being a victim.

Figure 6. Understanding user susceptibility to phishing with the THS model.

Conclusion

Based on the Heuristic-Systemic model of information processing, users' susceptibility to phishing can be reduced if they promote information processing in a systematic manner. By behaving rationally, users can prevent the emergence of psychological vulnerability such as habits and cognitive biases.

3.2.3. Model 3: Suspicion, cognition, and automaticity model

- Research field: Communication
- Scientists: Arun Vishwanath, Brynne Harrison and Yu Jie Ng
- Name: Suspicion, cognition, and automaticity model
- Acronym: SCAM
- Year: 2018

Description

In 2018, Vishwanath and his colleagues presented their work on the SCAM model (*Suspicion, Cognition, and Automaticity Model*) which builds on previous research, notably the THS model (*Heuristic-Systemic model of information processing*), to explain the susceptibility of individuals to phishing (Vishwanath et al., 2018).

The central element of this model is *Suspicion* considered to be the main internal predictor of individual vulnerability to phishing. Suspicion is defined as the degree of uncertainty an individual feels when interacting with a particular stimulus (Lyons et al., 2011).

This level of suspicion can be influenced by the type of information processing that the user favors. Strongly heuristic processing reduces suspicion of phishing emails because it relies on mental shortcuts and rapid assessment. On the other hand, systematic processing, which involves more in-depth analysis, leads to an increase in suspicion and, consequently, better protection against these fraud attempts.

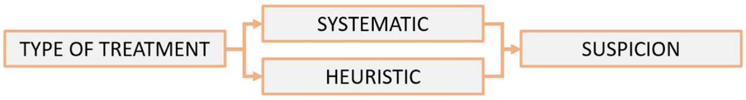


Figure 7. Suspicion is influenced by the type of treatment.

The SCAM model suggests that a key factor determines the type of information processing favoured by the user: **Cyber-risk beliefs**. These convictions, or beliefs, represent the cognitions most frequently mobilised by individuals when they evaluate online situations presenting risks (Griffin et al., 2002).

Cyber risk beliefs refer to the perceptions that users form of the dangers linked to their online behavior. These beliefs play a dual role: they not only influence the type of information processing chosen (heuristic or systematic), but they also directly impact the level of distrust felt when faced with potentially fraudulent stimuli, such as phishing emails (Vishwanath et al., 2018). A high perception of cyber risk may therefore encourage more systematic treatment and increased distrust.

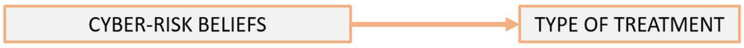


Figure 8. Beliefs about cyber-risks influence the type of treatment and suspicion.

Furthermore, the model also suggests that the individual's inability to self-regulate their behavior influences their habits. Thus, a user who maintains his habits is encouraged not to raise his suspicion regarding phishing emails.

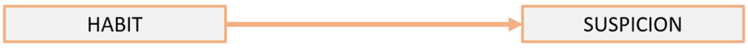


Figure 9. Habit influences suspicion.

Key Elements of the Theory

- Suspicion is identified as the main internal factor influencing a user's vulnerability to phishing.
- Increased use of heuristic processing reduces suspicion of fraudulent emails.
- According to the model, a strong perception of cyber risks encourages the user to adopt more systematic information processing.
- By favouring systematic processing, the user reduces their susceptibility to phishing attempts.
- Cyber-risk beliefs influence the way information is processed.
- The inability to self-regulate one's behavior leads to perpetuating habits that reduce vigilance against phishing.

Cyber context

Below is an alternative infographic of the SCAM model:

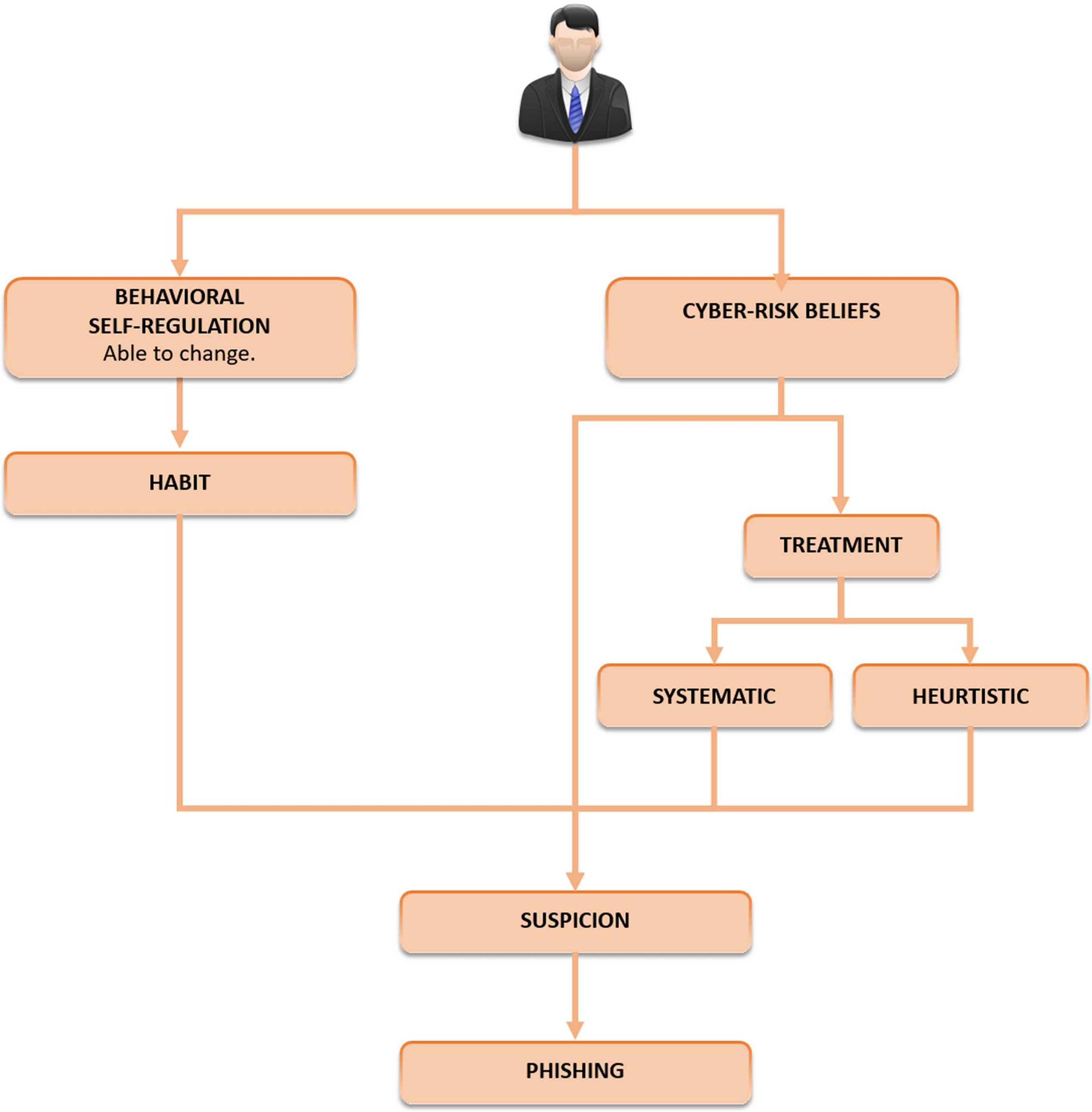


Figure 10. Alternative infographic.

Conclusion

Developing knowledge and beliefs relating to cyber risks makes it possible to influence the type of information processing carried out by the individual. Thus, strong beliefs contribute to systematic processing which results in increased distrust of phishing.

Additionally, by being able to self-regulate behavior to avoid habits, it becomes possible to reduce the risk of susceptibility to phishing.

3.2.4. Synthesis

Below is a non-exhaustive summary of the solutions proposed by the three explanatory models.

EXPLANATORY MODELS	SOLUTION
1 - RAT	Avoid the convergence of the three components in space and time (potential criminal, appropriate target, and incapable guardians) by promoting effective and present protection.
2 - THS	Promote a systematic information processing process.
3 - SCAM	Develop Cyber-risk beliefs in order to promote systematic treatment that increases suspicion of phishing. Increased suspicion reduces the risk of susceptibility. In addition, the ability to self-regulate to avoid habits also helps reduce the risk of susceptibility.

3.3. Section 2: Imagination and concept

3.3.1. Description

In the IT context, the concept of "attack surface" or "exposure surface" refers to all the vulnerable points through which an attacker could potentially penetrate into a system or network.

Inspired by this notion, a second surface can be considered and adapted to the psychological domain: **the Psychological Attack Surface** (PAS).

The PAS is seen as complementary, in that it represents all the mental and behavioral vulnerabilities that cybercriminals can exploit to manipulate or deceive individuals.

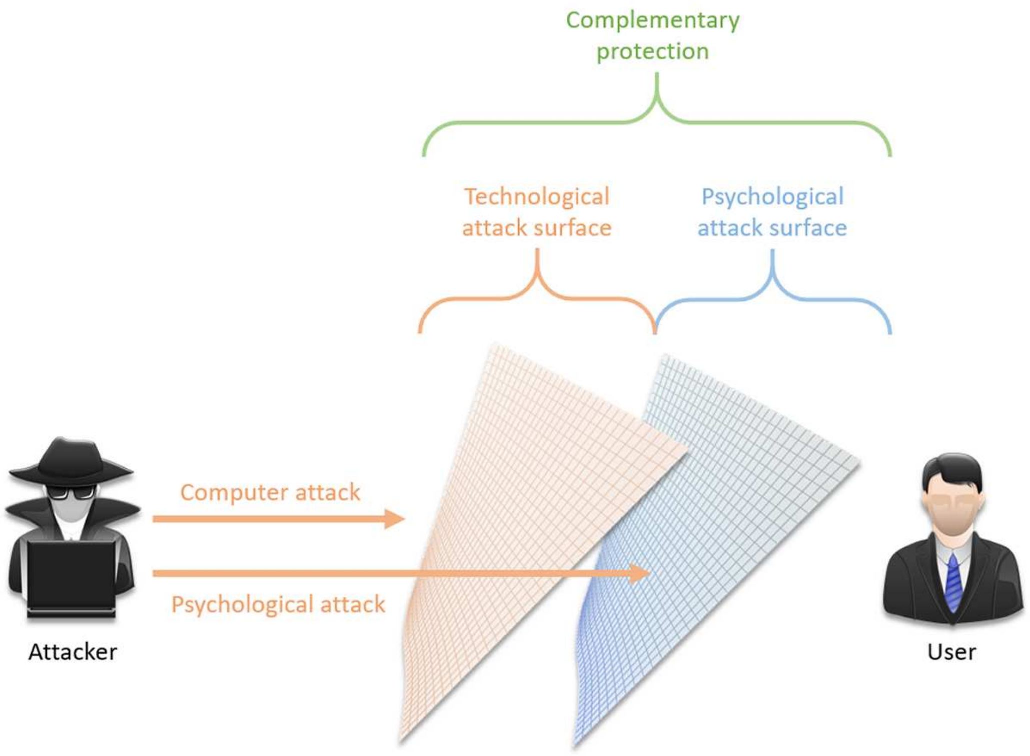
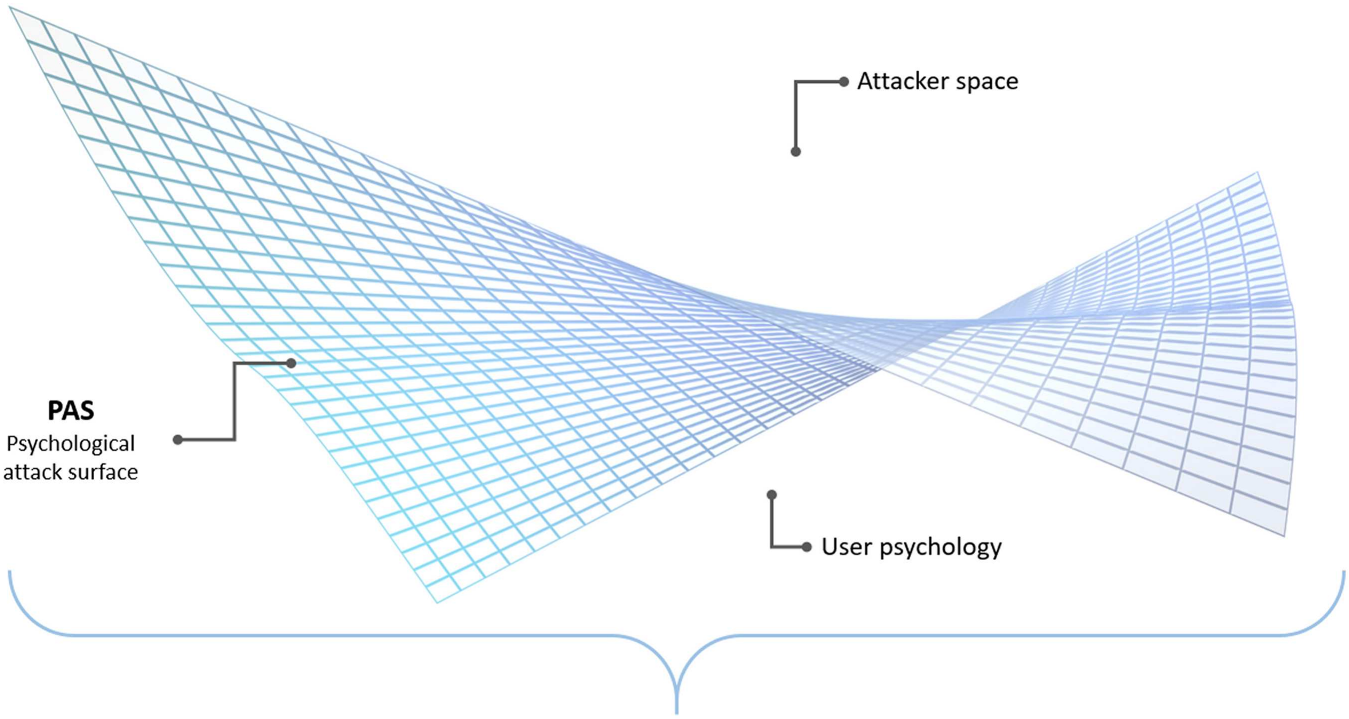


Figure 11. PAS: complementary protection.

3.3.2. Objective

The goal is to make PAS more **robust** and **minimise** its attack surface.

3.3.3. Understanding PAS: its vulnerabilities



Artistic depiction of the psychological attack surface (PAS): an abstract membrane that separates the attacker from the user's psychology.

Figure 12. PAS.

The psychological attack surface brings together the following vulnerable points (non-exhaustive) which can be exploited by the attacker during social engineering phases:

- **Habit**
  The usual way of acting.
- **Cognitive biases**
  Falsely logical thought pattern.
- **Weak self-regulation**
  Difficulty changing behavior.
- **Stress**
  Situation of excessive nervous tension which can prevent rationalisation.
- **Inexperience**
  The user has not been exposed to real examples of cyberattacks (psychological inoculation).
- **Emotional state**
  Strong emotions can disrupt reasoning.
- **Cyber-risk beliefs**
  A lack of belief in cyber-risks can encourage heuristic processing.
- **Heuristic**
  Using mental shortcuts to quickly formulate judgments or decisions.

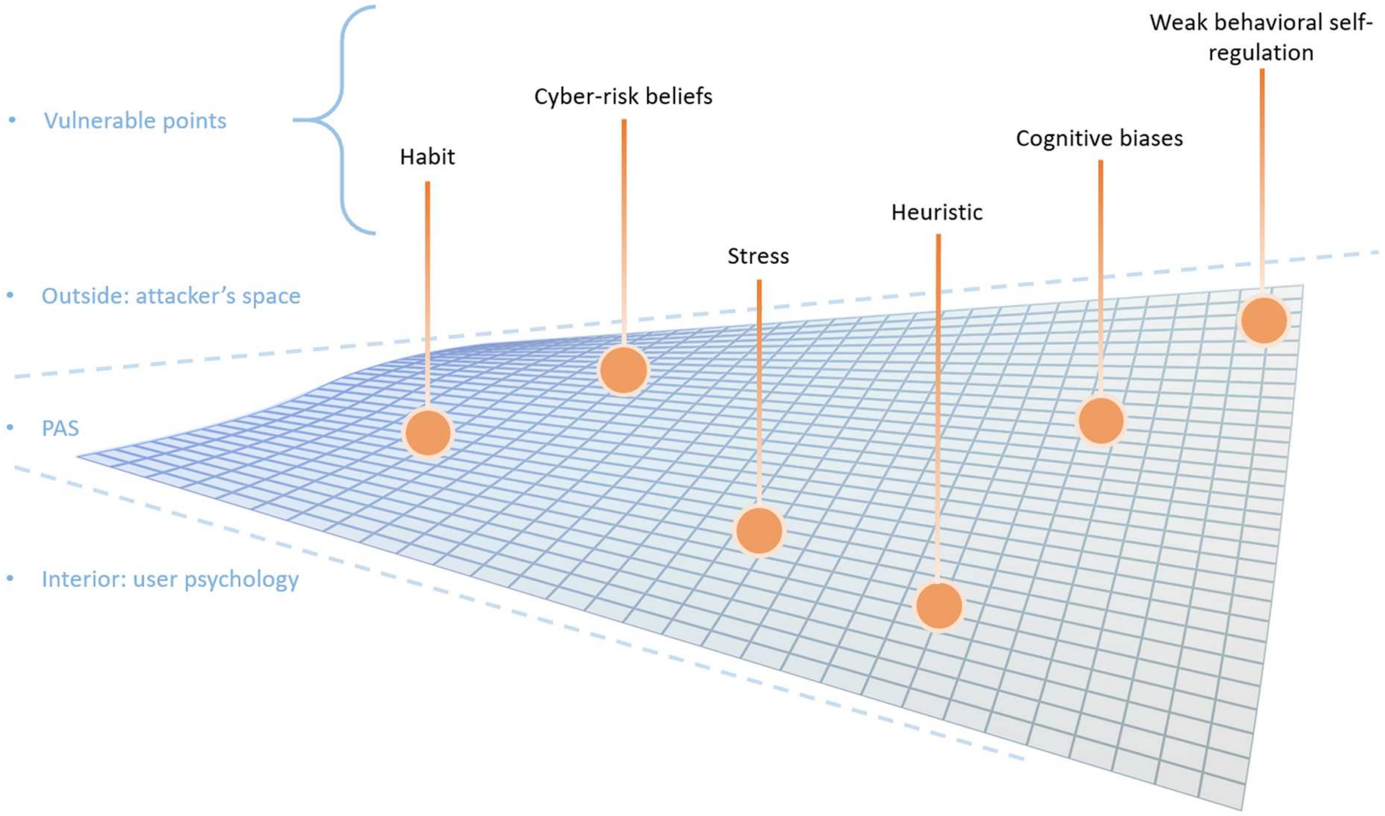

Vulnerable points
Outside: attacker's space
PAS
Interior: user psychology
Habit
Cyber-risk beliefs
Stress
Heuristic
Cognitive biases
Weak behavioral self-regulation

Figure 13. PAS.

3.3.4. Psychological preparation and prevention

An optimal reduction in the psychological attack surface would essentially rely on **psychoprophylaxis** of its users.

Psychoprophylaxis is psychological preparation aimed at preventing undesirable reactions that could disrupt the proper functioning of the body (Larousse, 2024). Applied in the cyber context this can be reformulated as follows: **cyberpsychological psychoprophylaxis** or **cyberpsychoprophylaxis.**

The theoretical framework of cyberpsychoprophylaxis could be established in 5 levels of improvement, the goal being to achieve hardening. These 5 levels are **SAISA** (the french version of the acronym): **Awareness / initiation**, **Learning**, **Psychological inoculation**, **Simulation** and **Hardening**.

SAISA
Psychological preparation
Awareness
Learning
Psychological inoculation
Simulation
Hardening

Figure 14. Cyberpsychoprophylaxis.

This psychological preparation would require coherent management of the PAS.

3.3.5. Planned management of PAS

PAS management could be carried out in six steps:

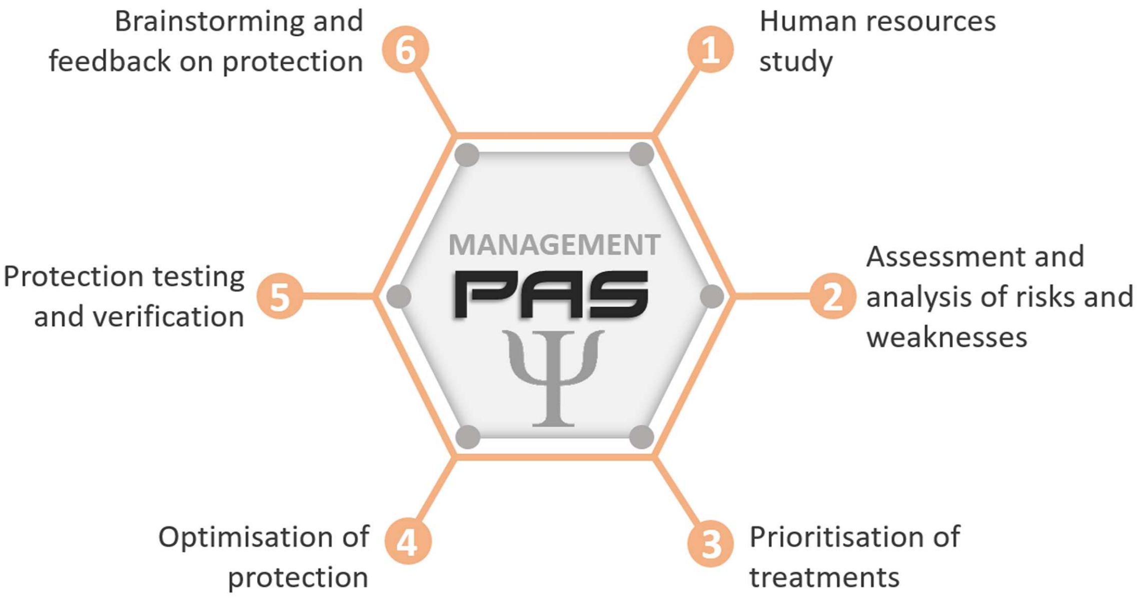

Human resources study
1
Assessment and analysis of risks and weaknesses
2
Prioritisation of treatments
3
Optimisation of protection
4
Protection testing and verification
5
Brainstorming and feedback on protection
6
MANAGEMENT
PAS
Ψ

Figure 15. PAS: management in six main steps.

- **1 - Human resources study**
  This involves taking into account the users affected by the psychological attack surface. For example, users who manage email and social media.

- **2 - Assessment and analysis of risks and weaknesses**
  This step consists of studying the psychological vulnerabilities of the users.

- **3 - Prioritisation of treatments**
  Depending on the workload required, it may be important to prioritise users most likely to be targeted by social engineering.

- **4 - Optimisation of protection**
  The objective of this step is to carry out all the necessary processing (presentations of tools and protection procedures, etc.).

- **5 - Protection testing and verification**
  Exercises and simulations can be applied to test user resistance to social engineering.

- **6 - Brainstorming and feedback**
  Listen to users' opinions and feelings regarding treatments (tools, aids, etc.). Feedback makes it possible to improve or reinforce certain actions. Brainstorming share new ideas and improvements.

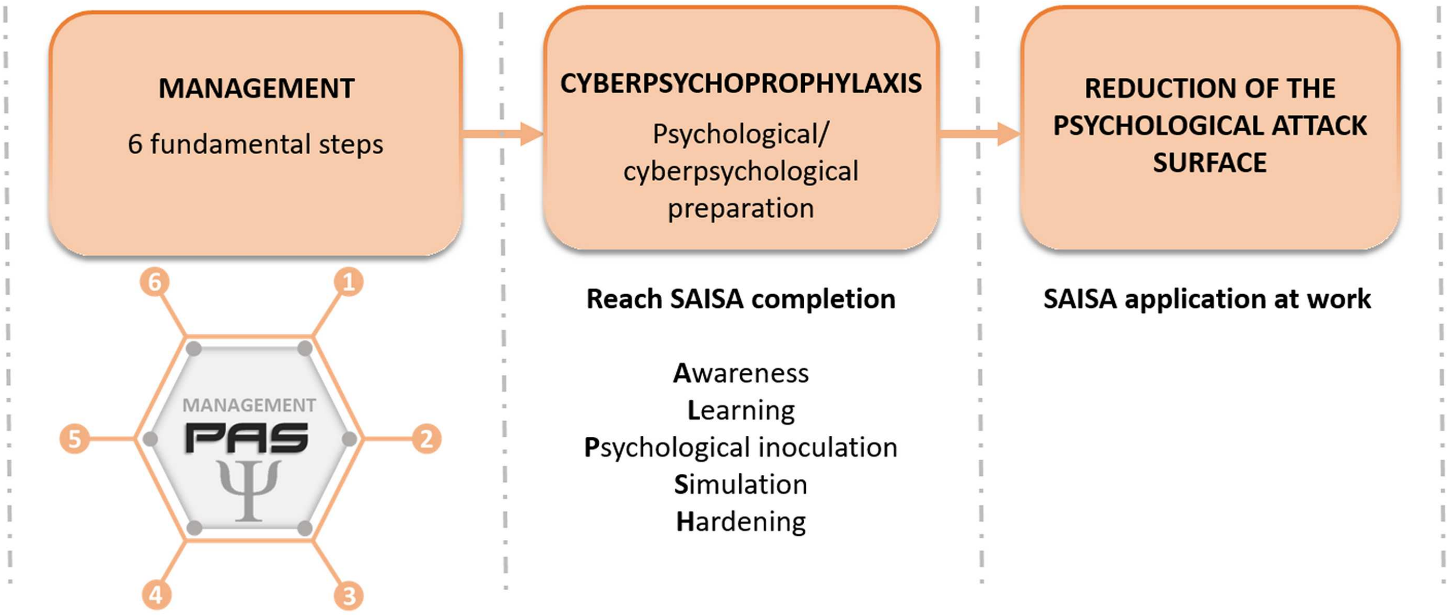

MANAGEMENT
6 fundamental steps
CYBERPSYCHOPROPHYLAXIS
Psychological/ cyberpsychological preparation
REDUCTION OF THE PSYCHOLOGICAL ATTACK SURFACE
6
1
MANAGEMENT
PAS
Ψ
5
2
4
3
Reach SAISA completion
Awareness
Learning
Psychological inoculation
Simulation
Hardening
SAISA application at work

Figure 16. From management to reduction of the attack surface.

3.3.6. Conclusion

The Psychological Attack Surface (PAS) brings together the different psychological vulnerable points through which an attacker could potentially manipulate an individual. Reducing this surface area would make it possible to counter the attacker's social engineering attempts. It is estimated that, to achieve an optimal reduction of this surface area, psychological preparation of users, called cyberpsychoprophylaxis, is essential.

A six-step management plan could help achieve this level of preparedness:

1. Human resources study,
2. Assessment and analysis of risks and weknesses,
3. Prioritisation of treatments,
4. Optimisation of protection,
5. Protection testing and verification,
6. Brainstorming and feedback on protection.

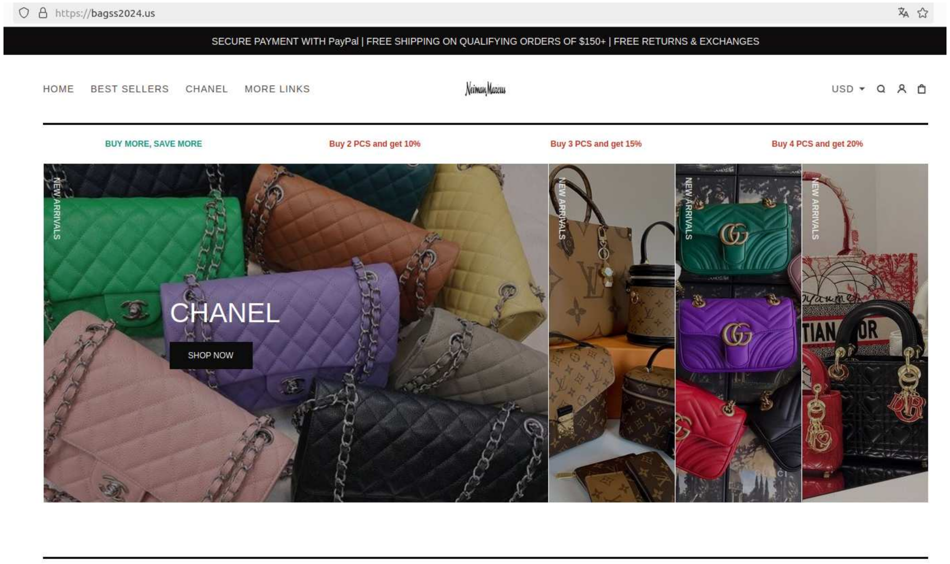
This process aims to strengthen the resilience of individuals in the face of psychological cyberattacks.

4. Copyscam: Big Sale in the Retail Sector

As part of monitoring the external attack surface of a ready-made clothing customer, aDvens' CERT has identified a scam campaign targeting the retail sector worldwide. The threat actor, dubbed Window Shopper, due to its strong propensity for targeting big names in the retail sector, appears to specialise in creating fake online sales websites that impersonate legitimate websites. Products at knockdown prices are offered to victims who are prompted to enter their credentials to log in and make payments. These payments are transferred to money laundering companies.

4.1. Victimology

The impersonated companies are mainly **Western brands** ranging from large commercial chains (Neiman Marcus, Lidl), to ready-to-wear companies such as Scotch & Soda and luxury brands such as Jimmy Choo or Jacquemus. There are also specialised websites offering sports items for sale (football, swimming or cycling), DIY tools or equipment. Window Shopper **targeted several French websites** but American (Amazon, Neiman Marcus, Cuyana, Victoria's Secret), Dutch (G-STAR, Scotch & Soda), Portuguese (Salsa Jeans), British (Jimmy Choo, ASOS), Australian (Ripcurl), Danish (Pandora), Spanish (Massimo Dutti) or even German (Lidl) brands are not spared.



https://bagss2024.us

SECURE PAYMENT WITH PayPal | FREE SHIPPING ON QUALIFYING ORDERS OF $150+ | FREE RETURNS & EXCHANGES

Figure 17. Example of an illegitimate website usurping Neiman Marcus brand.

4.2. Geographical location

All domain names were registered with the same IP address 104.18.73[.]116. The geolocation of this IP address is located in San Francisco, California. However, this information should be taken lightly as it comes from the Cloudflare content delivery network (CDN). Given the abundance of spoofed French domain names (Cabaïa, Cyrillus, Decathlon, Jacadi, Lacoste, Le Coq Sportif, Zadigue & Voltaire) in proportion to the other brands observed, it would seem that Window Shopper has a good knowledge of the French retail market. Furthermore, the repeated creation of domain names containing the name of the French president may suggest, with a moderate degree of confidence, that this threat actor is French. Indeed, it is one of the rare references that goes beyond the framework of the retail sector and the only one that has a political connotation of the whole wave of scams.

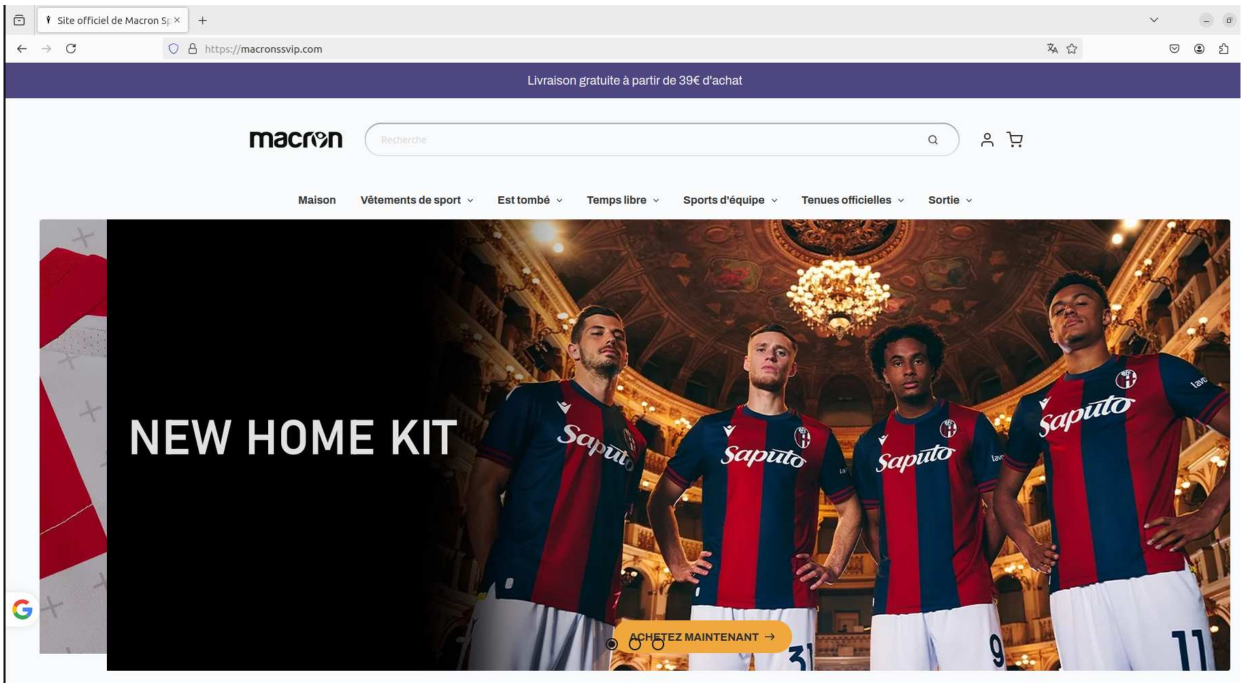


Figure 18. Screenshot of the home page of the illegitimate site macronssvip[.]com.

4.3. Modus operandi

4.3.1. IP address

The threat actor Window Shopper still uses the same IP address 104.18.73[.]116 (hosted at Cloudflare) to register its domain names. This modus operandi allowed aDvens' CERT to identify through reverse IP lookups hundreds of other domain names pretending to be retail companies. For this analysis, aDvens' CERT chose to work on a sample of 718 domain names, 342 of which are still active as of 20 September 2024.

4.3.2. Use of the typosquatting technique to register domain names

Window Shopper uses typosquatting to register its domain names. Typosquatting (MITRE ATT&CK: Acquire Infrastructure: Domains, T1583.001) is a social engineering attack technique that consists in registering domain names similar to legitimate domain names. The objective is twofold: to pretend to be the legitimate domain name and to capture part of the traffic addressed to it. The study of domain names purchased or created by the threat actor made it possible to identify a naming pattern around different forms of typosquatting:

- **spelling or typing error** within a word of the domain name
  (eg: vowel exchange, addition of characters in the domain name : garminstore[.]shop vs garmin[.]com).

- using a different **Top-Level Domain** (TLD)
  (eg : lecoqsport[.]shop vs lecoqsportif[.]com). The attacker's modus operandi shows a marked trend towards the use of .shop, .com and .top TLDs.

- **changing punctuation within the domain**
  added a hyphen to the domain name, removed a period from the domain name (eg : jimmychoo -eu [.]com vs row. jimmychoo[.]com.

Although frequently used by threat acters, the homoglyph technique - which consists in replacing a character that looks like another - is not used by Window Shopper.

The main domain name extensions (TLDs) represented are the following:

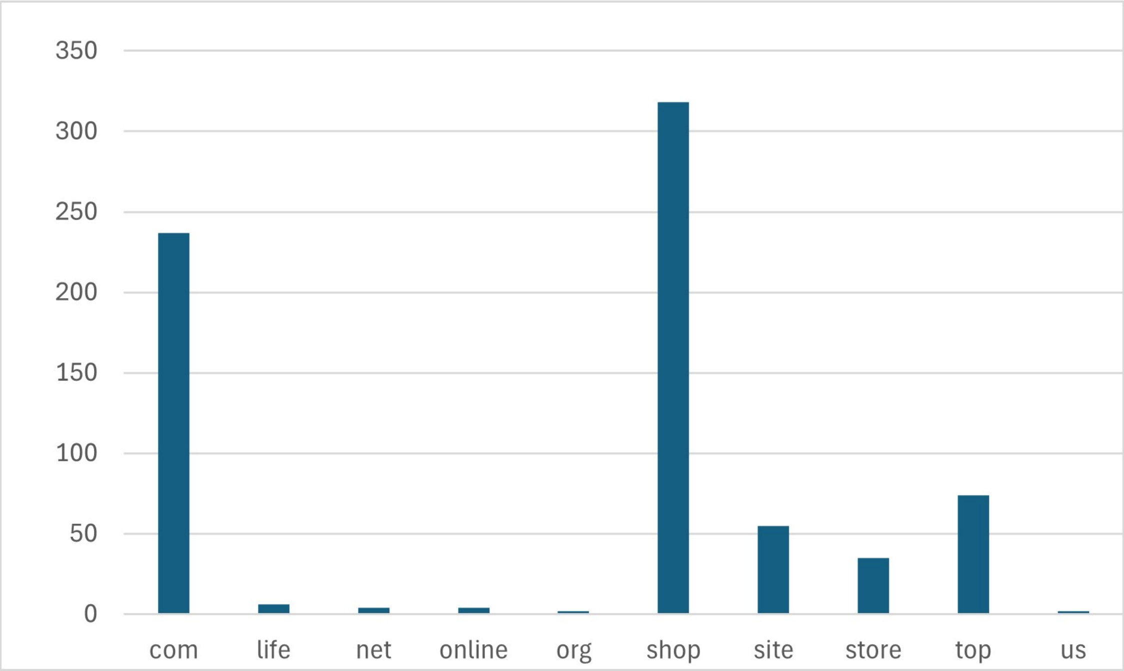


Figure 19. Top 10 TLDs. Source: aDvens' CERT.

4.3.3. Domain name creation date

The most widely used technique by the attacker is domain name registration. In some cases, the domain name creation dates suggest that Window Shopper purchased them. However, this technique is rarely used by the attacker and represents less than 1% of domain names. Almost 90% of the domain names analysed were registered during the year 2024. The others were mostly registered during the second half of 2023.

4.3.4. Retail site front panel

In their scam campaign, Window Shopper always uses the same modus operandi which consists of covering the domain names it has purchased or created with the front panel of legitimate websites. Some front panels of legitimate websites are also taken and affixed to fake brand names, invented by the cybercriminal.

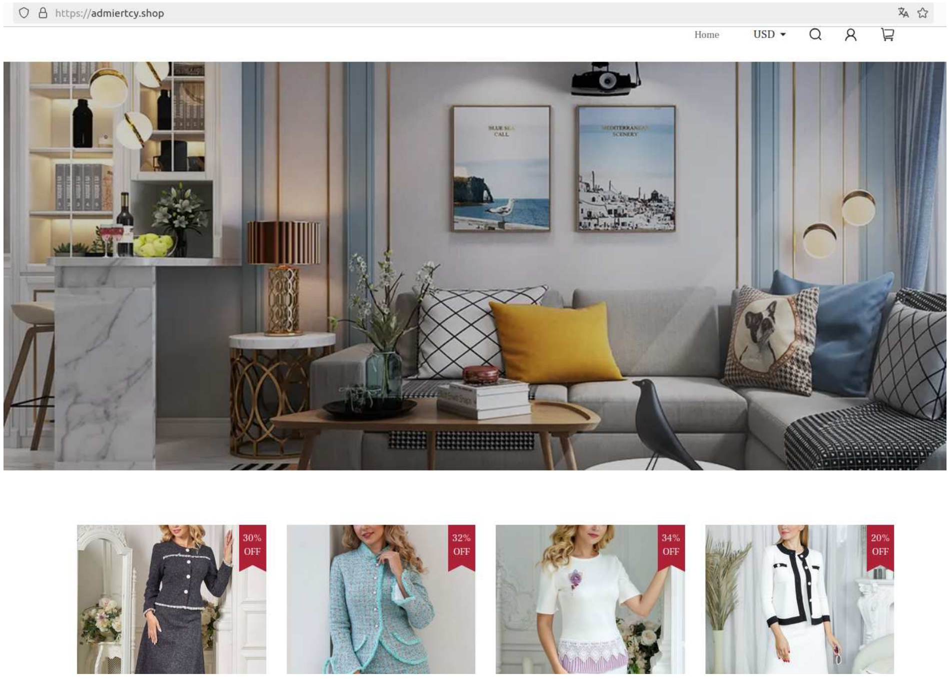


Figure 20. Website front panel taken over for multiple domain names created by the attacker.

Conversely, brand names may be used across different sites.

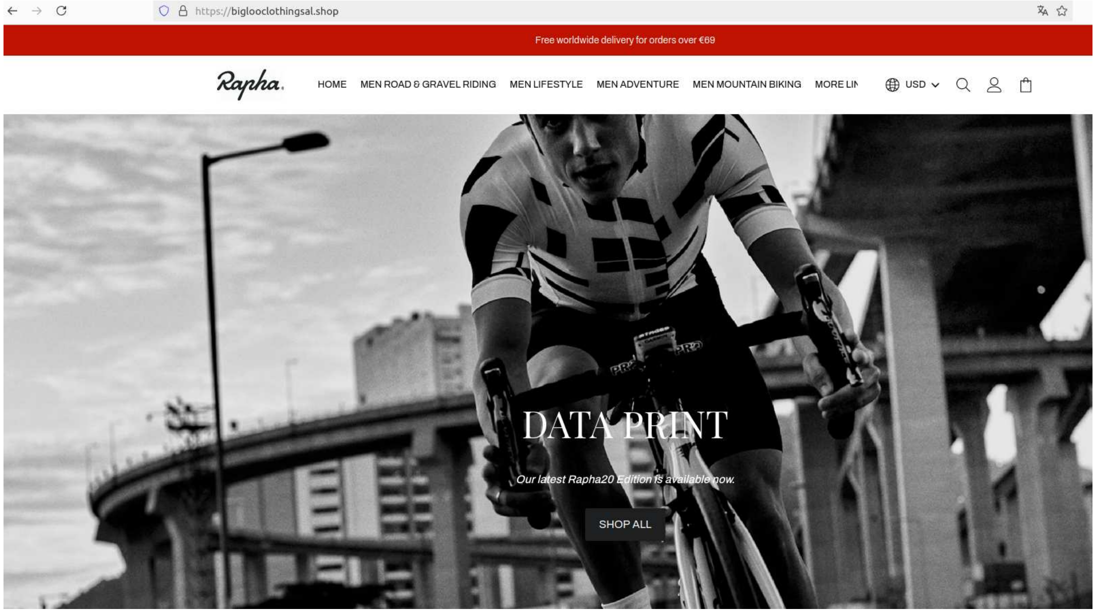
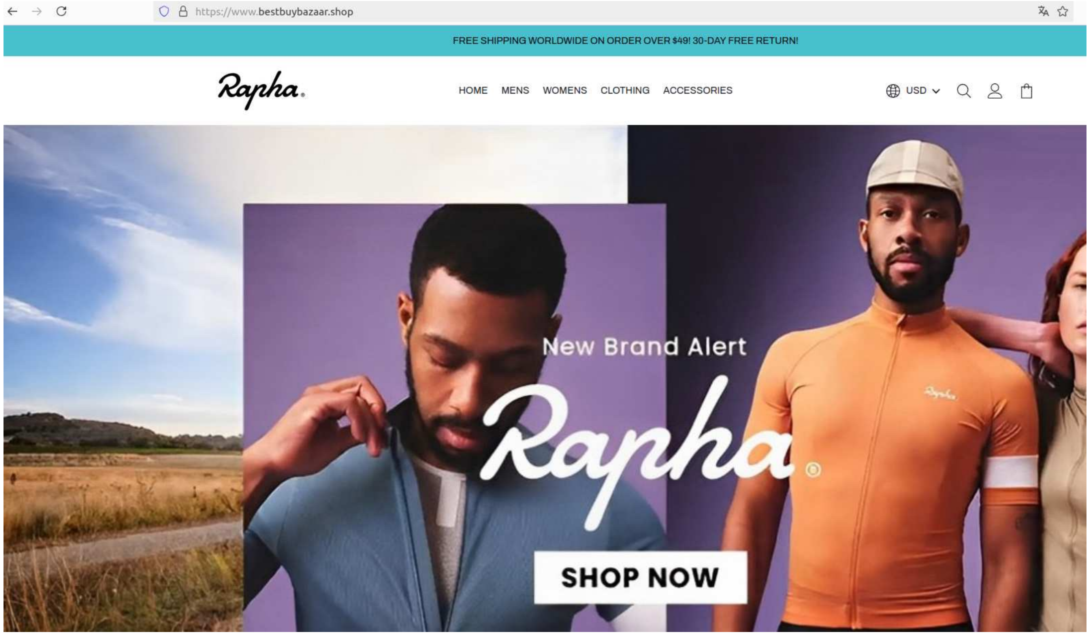

https://bigloclothingsal.shop
Free worldwide delivery for orders over €69
Rapha.
HOME
MEN ROAD & GRAVEL RIDING
MEN LIFESTYLE
MEN ADVENTURE
MEN MOUNTAIN BIKING
MORE LIN
USD
DATA PRINT
Our latest Rapha20 Edition is available now.
SHOP ALL

Figure 21. Front panel of different illegitimate website for the same brand name.


https://www.bestbuybazaar.shop
FREE SHIPPING WORLDWIDE ON ORDER OVER $49! 30-DAY FREE RETURN!
Rapha.
HOME
MENS
WOMENS
CLOTHING
ACCESSORIES
USD
New Brand Alert
Rapha.
SHOP NOW

aDvens' CERT was also able to identify clusters of domain names. Several domain names around the same theme were created in a short amount of time. Some can redirect to an illegitimate main domain name.

Nom de domaine	Statut	IP	Date de création	Registrar	Commentaire
bagsflash[.]com	Actif	104.18.73.116	18/11/2010	Namebright	Redirection vers bagstores[.]us
bagsgalaxy[.]com	Actif	104.18.73.116	07/07/2024	inwx	Redirection vers bagstores[.]us
bagss[.]us	Actif	104.18.73.116	08/07/2024	Dynadot	Redirection vers bagstores[.]us
bagstores[.]us	Actif	104.18.73.116	07/07/2024	Dynadot	Usurpation de Neiman Marcus

Figure 22. Example of cluster serial domain name creation and redirection to a main domain name. Source: aDvens' CERT.

4.3.5. Domain Name Registrar

More than 40 registrars were used to register the domain names of this scam campaign. This is high, if we take into account that Window Shopper uses only one IP address for the creation of its domain name. The main registrars used are Namesilo followed by Dynadoc Inc, Namecheap and Alibaba Cloud Computing. They alone account for more than half of the domain name registrations.

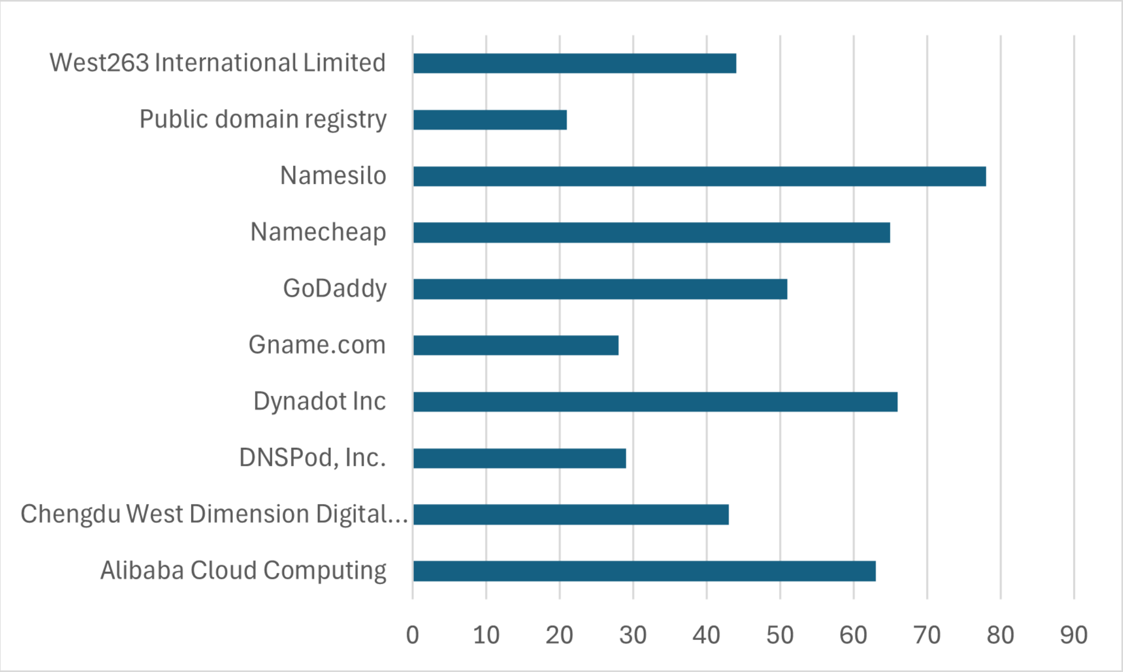
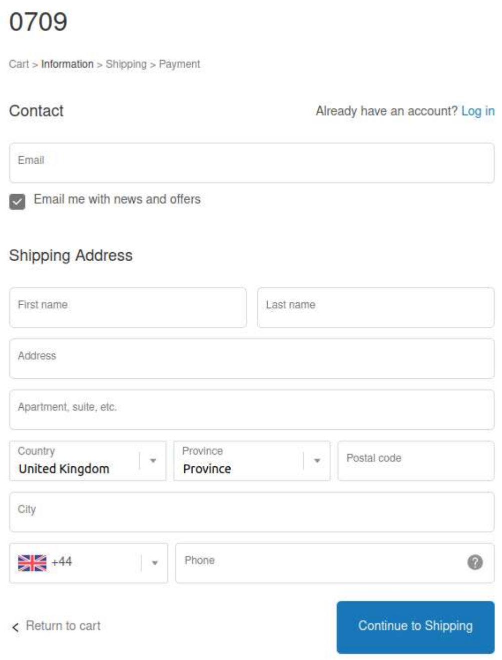


Figure 23. Top illegitimate domain name registrars. Source: aDvens' CERT.

4.3.6. Payment method

The victim is invited to pay for their purchases on the website's payment page. They must enter their personal data and bank details.



0709

Cart > Information > Shipping > Payment

Contact

Already have an account? Log in

Email

☑ Email me with news and offers

Shipping Address

First name

Last name

Address

Apartment, suite, etc.

Country
United Kingdom

Province
Province

Postal code

City

+44

Phone

< Return to cart

Continue to Shipping

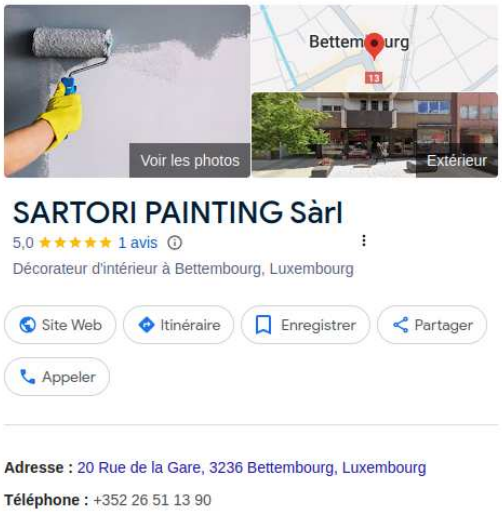
Figure 24. Example of a payment page on an illegitimate site.

Once the payment portal is displayed, aDvens' CERT was able to identify PayPal or Stripe payment portals. The latter is a payment service provider that allows companies to have an online payment solution on their website. To do this, the company must create a Stripe account that meets *Know Your Customer* (KYC) obligations.

4.3.7. Creation of companies to launder money

By conducting open source research, aDvens' CERT found that the names of the Stripe accounts displayed on the illegitimate sites referred to **shell companies probably created by the attacker**.

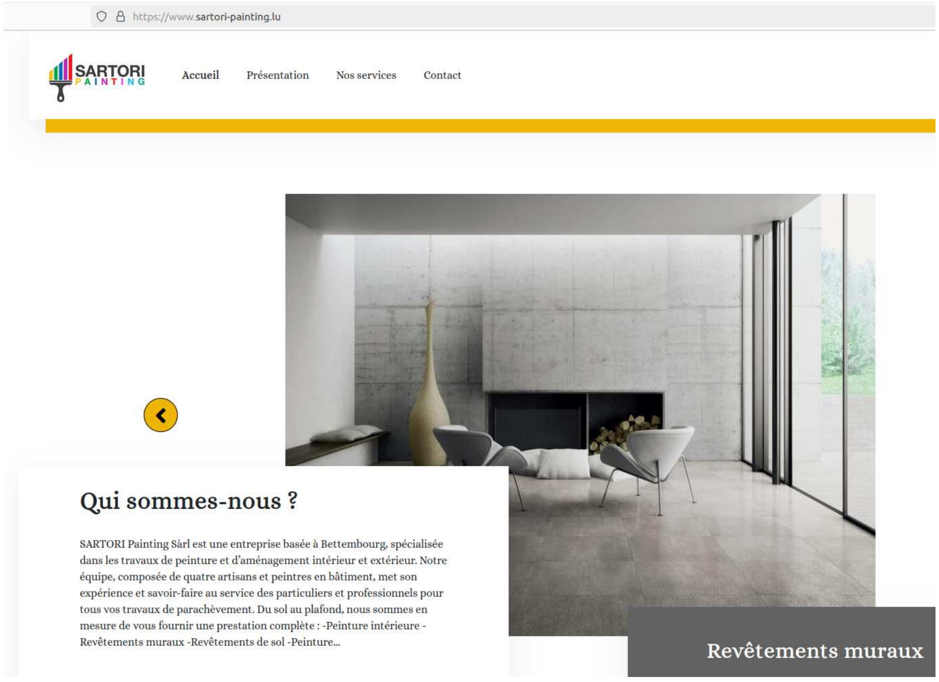
These shell companies include SARTORI PAINTING Sàrl, specialised in interior design and based in Luxembourg, or 29X LLC based in Colorado in the United States. 29X LLC is registered in the name of Victoria Shell (for anonymity reasons, aDvens' CERT used an alias). This person appears on Linkedin as working as an executive assistant at Adaapta, an environmental consulting firm located at the same address as the one registered for 29X LLC. It is likely that the threat actor spoofed this information to register a fictitious company.



SARTORI PAINTING Sàrl
5,0 ★★★★★ 1 avis
Décorateur d'intérieur à Bettembourg, Luxembourg

Adresse : 20 Rue de la Gare, 3236 Bettembourg, Luxembourg
Téléphone : +352 26 51 13 90

Figure 25. Contact information for Sartori Painting collected from open source intelligence.



Qui sommes-nous ?

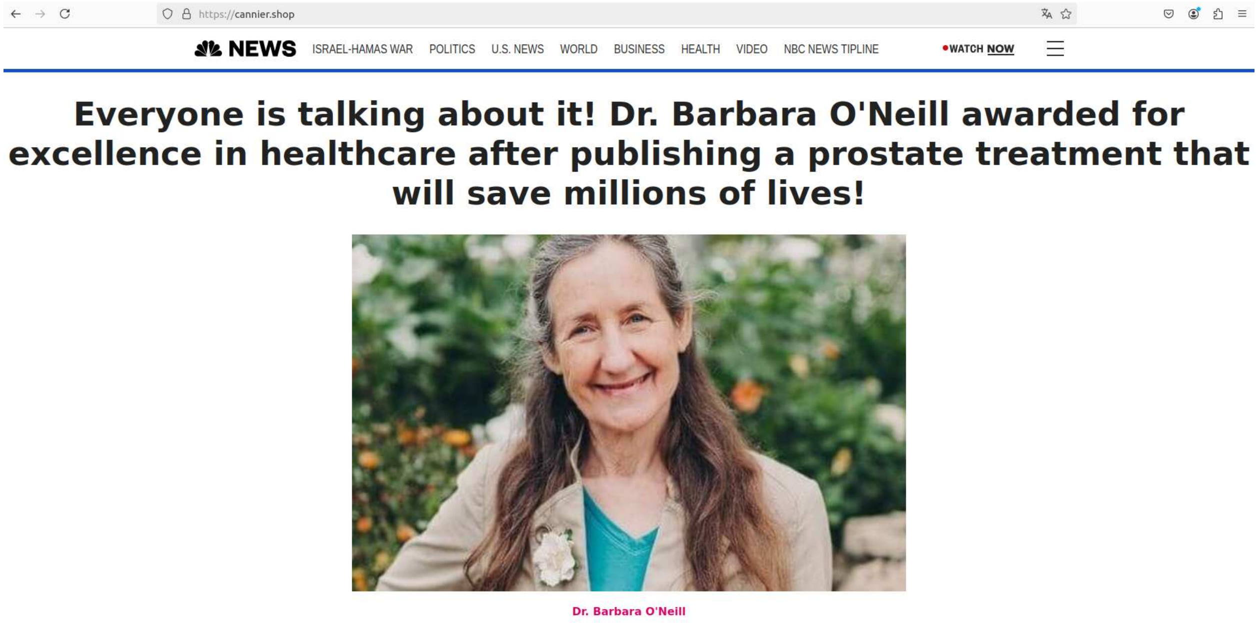
SARTORI Painting Sàrl est une entreprise basée à Bettembourg, spécialisée dans les travaux de peinture et d'aménagement intérieur et extérieur. Notre équipe, composée de quatre artisans et peintres en bâtiment, met son expérience et savoir-faire au service des particuliers et professionnels pour tous vos travaux de parachèvement. Du sol au plafond, nous sommes en mesure de vous fournir une prestation complète : -Peinture intérieure -Revêtements muraux -Revêtements de sol -Peinture...

Revêtements muraux

These shell companies allow the threat actor to launder the money earned from the fake online sales websites. This means that they have passed Stripe's verification barrier without being detected. Actions carried out by aDvens' CERT are underway with Stripe to alert them of the activities of these companies.

4.3.8. A campaign that goes beyond the retail website scam

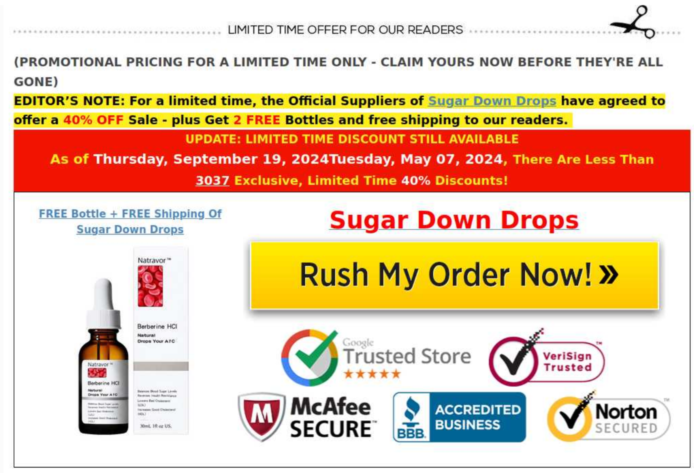
Surprisingly, the IP address 104.18.73[.]116 has occasionally been used for health scams. The same narrative on diabetes is relayed by several disinformation websites that usurp the logos of the American audiovisual channels NMC and MSNBC. The goal of this scam is to sell a miracle product against this chronic disease.



Everyone is talking about it! Dr. Barbara O'Neill awarded for excellence in healthcare after publishing a prostate treatment that will save millions of lives!

Dr. Barbara O'Neill

Figure 26. Screenshot of a health scam on an illegitimate website impersonating an audiovisual channel



LIMITED TIME OFFER FOR OUR READERS

(PROMOTIONAL PRICING FOR A LIMITED TIME ONLY - CLAIM YOURS NOW BEFORE THEY'RE ALL GONE)

EDITOR'S NOTE: For a limited time, the Official Suppliers of Sugar Down Drops have agreed to offer a 40% OFF Sale - plus Get 2 FREE Bottles and free shipping to our readers.

UPDATE: LIMITED TIME DISCOUNT STILL AVAILABLE

As of Thursday, September 19, 2024Tuesday, May 07, 2024, There Are Less Than 3037 Exclusive, Limited Time 40% Discounts!

FREE Bottle + FREE Shipping Of Sugar Down Drops

Sugar Down Drops

Rush My Order Now! »

Domain name	Usurped Media
cannier[.]shop	NBC
cinerrty[.]shop	MSNBC
cuineer[.]shop	MSNBC
hotheimall[.]com	-

5. Sources

CVE-2024-40711

- https://www.veeam.com/kb4649
- https://censys.com/fr/cve-2024-40711/
- https://nvd.nist.gov/vuln/detail/cve-2024-40711

CVE-2024-40766

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015
- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-011/
- https://nvd.nist.gov/vuln/detail/cve-2024-40766

CVE-2024-6670

- https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-August-2024
- https://nvd.nist.gov/vuln/detail/cve-2024-40766

Article Cyberpsychology Article : main used source

- Ribeiro, L., Guedes, I. S., Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *136*. *Computers & Security*.
https://www.sciencedirect.com/science/article/pii/S0167404823004686#bib0077

Cyberpsychology article - Definition

- Congnitive (LeRobert, 2024).
https://dictionnaire.lerobert.com/definition/cognitif
- Cyberespace (LeRobert, 2024).
https://dictionnaire.lerobert.com/definition/cyberespace
- Cyberpsychology (Bouchard, 2016).
https://www.cairn.info/revue-rhizome-2016-3-page-17.htm
- Heuristic and Systematic (Cuofano, 2024).
https://fourweekmba.com/fr/mod%C3%A8le-syst%C3%A9matique-heuristique/
- Postmodernity (Yousfi, 2013).
https://www.scienceshumaines.com/les-penseurs-de-la-postmodernite_fr_30366.html
- Psychoprophylaxis (Larousse, 2024).
https://www.larousse.fr/dictionnaires/francais/psychoprophylaxie/64875

Cyberpsychology article - Routine Activity Theory

- Graham, R., Triplett, R. (2016) . Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Research Gate*. *38*(12), 1-12.
https://www.researchgate.net/publication/310737084_Capable_Guardians_in_the_Digital_Environment_The_Role_of_Digital_Literacy_in_Reducing_Phishing_Victimization
- Leukfeldt, E. R., Yar, M. (2014) . Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Taylor & Francis Online*. *37*(3), 263-280.
https://www.tandfonline.com/doi/full/10.1080/01639625.2015.1012409
- Mathieu, C., Trudel, Yves. (2021). Cycles des crimes financiers et théorie des activités routinières / Chaire Desjardins en finance responsable. Cahier de recherche de l'Université de Sherbrooke. *BAnK numérique*.
https://collections.banq.qc.ca/ark:/52327/4663843
- Miró, F. (2014). Routine Activity Theory.*Wiley Online Library*.
https://onlinelibrary.wiley.com/doi/full/10.1002/9781118517390.wbetc198
- Miró-Llinares, F. (2014). Routine Activity Theory. *Research Gate*.
https://www.researchgate.net/profile/Fernando-Miro-Llinares/publication/328839261_Routine_Activity_Theory/links/5be5baf892851c6b27b295ac/Routine-Activity-Theory.pdf

- Routine activity theory (2024). In *Wikipedia*.
https://en.wikipedia.org/wiki/Routine_activity_theory
- Saini, N. (2016). Routine activity theory. *Slide Share*.
https://fr.slideshare.net/slideshow/routine-activity-theory/61245486#2
- Yar, M. (2005). The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory. *Sage Journals Home*. *2*(4).
https://journals.sagepub.com/doi/10.1177/147737080556056

Cyberpsychology article - Heuristic-Systematic Model of information processing

- Heuristic-systematic model of information processing (2024). In *Wikipedia*.
https://en.wikipedia.org/wiki/Heuristic-systematic_model_of_information_processing
- Le modèle de Traitement Heuristique Systématique de l'information : motivations multiples et régulation du jugement en cognition sociale. *L'Année psychologique*. 527-563.
https://www.persee.fr/doc/psy_0003-5033_2000_num_100_3_28658
- Chen, S., Duckworth, K., & Chaiken, S. (1999). Motivated Heuristic and Systematic Processing. *Psychological Inquiry*. *10*(1), 44-49.
https://static1.squarespace.com/static/50f6f441e4b08191027c661d/t/50fffc41e4b047a6c79e9e41/1358953537000/ChenDuckworth%26Chaiken1999PsychInquiry.pdf
- Tanner, L. (2005) L'étude d'un chercheur du Vermont soulève des questions sur les tactiques publicitaires des hôpitaux. *Rutlandherald*.
https://www-rutlandherald-com.translate.goog/news/vermont-researchers-study-raises-questions-about-hospitals-ad-tactics/article_77252f1d-f130-59b7-abda-d75a9b931642.html?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc
- Suri, R., Monroe, K. B. (2008). The Effects of Time Constraints on Consumers' Judgments of Prices and Products. *Journal of Consumer Research*. *30*(1), 92-104.
https://www.researchgate.net/publication/221599956
- Vishwanath, A., Herath, T., Chen, R., Wang, J., RaoWhy, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*. *51*(3), 576-586.
https://www.sciencedirect.com/science/article/abs/pii/S016792361100090X
- Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research*. *45*(8), 1146-1166.
https://www.researchgate.net/publication/278676335_Suspicion_Cognition_Automaticity_Model_SCAM_of_Phishing_Susceptibility
- Zanna, M. P., Olson, J. M., Herman, C. P. (1987). Social Influence : The Ontario Symposium, Volume 5. *Routledge*. *5*.
https://www.routledge.com/Social-Influence-The-Ontario-Symposium-Volume-5/Zanna-Olson-Herman/p/book/9780898596786

Cyberpsychology article - Suspicion, cognition, and automaticity model

- Griffin, R. J., Neuwirth, K., Giese, J., & Dunwoody, S. (2002). Linking the heuristic-systematic model and depth of processing. *Communication Research*, 29, 705-732.
https://epublications.marquette.edu/cgi/viewcontent.cgi?params=/context/comm_fac/article/1230/&path_info=griffin_6460pub.pdf
- Lyons, J. B., Stokes, C. K., Eschleman, K. J., Alarcon, G. M., & Barelka, A. J. (2011). Trustworthiness and IT Suspicion: An evaluation of the nomological network. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 53, 219-229.
https://www.researchgate.net/publication/51560765_Trustworthiness_and_IT_Suspicion_An_Evaluation_of_the_Nomological_Network
- Vishwanath, A., Harrison, B., Ng, Y. J.(2018). Suspicion, Cognition, Automaticity Model (SCAM) of Phishing Susceptibility. *Communication Research*. *45*(8).
https://www.researchgate.net/publication/278676335_Suspicion_Cognition_Automaticity_Model_SCAM_of_Phishing_Susceptibility#pf4