TLP:CLEAR
PAP:CLEAR

ATTACK CAMPAIGNS OF THE APT28 OPERATING MODE SINCE 2021

ILLUSTRATION OF THE THREAT AND RECOMMENDATIONS SECURITY

1.0

October 26, 2023

TLP:CLEAR
PAP:CLEAR

Summary

1. Summary

During its investigations, ANSSI analyzed several attack mode 1 compromise chains used for espionage including purposes. Some campaigns have been directed against French *APT28* organizations (MOAs) , government entities, businesses, universities, as well as research institutes and *think tanks.*

If attackers continue their brute force attack and vulnerability exploitation campaigns, ANSSI also notes that attackers reduce the risk of detection by compromising equipment that is poorly monitored and located on the periphery of the network 2 . In some cases, no backdoors are dropped on the compromised network.

This document is based on technical reports published in open source and elements collected during incident response operations carried out by ANSSI. It details the tactics, techniques and procedures (TTP) characteristic of the modus operandi's activities since the second half of 2021 (section 2) and offers a series of recommendations to protect against this type of attack (section 3).

1. Also known as *UAC-0028, Fancy Bear, FrozenLake, Sednit, Sofacy* or *Pawn Storm.*
2. Routers, gateways and mail servers, firewalls, *etc.*

2 Tactics, techniques & procedures

2.1 Recognition

During its investigations, ANSSI identified different recognition techniques used by *APT28.*

The modus operandi is based on the use of compromised email accounts to carry out phishing campaigns [T1597] [1, 2, 3, 4]. In some cases, the usernames and passwords of these accounts are present in data leak databases.

APT28 is also used in brute force attacks [T1110.003, T1110.004]. MOA operators largely target personal email accounts [2, 5, 6, 7, 8, 9]. These campaigns are intended to massively recover connection information *(credentials harvesting)* in order to feed attack dictionaries.
This information is then reused to target employee accounts.

In a campaign documented in late April 2023, *APT28* operators distributed phishing emails instructing users to update their systems by executing instructions in **PowerShell** language [8].
These instructions downloaded and ran a script containing two commands:

- tasklist, which allows you to list all the processes currently running; • systeminfo, which allows you to display detailed configuration information about a computer and its operating system. This information contains, for example, the list of installed security patches.

The script containing the two commands above was hosted on “mocky[.]io”. The results of the commands were sent to “mockbin[.]org”. MOCKY and MOCKBIN are public services for generating web endpoints to test, track, and simulate an HTTP request or response. The objective of the MOA operators was probably to recover information about the IT environment of their targets in order to subsequently carry out a larger attack against these information systems [8].

2.2 Capacity development

ANSSI identifies at least three areas of *APT28* capacity development :

- searching for zero *-day* vulnerabilities [T1212, T1587.004]; • the compromise of routers and personal email accounts [T1584.005, T1586.002]; • the use of open source tools and online services [T1588.002, T1583.006].

ANSSI investigations confirm *that APT28* exploited the *0-day* vulnerability CVE-2023-23397 affecting the Outlook for Windows product from March 2022 until June 2023.

According to other partners, during this period, the MOA would also have exploited other vulnerabilities, such as that affecting Microsoft Windows Support Diagnostic Tool (MSDT, CVE-2022-30190, also called Follina) as well as those targeting the Roundcube application (CVE-2020-12641, CVE-2020-35730, CVE-2021-44026) [1, 2, 10].

MOA operators build and maintain part of their attack infrastructures by compromising routers and personal email accounts of individuals and businesses (see section 2.1). These accesses mainly serve as a rebound to achieve strategic targets. MOA operators used compromised email accounts to send malicious emails and compromised routers to recover exfiltrated data.

During the CVE-2023-23397 vulnerability exploitation campaign , ANSSI was able to confirm *that APT28* employed at least twelve email accounts belonging to companies and eleven compromised Ubiquiti routers:

APT28 modus operandi attack campaigns since 2021

Issuer	MD5 file	Sending date	URI	Compromised router
maint[@]goldenloafuae[.]com	9f4172d554bb9056c8ba28e32c606b1e	2022-03-18	\\5.199.162.132\SCW	5,199,162,132
accounts[@]regencyservice[.]in	3d4362e8fe86d2f33acb3e15f1dad341	2022-04-14	\\101.255.119.42\event\2431	101.255.119.42
vikram.anand[@]4ginfosource[.]com	f60350585fbfc5dc968f45c6ef4e434d	2022-05-17	\\101.255.119.42\mail\a5b3553d	101.255.119.42
Unknown	92e22b7e96aca3f9d733ca609ab0b589	2022-10-05	*Unknown*	213.32.252.221
franch1.lanka[@]bplanka[.]com	43a0441b35b3db061cde412541f4d1e1	2022-10-25	\\168.205.200.55\test	168.205.200.55
mdelafuente[@]ukwwfze[.]com	9a97c56c9ea6d9ebde0968580ea28ea9	2022-10-25	*Unknown*	213.32.252.221
karina[@]bhpcapital[.]com	e68cbd4930e2781e0c1b19eb72ec0936	2022-10-26	*Unknown*	213.32.252.221
m.salim[@]tsc-me[.]com	b21dde4c19e2f6fc08a922e25de38cf5	2022-12-01	\\185.132.17.160\aojv43	185.132.17.160
ashoke.kumar[@]hbclife[.]in	b5d82be5813c7dacbd97ef5df073b260	2022-12-14	\\69.51.2.106\report	69.51.2.106
jayan[@]wizzsolutions[.]com	2bb4c6b32d077c0f80cda1006da90365	2022-12-29	\\113.160.234.229\istanbul	113.160.234.229
m.yasser[@]egymatec[.]ae	238334590d0f62d2a089bd87ad71b730	2023-03-15	\\85.195.206.7\lrmng	85.195.206.7
commercial[@]vanadrink[.]com	7ee19e6bd9f55ebc0dd6413c68346de6	2023-03-17	\\85.195.206.7\power	85.195.206.7
commercial[@]vanadrink[.]com	3b698278f225f1e5bace9d177a1a95e0	2023-03-21	\\61.14.68.33\rem	61.14.68.33
Unknown	ce65c51078b7c69a6f50b0b37a36293f	2023-03-28	\\24.142.165.2\req	24.142.165.2
m.nash[@]islandsailors[.]com	65fdbc35bc8c3a2f0e872dbbfd32c7a7	2023-03-29	\\42.98.5.225\ping	42.98.5.225

Fig. 2.1 – List of emails identified by ANSSI exploiting CVE-2023-23397.

During incident responses, ANSSI was able to confirm the use of the **Mimikatz** and **reGeorg** malicious tools by *APT28 :*

- **Mimikatz** is a tool which can be used in particular to extract stored passwords (or their fingerprints). in memory under Windows;
- **reGeorg** is a tunnel creation tool exploiting a compromised HTTP server on which a script (PHP, ASPX, JSP, etc.) is installed to relay traffic for other protocols (example: RDP, SSH, SMB) and thus bypass certain filtering rules.

Public reports indicate *that APT28* used the open source **Empire** framework when deployment of the **Graphite implant,** specific to the operating mode [11].

The use of these tools is part of a broader use of services available in open source. *APT28* relies on several hosting services such as “neocities[.]org”, “frge[.]io”, “tinyhost[.]fr”, “mockbin[.]org”, “mocky[.]io”, as well as the free hosting service INFINITYFREE [5, 8]. Other services of the same type may have been used by *APT28.* ANSSI also observes the reuse of domain names and servers between different campaigns since 2021.

Finally, *APT28* relies on a set of virtual private network *(VPN)* services for its malicious activities (account logins, brute force attacks, exploitation of vulnerabilities). These service providers *VPNs* accept cryptocurrencies and highlight the non-traceability of data [12, 13].

A non-exhaustive list of *VPN* services used by the MOA is available below:

Trusted VPNs	
SurfShark	Strong
ExpressVPN	Strong
CactusVPN	Strong
ProtonVPN	Strong
PrivateVPN	Moderate
IPVanish	Moderate
NordVPN	Moderate
WorldVPN	Weak
PureVPN	Weak
VPNSecure	Weak

Fig. 2.2 – List of *VPN* services probably used by *APT28.*

2.3 Initial access

ANSSI observes three main initial access methods used by the MOA since 2021:

- sending phishing emails redirecting to a fake authentication page;
- sending emails exploiting vulnerabilities in the email client;
- targeting authentication interfaces through the use of valid credentials or brute force attacks.

APT28 has been used on numerous occasions to conduct targeted phishing campaigns [T1566]. These campaigns rely in particular on social engineering techniques to redirect victims to pages to retrieve connection information. For example, MOA operators created phishing pages imitating the Office 365 login page of the targeted entities.

The MOA also distributed phishing emails with the aim of exploiting vulnerabilities in the client of messaging. Some vulnerabilities 3 do not require action from the user. The subject of these emails is often built around a single term: “Silence. », “Celebration”, “Interest. ”, *etc.*

These observations corroborate the phishing activities linked to the operating mode and documented in open source by counterparts of ANSSI and publishers of security solutions, including CERT-UA, CLUSTER25 and TRELLIX [2, 3, 14, 15, 11].

Since at least 2020, brute force attacks have been one of the methods most used by *APT28* [T1190]. ANSSI investigations confirm that the MOA carried out this type of attack against email servers and firewalls exposed on the Internet using password dictionaries.

In other cases, the MOA identified legitimate accounts and logged into them after the brute force attack or by successful enumeration of current passwords *(password spraying)* (see section 2.1) [T1078]. These actions are carried out through *VPN* services or the Tor anonymization network with infrastructures that can understand more than 1000 different IP addresses [16, 13].

2.4 Exploitation, persistence & privilege escalation

The *APT28* operating mode is able to exploit vulnerabilities in order to gain privilege on workstations compromised clients, servers or equipment.

In one of the incidents involving the MOA, ANSSI identified the exploitation of vulnerabilities CVE-2020-0688 And CVE-2020-17144 against an Exchange server exposed through an *Outlook Web Access* (OWA) interface. THE

3. Including CVE-2023-23397.

MOA exploited these vulnerabilities from a valid account in order to execute code remotely on the server. The **reGeorg** tool was notably used to maintain access to the server [T1505.003].

To remain on the compromised network, *APT28* also creates user accounts [T1136] which, for example, imitate the identity of the targeted entity or use generic terms such as “guest”, “admin”, *etc.*

Beyond these observations, the MOA is known to have used more advanced techniques. The *APT28* **Graphite** implant would, for example, employ a *Component Object Model (COM) Hijacking* [T1546.015][4] technique as a persistence mechanism [11].

MOA operators generally identify unmonitored areas in the victim's information system to maintain themselves and perform collection and exfiltration actions. Certain MOA implants such as **CredoMap** and the codes deployed to exploit vulnerabilities in the Roundcube application directly collect and exfiltrate the information sought without implementing any means of persistence.

However, ANSSI was able to note in its incident responses that several *APT28* campaigns did not use any specific code or mechanism to maintain access to the victim's network, gain privilege or become lateralized. In certain cases, the attacker carries out data exfiltration directly (see section 2.6).

2.5 Collection & command and control mechanisms

To collect data, *APT28* uses both generic tools and a set of malicious codes specific to the operating mode. During the attack campaign against Exchange servers, ANSSI was able to observe the use of TTPs already documented in open source [13, 17], including:

- recovery of authentication secrets stored in the memory of the LSASS process, either by using the **Mimikatz tool,** or by using the MiniDump function of the “comsvcs.dll” library [T1003.001];
- the use of native utilities like “ntdsutil.exe” to recover the contents of the database [T1003.003];
- the use of the “certutil.exe” tool to download remote resources in the compromised environment[5] [T1105];
- recovery of the contents of the email boxes of personalities of interest probably identified in Active Directory[5] upstream.

ANSSI carried out an analysis of CVE-2023-23397 following the publication by MICROSOFT [18]. Exploitation by *APT28* consists of sending emails or Outlook meeting requests in order to trigger an SMB connection [4, 19]. Targeted accounts automatically attempt authentication with an SMB service controlled by the attacker. This authentication allows it to retrieve the Net-NTLMv2 authentication digest. The attacker is then able to relay this fingerprint to other services supporting this type of authentication [T1528].

APT28's command and control (C2) infrastructure relies in particular on legitimate services. For example, the **Graphite** and **DriveOcean** implants used by the MOA rely respectively on OneDrive and Google Drive services [14, 20]. This technique allows attackers to reduce the risk of detection. It is also more difficult for an entity to prohibit traffic to these services.

Finally, the MOA probably recovers a set of access data *via* its phishing campaigns against individual email boxes or the use of its **CredoMap implant,** which allows the collection of browser identifiers and cookies. These data are probably used *a posteriori* to carry out compromises on a larger scale or to be permanently installed in an information system [T1555.003, T1539] [5].

4. COM objects are WINDOWS mechanisms allowing software to interact with each other through the operating system.
5. “certutil.exe” and “ntdsutil.exe” are legitimate binaries present on the system whose use is being misused here (commonly called *Living Off The Land Binary* and abbreviated LOLBin).

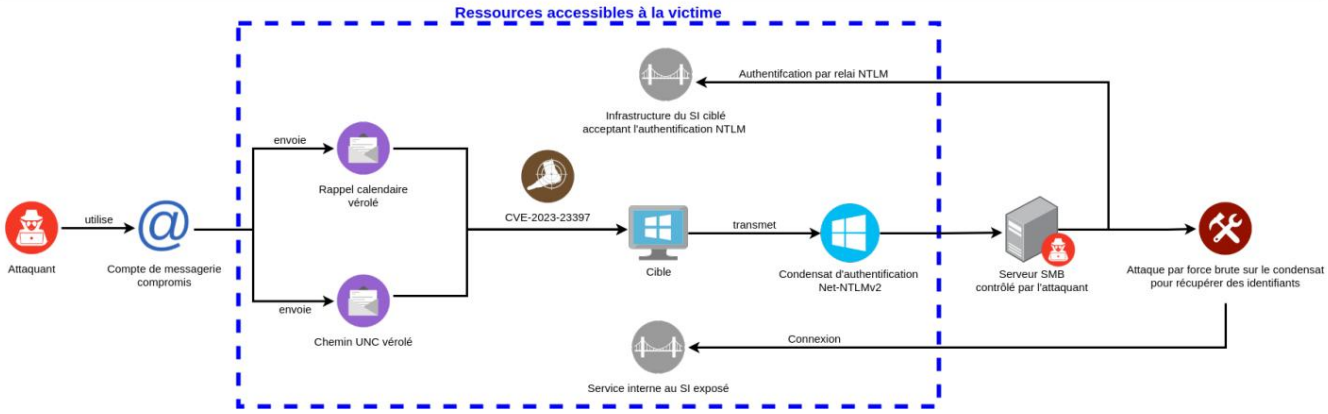

Fig. 2.3 – Diagram presenting the exploitation possibilities of CVE-2023-23397 by *APT28.*

2.6 Exfiltration

ANSSI observed MOA *APT28* apply different exfiltration techniques focused solely on email recovery.

During its investigations, ANSSI noted the compromise of an email management gateway operated by an outsourcer of the victim. MOA operators analyzed the emails exchanged for several weeks before applying filters to specific templates in order to exfiltrate content of interest. Using an archiving rule, each email matching one of the filters was archived on a server controlled by the attacker.

In some cases, the MOA used the login secrets of its victim's mailbox to access content of interest without implementing an automated exfiltration mechanism.

These TTPs are part of the continuity of MOA operations documented in open source, like the compromise of the servers hosting the Roundcube application. In this campaign, MOA exfiltrated the contents of email boxes through redirection rules [10].

The **CredoMap** implant uses a compromised email account to exfiltrate data from retrieved browsers [2, 20, 21]. In perated *via* the IMAP [6] other campaigns, the MOA used online services like PIPEDREAM, MOCKBIN or MOCKY protocol to recover the exfiltrated content [3, 5, 6, 7, 22].

ANSSI observes increased targeting by the MOA against messaging infrastructures for strategic espionage purposes. This targeting is carried out through different techniques, demonstrating the MOA's ability to collect information on the victim in advance in order to adapt the level of sophistication of its attacks.

6. *Internet Message Access Protocol* (IMAP) is a protocol for accessing and manipulating electronic messages on a server.

3 Recommendations

To deal with this type of threat, ANSSI recalls the importance of having a global approach to security, in particular *through* carrying out a risk assessment. This must make it possible to identify:

• the assets to be protected; • the
current state of the information system supporting them and the skill level of the people using or operating it; • the nature of the threats for which it
is appropriate to prepare; • and therefore the appropriate security measures that must
be implemented and, above all, maintained over time.

In this section, the following security measures will be detailed:

• Security of email exchanges
  • Confidentiality of email exchanges • Secure exchange platform •
  Reduction of risks of hijacking emails
  from the user mailbox • Reduction of risks of hijacking emails in transit • Identity theft sending booby-trapped emails
  from or to interlocutors • Reduction of the attack surface of web messaging
  interfaces *(webmail)* • Reduction of the risk of lateralization from Microsoft Exchange servers • Secure
  messaging architecture • Investigation capabilities to identify malicious emails

• Security of authentication data
  • Reduced risks from database leaks • Reduced risks from online brute force attacks
  • Reduced risks from phishing campaigns • Reduced risks from attacks targeting NTLM

• Security of user stations
  • Malicious software and drivers or diverted for malicious purposes • Limit the
  possibilities of lateralization from a compromised user station • Securing access to content hosted
on the Internet
  • Implementation of a proxy server and controlled TLS inspection • Identify and limit
  the misuse of specialized online services

These recommendations come from the following guides:

• “Guide to the EBIOS Risk Manager method” [23]; •
“Recommendations for multi-factor authentication and passwords” [24]; • “Recommendations relating to the
interconnection of an information system to the Internet” [25]; • “Recommendations for the implementation of a
software restrictions policy under Windows” [26]; • “Security recommendations for the architecture of a logging system” [27]; •
“Security recommendation for logging Microsoft Windows systems in an environment

Active Directory” [28];
• “Active Directory checkpoints” [29]; • “Class of
vulnerabilities in Active Directory environment” [30]

3.1 Security of email exchanges

The APT28 MOA focuses on emails that can be exchanged within an entity. Email is a seemingly ordinary communication medium, but which can prove to be a source of information of interest (ongoing negotiations, orders, strategic documents, reports, economic and administrative documents, appointments, etc. .) for an MOA interested in an entity and its ecosystem (prospects, customers, suppliers, commercial and non-commercial partners, regulatory authority, advice, etc.).

Unfortunately, it is often difficult, if not impossible, to ensure that none of the servers providing email routing (mail transfer agents, filtering gateway, message management gateway, mail servers) are being tricked into obtaining a copy of the exchanges or to alter them.

R1

Confidentiality of email exchanges

Even if its implementation can be complex and cannot be systematic, the most effective security measure remains end-to-end encryption of emails or attachments likely to contain sensitive information (for example via *Zed !,* S/MIME, PGP, encrypted archive). Note that the secrets or authentication data used for (de)encryption must be shared with the interlocutors through another secure channel.

When implementing this type of security measure, we must not forget to set up a escrow for encryption secrets: if the bearer(s) of these secrets were to be unavailable temporarily or permanently, the continuity activity could be affected.

R2

Secure exchange platform

The use of a secure exchange platform in addition to emails is also recommended in order to transmit sensitive information. Securing this type of platform must be the subject of particular care (for example: multi-factor authentication, reduction of the functionality surface and therefore the attack surface to what is strictly necessary, purging at regular intervals of data in transit , on-the-fly encryption, etc.)

R3

Reduction of risks of email hijacking from the user mailbox

Many email applications allow users to create automatic copying and redirection rules for emails received or sent. MOA APT28 sometimes uses this type of mechanism when compromising its targets' mailboxes. Since the functionality is already present, its activation can often be done discreetly and remain unnoticed by the legitimate user for a long time.

When the applications allow it, and if this type of mechanism is not necessary for a compelling reason, ANSSI recommends deactivating them as far as possible. Failing that, make them configurable only to people or services who absolutely need them.

ANSSI also recommends a periodic review of this type of redirection configuration in order to ensure their legitimacy.

R4

Reduced risks of emails being hijacked in transit

It is important to remember that an attacker may choose to directly attack email filtering gateways located upstream of an entity's receiving server.
Thus, in the event of suspicion of email compromise and in the absence of suspicious traces on the information system, it is important to investigate these upstream bricks. First of all, by checking that their configuration is consistent and has not been altered (filtering, selection, redirection, etc.), for example to make a copy of all or part of the emails to a third-party server.
Then, by checking that these gateways are up to date with their security patches or do not publicly expose an administration interface, likely to offer an entry point to an attacker.
If necessary, digital investigations should be carried out in search of traces of compromise.

In the case where services are outsourced or operated by a service provider, it is necessary to ensure that the service integrates all the security mechanisms and configuration options meeting the need, in particular the following
points: • encryption of
communications; • partitioning, same software, with
other clients; • event logging and configuration auditability; •
capabilities for detecting security incidents or unusual events.

If doubts persist, additional digital investigations with the service provider should be carried out.

R5

Identity theft when sending booby-trapped emails to or from interlocutors

Without having to compromise an email account, it is easy for an attacker to forge emails with the domain name of an entity or its interlocutors. This ploy can be used to fool a user by sending them emails that appear to come from a regular contact. To limit the nuisance of these emails, before their receipt by users, ANSSI encourages the implementation of certain protocols whose role is to verify the authenticity and integrity of emails. They require configuration, not only by the sending entity on the DNS records of its domain names, but also by the recipient entity on its receiving SMTP servers. These protocols are:

- **Sender Policy Framework** (SPF) which allows you to specify the IP addresses of authorized servers to send emails from a domain;
- **DomainKeys Identified** Mail (DKIM) which allows authentication of the email domain an email using a cryptographic signature;
- **Domain-based Message Authentication, Reporting and Conformance** (DMARC) which notably allows an entity to define a processing policy for its sent emails based on SPF and DKIM compliance results.

R6

Reduction of the attack surface of webmail interfaces (webmail)

Web messaging interfaces are prime targets because of their very large attack surface, linked to their wealth of features. The last three years have been particularly marked by the discovery and publication of numerous vulnerabilities affecting several of these services. Many of these vulnerabilities did not require any prior authentication and sometimes access to a single account was enough to jeopardize the entire application. APT28, like many other actors, made massive use of these loopholes. ANSSI has dealt with and continues to deal with numerous cases of compromise having this type of service as their starting point.

When web messaging interfaces are implemented, ANSSI strongly recommends not exposing them publicly on the Internet and only making them accessible internally or *via* a VPN for people in a nomadic or teleworking situation.

However, if for compelling operational reasons these accesses must be exposed, it is recommended, on the basis of risk assessment, to implement an access chain with dedicated resources, access restrictions only to the mailboxes concerned and a reinforced detection strategy, for example:

- an exhibition server (example: web messaging portal) hosted within the exhibition area exposed
services; • configuration of access only to the mailboxes concerned; •
protection of the exposure server by a reverse *proxy server,* or even an application firewall, hosted in a relay services zone;
- the implementation of two-factor authentication for users, possibly with the provision of an electronic certificate; • the definition of a
reinforced detection strategy (geolocation of connections, number of failed authentications, volumes of emails exchanged); • rigorous monitoring of the
publication of vulnerabilities affecting this type of application and appropriate responsiveness will also be decisive.

However, it is important to note that as part of a Microsoft Exchange infrastructure, it is not possible to decouple webmail functionality from other functionality of a Microsoft Exchange server or *cluster .* However, by nature, a Microsoft Exchange server has a very strong influence in a Microsoft ecosystem, because it notably allows the management of all accounts (with the exception of those constituting Tier 0 of an Active Directory domain) and this goes beyond the simple scope of the email function. Consequently, the compromise of a Microsoft Exchange server, for example through its web interface, will jeopardize the Information System.

R7

Reducing the risk of lateralization from Microsoft Exchange servers

Due to misconfiguration or historical configuration, a Microsoft Exchange server may have privileged rights in an Active Directory (AD) environment. In the event of a compromise, an attacker can abuse this situation to elevate his privileges and take control of an AD directory, thereby leading to the compromise of the associated information system.
In the interests of in-depth security, ANSSI encourages checking that the AD directory has been hardened to avoid the risk of elevation of privilege in the event of a compromise of a Microsoft Exchange server [29] .

R8

Secure messaging architecture

In order to protect the internal information system from malicious emails *(phishing, spear phishing,* etc.), it is recommended to build an architecture based on email relay servers within a secure gateway [25].

For messaging needs external to the entity (i.e. with an interconnection to the Internet), at least one SMTP server must be positioned within the secure Internet gateway. However, taking into account the complexity and associated costs, it is recommended to dedicate an SMTP server for sending and another for receiving emails (for example: two separate virtual machines) within the secure Internet gateway. . They must be configured accordingly: • a sending SMTP server only accepts emails from a list of authorized servers (internal relay servers or mailbox servers) and provides header cleaning functions in order to to limit the disclosure of information that can be reused by an attacker (for example, by removing “received” or “X-” headers); • a receiving SMTP server applies the initial security policies, provides protocol and content analysis functions, qualifies emails requiring quarantine and ultimately transmits the emails to another relay server *of* the entity or to a mailbox server; • a relay server within the internal information system chained to the sending and delivery servers reception exposed to the Internet through the secure gateway.

Note that if ultimately a single server is positioned within the secure Internet gateway to ensure this interface function between the internal and external, the logic for configuring the sending, receiving and relay functions remains applicable.

For internal messaging needs (i.e. without interconnection to the Internet), deploy at least one relay server within the internal information system which will be dedicated to internal needs only. Under no circumstances should this server be chained to an SMTP server exposed on the Internet.

R9

Investigative capabilities to identify malicious emails

The security and filtering devices placed upstream of the mail servers are not infallible, and malicious messages may be received by users. It is then important to know the logging and search capabilities. These mechanisms may be used when, on the basis of a report, one or more suspicious emails and associated activities must be sought.

Thus, when indicators of compromise *(IoC)* are shared, they most often relate to: • one or more sender/recipient addresses; • a malicious or hijacked domain; • the subject of the email; • the body of the email containing a text, link, a set of keywords; • a transmission/reception period.

Concerning attachments, the indicators most often relate to:

- name;
- extension;
- metadata; •
- MD5/SHA1/SHA256 fingerprints;
- content.

These IoCs can be precise or even relate to a characteristic pattern that can be searched for example through a rational expression or a Yara rule.

Identifying a malicious email should be seen as a starting point for an investigation and should not just be a matter of removal. If possible, it is recommended to try to answer the following questions:

- was the malicious email blocked or not by upstream filtering devices? In either case, what were the conclusions of the analysis of these upstream solutions?
- is it possible to retrieve a copy? • have several users received this same email? • are there other variations of this email in the environment? • did the person(s) concerned actually receive, open, delete, transfer the email or its attachments? If so when, how, to whom?
- have any suspicious system or network activities been observed from these users' accounts or computers following previously identified actions?

To answer these questions, it is necessary to have different logging points that can be collected and correlated: filter gateway, mail server, user station, network proxy, firewall, Active Directory (if applicable). These events may have occurred several months ago, so it is recommended, in accordance with legal or regulatory constraints and the capabilities of the entity, to sufficiently scale the retention of this logging.

Finally, discussing with the person(s) concerned about the actions they may have taken around this email is also important. Indeed, some emails sometimes do not contain any malicious payload or links, but only a list of instructions to be carried out by the user. In addition, it may sometimes be able to explain the context preceding receipt of the malicious email.

3.2 Security of authentication data

R10

Reduction of risks caused by databases of data leaks

Like many MOAs, APT28 exploits databases of data leaks in search of still valid passwords.

To deal with this type of risk, several additional measures are recommended [24] :

- implement multi-factor authentication; • favor the use of a well-remembered password for which the user is aware of its sensitivity, rather than renewing it at short intervals (for example, every 90 days) as previously recommended;
- raise awareness of the use of separate authentication secrets to access different services vices, and encourage the use of secure password vaults;
- promote the implementation of single authentication services (Single Sign On) such as Kerberos, in order to limit the number of authentication secrets to memorize;
- audit the strength of user passwords at regular intervals and request renewal if necessary.

R11

Reducing the risks caused by online brute force attacks

To reduce the risk of compromise of user accounts on online services, it is recommended [24] : • to ensure that default accounts and passwords have been deactivated or changed; • define a strong password policy, including verification upon entry; • implement multi-factor authentication; • implement mechanisms detecting multiple authentication attempts from one or more distinct IP addresses, which are able to block them or reduce the number of possible attempts; • audit the strength of user passwords at regular intervals and request renewal if necessary.

R12

Reducing the risks associated with phishing campaigns

Phishing remains a safe bet for attackers. When done in an elementary manner, success rates can nevertheless be high. When done carefully, even an experienced user can get tricked. While malicious email phishing campaigns remain a very popular classic route, we must not forget the other forms of possible phishing campaigns. For example :

- *via* messages on social networks;
- *via* SMS messages or instant messaging (WhatsApp, Signal, Telegram, TikTok, Slack, Discord, Facebook Messenger, etc.);
- *via* telephone calls;
- *via* connection redirection attacks when Internet browsing is carried out in HTTP.

Users must therefore be trained to recognize the different forms of phishing, but also possible phishing pages. This awareness must take into account the scenario where a contact's means of communication have been hijacked by an attacker.

Separating professional and personal means of communication is an important security measure, as it reduces the risk of confusion between communication channels that could be targeted by phishing campaigns.

Although not foolproof, using multi-factor authentication mechanisms to protect access to services is a particularly effective security measure to combat common login secret theft via phishing scenarios.

The success of some phishing campaigns relies on the theft of brand identity. Implementing technical, organizational and legal means to deal with it is often necessary to:

- filter emails usurping the addresses of an entity (see above);
- detect, block and close malicious domains exploiting opportunistic typos *(typosquatting);*
- detect, block and close malicious sites or pages usurping the identity of a user treprise.

R13

Reducing the risks caused by attacks targeting NTLM

Similar to MOA APT28's use of CVE-2023-23397, attacks targeting NTLM secrets and challenge-responses are very common. They open up possibilities for offline brute force attacks to obtain user passwords and also allow NTLM relay attacks to be carried out. In the context of this vulnerability, correctly implemented network hygiene makes it possible to invalidate the exploitation as described earlier in this document. Indeed, the MOA needs the victim to be able to establish an SMB connection from their workstation to a machine that they control (in this case, compromised routers). However, except in very special cases, no SMB flow should be authorized out of a corporate network. The firewall of the user station or at the edge of the network must block this attempt and attract the attention of the security teams. However, if for compelling reasons the establishment of external SMB connections must be permitted, a white list of destinations should be established.

Furthermore, outgoing connections from the internal information system should not use internal *single sign-on (SSO)* by default; To do this, a list of domains authorized to rely on internal SSO should be established and applied to the entire information system.

NTLM secrets and challenge-answers are inherently vulnerable to brute force attacks aimed at trying to recover the associated passwords. A policy of strong passwords and non-reuse of passwords must therefore be applied [24].

The global disabling of NTLM authentication in favor of exclusive use of Ker-beros also makes these attacks inoperable. This is a particularly effective generic measure. However, NTLM authentication is often still necessary for the proper functioning of certain applications not migrated to Kerberos, and it is therefore not always possible to prohibit NTLM globally. To take into account this complexity of implementation, the progressive developments carried out by Microsoft (for example through recent versions of Windows 11), and the constraints of spreading out over time such a migration, ANSSI encourages start as a priority with the most critical services or those providing an IT asset management function, by disabling outgoing connections using NTLM for these servers (for example for the following servers and services: domain controllers, Microsoft Exchange, Microsoft Endpoint Configuration Manager , System Center Configuration Manager, etc.).

ANSSI has a page dedicated to the subject available on the CERT-FR website [30].
Finally, Microsoft has made available a set of tools and recommendations to help investigate potential exploitation of the CVE-2023-23397 vulnerability [31].

3.3 Security of user stations

R14

Malicious or misused software and drivers

APT28 has its own arsenal of malicious tools. However, like many malicious actors, the MOA also uses legitimate tools imported by it or available by default on the targeted systems as part of its attacks. The misuse of the latter for malicious purposes aims to complicate detection and thus reinforce its level of discretion. Thus, several complementary lines of defense in depth are necessary.

Firstly, it is appropriate to use the basic lines of defense integrated into the operating system as well as antiviral solutions and to activate: • detection of potentially unwanted applications/programs (Potentially Unwanted Applications/Programs (PUA / PUP)); • detection of compromised drivers and firmware; • the integrity of memory protection; • *Microsoft Defender Application Guard* [32]; • *Credential Guard.*

In addition, monitoring detection alerts that will be raised is essential in order to be able to react promptly if necessary.

Secondly, advanced lines of defense should be used to limit the effectiveness of malicious or diverted software not detected by antiviral solutions:

- define and implement a software restriction policy in order to restrict execution to a list of duly authorized programs or locations (for example: as part of implementing a blacklist by blocking temporary directories from which email attachments are opened) [26];

- define a rigorous network filtering policy at the user station level, in order first of all to strictly block incoming flows with the exception of duly authorized flows, then by restricting outgoing flows according to their nature and destinations; • set up an efficient and secure logging system [27, 28]; • set up monitoring of these logs and implement detection heuristics aimed at looking for diversions of legitimate applications for malicious purposes.

Identifying and monitoring over time applications and drivers that can be hijacked for malicious purposes can be a tedious task. Community projects exist [33, 34].

R15

Limit the possibilities of lateralization from a compromised user station

When the APT28 MOA manages to compromise a user station, it not only exfiltrates the available information, but can also seek to lateralize itself within the information system. The entity's risk management must include one or more scenarios on the compromise of user stations and must take into account the importance of the resilience of the infrastructure in the face of this risk. This work must determine, in a coherent and maintainable manner, different segmentation strategies:
• network, • application, • functional
(for
example:
users, privileged users, administrators, administrative
AD tors, etc.)
• physical and logical,
• etc.

ANSSI reminds that in the context of a Microsoft AD environment, the directory must at least have a basic level of security that has not been weakened since its installation (which corresponds for example to level 3 of the ANSSI standard) [29] .

3.4 Securing access to content hosted on the Internet

R16

Implementation of a proxy server and mastered TLS inspection

It is essential to avoid any direct access from a user station or a server to the Internet.
To do this, a Web proxy server must act as a relay and implement security functions: authentication, access control, content analysis, logging, etc.
All access to content hosted on the Web must be authenticated individually for users and unambiguously for the services.

The number of sites accessible via HTTPS is constantly increasing and constitutes a major advance in securing communications to the extent that the associated TLS configuration is state of the art. The downside is that, if it involves access to phishing sites *or* hosting malicious code, it is theoretically impossible to detect suspicious content in all encrypted traffic. To overcome this, implementing TLS inspection is a possibility. This must *ultimately* make it possible to analyze the content and ensure the pro-to-school conformity of the exchanges. TLS inspection therefore meets the need for malicious code detection and must, where appropriate, be implemented securely within the relay service area. The choice of equipment carrying out this inspection is structuring; this must in particular allow state-of-the-art configuration of cryptographic parameters [25].

R17

Identify and limit the misuse of specialized online services

There are many services online to simulate customizable endpoints (“mockbin[.]org”, “mocky[.]io”, “pipedream[.]com”, “frge[.]io”, “webhook [.]site”, etc.). These specialized legitimate services can be used in a roundabout way for malicious purposes, for example to carry out phishing campaigns *or* to carry out data exfiltration. It should be noted that these services meet very specialized business needs. It is appropriate to question the need for access to this type of service and, if necessary, to authorize their access on a case-by-case basis.

The security mechanisms detailed in the previous recommendation make it possible to implement appropriate filtering policies or a *posteriori* research in the event of a need for investigation.

4 Bibliography

[1] MALWAREBYTES. *Russia's APT28 Uses Fear of Nuclear War to Spread Follina Docs in Ukraine.* June 21, 2022.
URL: https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine.

[2] CERT-UA. *Computer attack on the APT28 group using CredoMap malicious code.* June 20, 2022.
URL: https://cert.gov.ua/article/341128.

[3] CERT-UA. *Computer attack on the APT28 group using CredoMap_V2 malicious code.* May 6, 2022.
URL: https://cert.gov.ua/article/40106.

[4] SOCRADAR. *Microsoft Fixes Exploited Zero-Days in March Patch Tuesday (CVE-2023-23397 & CVE-2023-24880).* March 15, 2023.
URL: https://socradar.io/microsoft-fixes-exploited-zero-days-in-march-patch-tuesday-cve-2023-23397-cve-2023-24880/.

[5] SEKOIA. *APT28 Leverages Multiple Phishing Techniques to Target Ukrainian Civil Society.* May 5, 2023.
URL: https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/.

[6] CERT-UA. *Phishing attacks from the APT28 group aimed at obtaining authentication data for public messaging services.* July 8, 2023.
URL: https://cert.gov.ua/article/5105791.

[7] CERT-UA. *Phishing campaign using the UKR.NET service theme and QR codes.* March 16, 2022.
URL: https://cert.gov.ua/article/37788.

[8] CERT-UA. *APT28 computer attack: distribution of emails containing “instructions” for “updating the operating system ”.* April 28, 2023.
URL: https://cert.gov.ua/article/4492467.

[9] GOOGLE. *Threat Horizons.* December 7, 2021.
URL: https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf.

[10] RECORDED FUTURE. *BlueDelta Exploits Ukrainian Government Roundcube Mail Servers to Support Espionage Activities.* June 20, 2023.
URL: https://go.recordedfuture.com/hubfs/reports/cta-2023-0620.pdf.

[11] CLUSTER25. *In the Footsteps of the Fancy Bear: PowerPoint Mouse-over Event Abused to Deliver Graphite Implants.* September 23, 2022.
URL: https://blog.cluster25.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint-graphite/.

[12] CLUSTER25. *A Not so Fancy Game Exploring the New Skinnyboy Bear's Backdoor.* June 4, 2021.
URL: https://blog.cluster25.duskrise.com/2021/06/03/a-not-so-fancy-game-apt28-skinnyboy.

[13] NOS. *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments.* July 1 , 2021.
1 URL: https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOOO158036-21.PDF .

[14] TRELLIX. *Prime Minister's Office Compromised: Details of Recent Espionage Campaign.* January 25, 2022.
URL: https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/prime-ministers-office-compromised.html.

[15] SECURITYSCORECARD. *A Deep Dive Into the APT28's Stealer Called CredoMap.* September 28, 2022.
URL: https://securityscorecard.com/research/apt28s-stealer-called-credomap/.

[16] MICROSOFT. *STRONTIUM: Detecting New Patterns in Credential Harvesting.* September 11, 2020.
URL: https://www.microsoft.com/en-us/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/.

[17] NCSC-UK, CISA, FBI AND NSA. *Advisory: APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers.* April 18, 2023.
URL: https://www.ncsc.gov.uk/files/Advisory_APT28-exploits-known-vulnerability.pdf.

[18] ANSSI. *CERT-FR alert bulletin: vulnerability in Microsoft Outlook.* March 15, 2023.
URL: https://www.cert.ssi.gouv.fr/alarme/CERTFR-2023-ALE-002/.

[19] MICROSOFT. *Guidance for Investigating Attacks Using CVE-2023-23397.* March 24, 2023.
URL: https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/.

[20] TREND MICRO. *Pawn Storm's Lack of Sophistication as a Strategy.* December 21, 2020.
URL: https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html.

[21] TRELLIX. *Growling Bears Make Thunderous Noise.* June 6, 2022.
URL: https://www.trellix.com/en-us/about/newsroom/stories/research/growling-bears-make-thunderous-noise.html.

[22] CERT-UA. *APT28 computer attack: msedge used as loader, TOR and mockbin.org/ website.hook services used as control center.* September 4, 2023.
URL: https://cert.gov.ua/article/5702579.

[23] ANSSI. *Guide to the EBIOS Risk Manager method.*
URL: https://cyber.gouv.fr/ebios-rm.

[24] ANSSI. *Recommendations for multi-factor authentication and passwords.* October 8, 2021.
URL: https://cyber.gouv.fr/guide-AUTH.

[25] ANSSI. *Recommendations relating to the interconnection of an information system to the Internet.* June 19, 2020.
URL: https://cyber.gouv.fr/guide-interconnexion-si-internet.

[26] ANSSI. *Recommendations for implementing a software restrictions policy under Windows.* Jan 13-last 2017.
URL: https://cyber.gouv.fr/guide-windows-restrictions-logicielles.

[27] ANSSI. *Security recommendations for logging system architecture.* January 28, 2022.
URL: https://cyber.gouv.fr/guide-journalisation.

[28] ANSSI. *Security recommendations for logging Microsoft Windows systems in the environment Active Directory.* January 28, 2022.
URL: https://cyber.gouv.fr/guide-journalisation-windows.

[29] ANSSI. *Active Directory checkpoints.* October 18, 2022.
URL: https://cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/.

[30] ANSSI. *Class of vulnerabilities in Active Directory environment.* October 18, 2022.
URL: https://cert.ssi.gouv.fr/dur/CERTFR-2021-DUR-001/.

[31] MICROSOFT. *Guidance for investigating attacks using cve-2023-23397.* March 24, 2023.
URL: https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/.

[32] MICROSOFT. *Microsoft Defender Application Guard overview.* July 13, 2023.
URL: https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/microsoft-defender-application-guard/md-app-guard-overview.

[33] LOLBAS-PROJECT. *Community project: Living Off The Land Binaries, Scripts and Libraries.*
URL: https://lolbas-project.github.io/.

[34] LOLDRIVERS. *Community project: Living Off The Land Drivers.*
URL: https://www.loldrivers.io/.

1.0 - October 26, 2023

NATIONAL INFORMATION SYSTEMS SECURITY AGENCY

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
cert.ssi.gouv.fr / cert-fr@ssi.gouv.fr