TLP:CLEAR
PAP:CLEAR

# CAMPAGNES D'ATTAQUES DU MODE OPÉRATOIRE APT28 DEPUIS 2021

## ILLUSTRATION DE LA MENACE ET RECOMMANDATIONS DE SÉCURISATION

1.0

26 octobre 2023

# Sommaire

# 1 Résumé

Lors de ses investigations, l'ANSSI a analysé plusieurs chaînes de compromission du mode opératoire d'attaque (MOA) *APT28* [1] utilisées à des fins d'espionnage. Certaines campagnes ont été dirigées contre des organisations françaises, dont des entités gouvernementales, des entreprises, des universités, ainsi que des instituts de recherche et des groupes de réflexion (*think tanks*).

Si les attaquants poursuivent leurs campagnes d'attaque par force brute et d'exploitation de vulnérabilités, l'ANSSI constate par ailleurs que les attaquants réduisent le risque de détection en compromettant des équipements peu surveillés et situés en périphérie du réseau [2]. Dans certains cas, aucune porte dérobée n'est déposée sur le réseau compromis.

Ce document s'appuie sur des rapports techniques publiés en source ouverte et des éléments collectés durant des opérations de réponse à incident réalisées par l'ANSSI. Il détaille les tactiques, techniques et procédures (TTP) caractéristiques des activités du mode opératoire depuis la seconde moitié de l'année 2021 (section 2) et propose une série de recommandations pour se prémunir contre ce type d'attaque (section 3).

1. Également connu sous les noms de *UAC-0028*, *Fancy Bear*, *FrozenLake*, *Sednit*, *Sofacy* ou encore *Pawn Storm*.
2. Routeurs, passerelles et serveurs de messagerie, pare-feux, *etc.*

# 2 Tactiques, techniques & procédures

## 2.1 Reconnaissance

Durant ses investigations, l'ANSSI a identifié différentes techniques de reconnaissance employées par *APT28*.

Le mode opératoire repose sur l'utilisation de comptes de messagerie compromis pour mener ses campagnes d'hameçonnage [T1597] [1, 2, 3, 4]. Dans certains cas, les identifiants et mots de passe de ces comptes sont présents dans des bases de fuites de données.

*APT28* est également employé dans des attaques par force brute [T1110.003, T1110.004]. Les opérateurs du MOA ciblent très largement des comptes de messagerie personnels [2, 5, 6, 7, 8, 9]. Ces campagnes sont destinées à récupérer massivement des informations de connexion (*credentials harvesting*) afin d'alimenter des dictionnaires d'attaque. Ces informations sont ensuite réutilisées pour cibler des comptes d'employés.

Dans une campagne documentée fin avril 2023, les opérateurs d'*APT28* ont diffusé des courriels d'hameçonnage indiquant aux utilisateurs de mettre à jour leur système en exécutant des instructions en langage **PowerShell** [8]. Ces instructions permettaient de télécharger et d'exécuter un script contenant deux commandes :

- `tasklist`, qui permet de lister l'ensemble des processus en cours d'exécution ;
- `systeminfo`, qui permet d'afficher les informations de configuration détaillées d'un ordinateur et de son système d'exploitation. Ces informations contiennent par exemple la liste des correctifs de sécurité installés.

Le script contenant les deux commandes ci-dessus était hébergé sur « `mocky[.]io` ». Le résultat des commandes était envoyé en direction de « `mockbin[.]org` ». MOCKY et MOCKBIN sont des services publics permettant de générer des points de terminaison web afin de tester, suivre et simuler une requête ou une réponse HTTP. L'objectif des opérateurs du MOA était probablement de récupérer des informations sur l'environnement informatique de leurs cibles afin de mener ultérieurement une attaque de plus grande envergure contre ces systèmes d'information [8].

## 2.2 Développement des capacités

L'ANSSI identifie au moins trois axes de développement de capacités d'*APT28* :

- la recherche de vulnérabilités du jour zéro (*0-day*) [T1212, T1587.004] ;
- la compromission de routeurs et de comptes de messagerie personnels [T1584.005, T1586.002] ;
- l'utilisation d'outils disponibles en source ouverte et de services en ligne [T1588.002, T1583.006].

Les investigations de l'ANSSI confirment qu'*APT28* a exploité la vulnérabilité *0-day* CVE-2023-23397 affectant le produit Outlook pour Windows à partir de mars 2022 et jusqu'en juin 2023.

Selon d'autres partenaires, sur cette période, le MOA aurait par ailleurs exploité d'autres vulnérabilités, comme celle touchant Microsoft Windows Support Diagnostic Tool (MSDT, CVE-2022-30190, aussi appelée Follina) ainsi que celles ciblant l'application Roundcube (CVE-2020-12641, CVE-2020-35730, CVE-2021-44026) [1, 2, 10].

Les opérateurs du MOA constituent et maintiennent une partie de leurs infrastructures d'attaque en compromettant des routeurs et des comptes de messagerie personnelle de particuliers et d'entreprises (cf. section 2.1). Ces accès servent principalement de rebond pour atteindre des cibles stratégiques. Les opérateurs du MOA utilisaient en effet les comptes de messageries compromis pour envoyer des courriels malveillants et les routeurs compromis pour récupérer des données exfiltrées.

Durant la campagne d'exploitation de la vulnérabilité CVE-2023-23397, l'ANSSI a pu confirmer qu'*APT28* employait au moins douze comptes de messagerie appartenant à des entreprises et onze routeurs Ubiquiti compromis :

Campagnes d'attaques du mode opératoire APT28 depuis 2021

| Émetteur | MD5 du fichier | Date d'envoi | URI | Routeur compromis |
|---|---|---|---|---|
| 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 |
| *Inconnu* | 92e22b7e96aca3f9d733ca609ab0b589 | 2022-10-05 | *Inconnu* | 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 | *Inconnu* | 213.32.252.221 |
| karina[@]bhpcapital[.]com | e68cbd4930e2781e0c1b19eb72ec0936 | 2022-10-26 | *Inconnu* | 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 |
| *Inconnu* | 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 – Liste des courriels identifiés par l'ANSSI exploitant la CVE-2023-23397.

Lors de réponses à incident, l'ANSSI a pu confirmer l'utilisation des outils malveillants **Mimikatz** et **reGeorg** par *APT28* :

- **Mimikatz** est un outil qui peut notamment servir à extraire les mots de passe (ou leurs empreintes) stockés en mémoire sous Windows ;
- **reGeorg** est un outil de création de tunnels exploitant un serveur HTTP compromis sur lequel un script (PHP, ASPX, JSP, etc) spécifique est installé pour relayer du trafic pour d'autres protocoles (exemple : RDP, SSH, SMB) et ainsi contourner certaines règles de filtrage.

Des rapports publics indiquent qu'*APT28* aurait utilisé le cadriciel **Empire**, disponible en source ouverte, lors du déploiement de l'implant **Graphite**, spécifique au mode opératoire [11].

L'emploi de ces outils s'inscrit dans une utilisation plus large de services disponibles en source ouverte. *APT28* s'appuie en effet sur plusieurs services d'hébergement comme « `neocities[.]org` », « `frge[.]io` », « `tinyhost[.]fr` », « `mockbin[.]org` », « `mocky[.]io` », ainsi que le service d'hébergement gratuit InfinityFree [5, 8]. D'autres services du même type ont pu être utilisés par *APT28*. L'ANSSI observe également la réutilisation de noms de domaines et de serveurs entre différentes campagnes depuis 2021.

Enfin, *APT28* s'appuie sur un ensemble de services de réseau privé virtuel (*VPN*) pour ses activités malveillantes (connexions à des comptes, attaques par force brute, exploitation de vulnérabilités). Ces fournisseurs de services *VPN* acceptent les cryptomonnaies et mettent en avant la non-traçabilité des données [12, 13].

Une liste non exhaustive des services *VPN* employés par le MOA est disponible ci-dessous :

| VPN observés | Confiance |
|---|---|
| SurfShark | Forte |
| ExpressVPN | Forte |
| CactusVPN | Forte |
| ProtonVPN | Forte |
| PrivateVPN | Modérée |
| IPVanish | Modérée |
| NordVPN | Modérée |
| WorldVPN | Faible |
| PureVPN | Faible |
| VPNSecure | Faible |

Fig. 2.2 – Liste des services *VPN* probablement utilisés par *APT28*.

## 2.3 Accès initial

L'ANSSI observe trois principales méthodes d'accès initial employées par le MOA depuis 2021 :

- l'envoi de courriels d'hameçonnage redirigeant vers une fausse page d'authentification ;
- l'envoi de courriels exploitant des vulnérabilités dans le client de messagerie ;
- le ciblage d'interfaces d'authentification par l'utilisation d'identifiants valides ou d'attaques par force brute.

*APT28* a été employé à de nombreuses reprises pour conduire des campagnes d'hameçonnage ciblé [T1566]. Ces campagnes s'appuient notamment sur des techniques d'ingénierie sociale pour rediriger les victimes vers des pages de récupération d'informations de connexion. Les opérateurs du MOA ont par exemple créé des pages d'hameçonnage imitant la page de connexion Office 365 des entités ciblées.

Le MOA a également diffusé des courriels d'hameçonnage dans le but d'exploiter des vulnérabilités dans le client de messagerie. Certaines vulnérabilités [3] ne nécessitent pas d'action de la part de l'utilisateur. L'objet de ces courriels est souvent construit autour d'un terme unique : « `Silence.` », « `Celebration` », « `Interest.` », *etc*.

Ces observations corroborent les activités d'hameçonnage liées au mode opératoire et documentées en source ouverte par des homologues de l'ANSSI et des éditeurs de solutions de sécurité, dont le CERT-UA, CLUSTER25 et TRELLIX [2, 3, 14, 15, 11].

Depuis au moins 2020, les attaques par force brute sont une des méthodes les plus employées par *APT28* [T1190]. Les investigations de l'ANSSI confirment que le MOA a conduit ce type d'attaque contre des serveurs de messagerie et des pare-feux exposés sur Internet en utilisant des dictionnaires de mots de passe.

Dans d'autres cas, le MOA a identifié des comptes légitimes et s'y est connecté une fois l'attaque par force brute ou par énumération de mots de passe courants (*password spraying*) réussie (cf. section 2.1) [T1078]. Ces actions sont menées au travers de services de *VPN* ou du réseau d'anonymisation Tor avec des infrastructures pouvant comprendre plus de 1 000 adresses IP différentes [16, 13].

## 2.4 Exploitation, persistance & élévation de privilèges

Le mode opératoire *APT28* est en mesure d'exploiter des vulnérabilités afin de gagner en privilège sur les postes clients, les serveurs ou les équipements compromis.

Dans l'un des incidents impliquant le MOA, l'ANSSI a identifié l'exploitation des vulnérabilités CVE-2020-0688 et CVE-2020-17144 à l'encontre d'un serveur Exchange exposé au travers d'une interface *Outlook Web Access* (OWA). Le

3. Dont la CVE-2023-23397.

MOA a exploité ces vulnérabilités depuis un compte valide afin d'exécuter du code à distance sur le serveur. L'outil **reGeorg** a notamment été utilisé pour pérenniser l'accès au serveur [T1505.003].

Pour se maintenir sur le réseau compromis, *APT28* crée par ailleurs des comptes utilisateur [T1136] qui imitent par exemple l'identité de l'entité ciblée ou encore utilisent des termes génériques comme « `guest` », « `admin` », *etc*.

Au-delà de ces observations, le MOA est connu pour avoir utilisé des techniques plus avancées. L'implant **Graphite** d'*APT28* emploierait par exemple une technique de *Component Objet Model (COM) Hijacking*[4] [T1546.015] comme mécanisme de persistance [11].

Les opérateurs du MOA identifient généralement des zones non surveillées dans le système d'information de la victime pour se maintenir et effectuer des actions de collecte et d'exfiltration. Certains implants du MOA comme **CredoMap** et les codes déployés pour l'exploitation de vulnérabilités dans l'application Roundcube collectent et exfiltrent directement les informations recherchées sans mettre en place de moyen de persistance.

Cependant, l'ANSSI a pu constater dans ses réponses à incident que plusieurs campagnes d'*APT28* n'employaient aucun code ou mécanisme spécifique pour maintenir un accès sur le réseau de la victime, gagner en privilège ou se latéraliser. Dans certains cas, l'attaquant procède directement à l'exfiltration de données (cf. section 2.6).

## 2.5 Collecte & mécanismes de commande et de contrôle

Pour collecter des données, *APT28* utilise à la fois des outils génériques et un ensemble de codes malveillants propres au mode opératoire. Durant la campagne d'attaques contre des serveurs Exchange, l'ANSSI a pu observer l'utilisation de TTP déjà documentées en source ouverte [13, 17], parmi lesquelles :

- la récupération des secrets d'authentification stockés dans la mémoire du processus LSASS, soit en utilisant l'outil **Mimikatz**, soit en faisant appel à la fonction `MiniDump` de la bibliothèque « `comsvcs.dll` » [T1003.001] ;
- l'utilisation d'utilitaires natifs comme « `ntdsutil.exe` » pour récupérer le contenu de la base de données Active Directory[5] [T1003.003] ;
- l'emploi de l'outil « `certutil.exe` » pour être en mesure de télécharger des ressources distantes dans l'environnement compromis[5] [T1105] ;
- la récupération du contenu des boîtes de courriels de personnalités d'intérêt probablement identifiées en amont.

L'ANSSI a procédé à l'analyse de la CVE-2023-23397 suite à la publication par Microsoft [18]. L'exploitation par *APT28* consiste en l'envoi de courriels ou de demandes de réunions Outlook afin de déclencher une connexion SMB [4, 19]. Les comptes ciblés réalisent automatiquement une tentative d'authentification auprès d'un service SMB contrôlé par l'attaquant. Cette authentification lui permet de récupérer le condensat d'authentification NetNTLMv2. L'attaquant est ensuite en mesure de relayer cette empreinte auprès d'autres services supportant ce type d'authentification [T1528].

L'infrastructure de commande et de contrôle (C2) d'*APT28* repose notamment sur des services légitimes. À titre d'exemple, les implants **Graphite** et **DriveOcean** employés par le MOA s'appuient respectivement sur des services OneDrive et Google Drive [14, 20]. Cette technique permet aux attaquants de réduire le risque de détection. Il est également plus difficile pour une entité d'interdire le trafic vers ces services.

Enfin, le MOA récupère probablement un ensemble de données d'accès *via* ses campagnes d'hameçonnage contre des boîtes de courriels de particulier ou l'utilisation de son implant **CredoMap**, qui permet de collecter des identifiants et des cookies de navigateurs. Ces données sont probablement utilisées *a posteriori* pour mener des compromissions à plus large échelle ou s'installer durablement dans un système d'information [T1555.003, T1539] [5].

4. Les objets COM sont des mécanismes Windows permettant à des logiciels d'interagir entre eux au travers du système d'exploitation.
5. « `certutil.exe` » et « `ntdsutil.exe` » sont des binaires légitimes présents sur le système dont l'utilisation est ici détournée (couramment appelé *Living Off The Land Binary* et abrégé LOLBin).

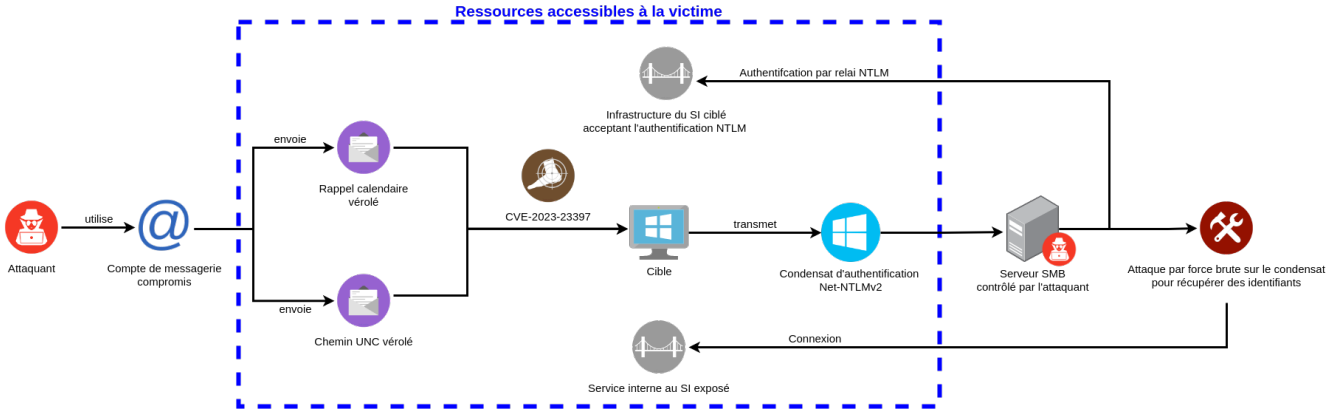


Fig. 2.3 – Schéma présentant les possibilités d'exploitation de la CVE-2023-23397 par *APT28*.

## 2.6 Exfiltration

L'ANSSI a observé le MOA *APT28* appliquer différentes techniques d'exfiltration concentrées uniquement sur la récupération de courriels.

Lors de ses investigations, l'ANSSI a constaté la compromission d'une passerelle de gestion de courriel opérée par un infogérant de la victime. Les opérateurs du MOA ont analysé pendant plusieurs semaines les courriels échangés avant d'appliquer des filtres sur des modèles spécifiques afin d'exfiltrer du contenu d'intérêt. Au moyen d'une règle d'archivage, chaque courriel correspondant à l'un des filtres était archivé sur un serveur contrôlé par l'attaquant.

Dans certains cas, le MOA utilisait les secrets de connexion de la boîte de messagerie de sa victime afin d'accéder au contenu d'intérêt sans mettre en place de mécanisme d'exfiltration automatisé.

Ces TTP s'inscrivent dans la continuité des opérations du MOA documentées en source ouverte, à l'instar de la compromission des serveurs hébergeant l'application Roundcube. Dans cette campagne, le MOA a exfiltré le contenu des boîtes de messagerie électronique par le biais de règles de redirection [10].

L'implant **CredoMap** utilise un compte de messagerie compromis pour exfiltrer les données de navigateurs récupérés *via* le protocole IMAP [6] [2, 20, 21]. Dans d'autres campagnes, le MOA a utilisé des services en ligne comme PIPEDREAM, MOCKBIN ou MOCKY pour récupérer le contenu exfiltré [3, 5, 6, 7, 22].

L'ANSSI observe un ciblage accru par le MOA à l'encontre d'infrastructures de messagerie à des fins d'espionnage stratégique. Ce ciblage est réalisé au travers de différentes techniques, démontrant la capacité du MOA à collecter des informations sur la victime en amont afin d'adapter le niveau de sophistication de ses attaques.

6. *Internet Message Access Protocol* (IMAP) est un protocole permettant d'accéder et de manipuler des messages électroniques sur un serveur.

# 3 Recommandations

Pour faire face à ce type de menace, l'ANSSI rappelle l'importance d'avoir une approche globale de la sécurité, notamment *via* la réalisation d'une appréciation des risques. Celle-ci doit permettre d'identifier :

- les actifs devant être protégés ;
- l'état actuel du système d'information les supportant et du niveau de compétence des personnes l'utilisant ou l'opérant ;
- la nature des menaces vis-à-vis desquelles il convient de se préparer ;
- et par conséquent les mesures de sécurité appropriées devant être mises en œuvre et surtout entretenues dans le temps.

Dans cette section, les mesures de sécurité suivantes seront détaillées :

- Sécurité des échanges par courriers électroniques
  - Confidentialité des échanges par courriers électroniques
  - Plateforme d'échanges sécurisés
  - Réduction des risques de détournement de courriels depuis la boite de messagerie utilisateur
  - Réduction des risques de détournement des courriels en transit
  - Usurpation d'identité l'envoi de courriels piégés depuis ou vers des interlocuteurs
  - Réduction de la surface d'attaque des interfaces de messagerie web (*webmail*)
  - Réduction du risque de latéralisation depuis les serveurs Microsoft Exchange
  - Architecture de messagerie sécurisée
  - Capacités d'investigation pour identifier des courriels malveillants
- Sécurité des données d'authentification
  - Réduction des risques engendrés par les bases de fuites de données
  - Réduction des risques engendrés par les attaques par force brute en ligne
  - Réduction des risques liés aux campagnes d'hameçonnage
  - Réduction des risques engendrés par les attaques ciblant NTLM
- Sécurité des postes utilisateurs
  - Logiciels et pilotes malveillants ou détournés à des fins malveillantes
  - Limiter les possibilités de latéralisation depuis un poste utilisateur compromis
- Sécurisation de l'accès aux contenus hébergés sur Internet
  - Mise en œuvre d'un serveur mandataire et inspection TLS maitrisée
  - Identifier et limiter l'utilisation détournée de services spécialisés en ligne

Ces recommandations sont issues des guides suivants :

- « Guide de la méthode EBIOS Risk Manager » [23] ;
- « Recommandations relatives à l'authentification multifacteur et aux mots de passe » [24] ;
- « Recommandations relatives à l'interconnexion d'un système d'information à Internet » [25] ;
- « Recommandations-pour la mise en oeuvre dune politique de restrictions logicielles sous windows » [26] ;
- « Recommandations de sécurité pour l'architecture d'un système de journalisation » [27] ;
- « Recommandation de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory » [28] ;
- « Points de contrôles Active Directory » [29] ;
- « Classe de vulnérabilités en environnement Active Directory » [30]

## 3.1 Sécurité des échanges par courriers électroniques

Le MOA APT28 s'intéresse aux courriers électroniques qui peuvent être échangés au sein d'une entité. Le courriel est un support de communication d'apparence ordinaire, mais qui peut se révéler être une source d'information d'intérêt (négociations en cours, commandes, documents stratégiques, rapports, documents économiques et administratifs, rendez-vous, etc.) pour un MOA s'intéressant à une entité et son écosystème (prospects, clients, fournisseurs, partenaires commerciaux comme non-commerciaux, autorité de régulation, conseils, etc.).

Malheureusement, il est souvent difficile, voire impossible, de garantir qu'aucun des serveurs assurant le routage des courriels (agents de transfert de courriels, passerelle de filtrage, passerelle de gestion des messages, serveurs de messagerie) n'est piégé pour obtenir une copie des échanges ou pour les altérer.

R1

### Confidentialité des échanges par courriers électroniques

Même si sa mise en œuvre peut s'avérer complexe et ne peut être systématique, la mesure de sécurité la plus efficace reste le chiffrement de bout en bout des courriels ou des pièces jointes susceptibles de contenir des informations sensibles (par exemple *via* Zed!, S/MIME, PGP, archive chiffrée). À noter que les secrets ou données d'authentification utilisés pour le (dé)chiffrement doivent être partagés avec les interlocuteurs au travers d'un autre canal, sécurisé.

Lors de la mise en œuvre de ce type de mesure de sécurité, il ne faut pas oublier de mettre en place un séquestre des secrets de chiffrement : si le ou les porteurs de ces secrets venaient à être indisponibles de façon ponctuelle ou permanente, la continuité d'activité pourrait en être affectée.

R2

### Plateforme d'échanges sécurisés

L'emploi d'une plateforme d'échanges sécurisés en complément des courriels est également recommandé afin d'y faire transiter les informations sensibles. La sécurisation de ce type de plateforme devra faire l'objet d'un soin particulier (par exemple : authentification multifacteurs, réduction de la surface de fonctionnalité et donc de la surface d'attaque au strict nécessaire, purge à intervalles réguliers des données en transit, chiffrement à la volée, etc.)

R3

### Réduction des risques de détournement de courriels depuis la boite de messagerie utilisateur

De nombreuses applications de messagerie permettent aux utilisateurs de créer des règles de copie et redirection automatique des courriels reçus ou émis. Le MOA APT28 se sert parfois de ce type de mécanisme lorsqu'il compromet les boîtes de messagerie de ses cibles. La fonctionnalité étant déjà présente, son activation peut souvent se faire de façon discrète et rester longtemps inaperçue de l'utilisateur légitime.

Lorsque les applications le permettent, et si ce type de mécanisme n'est pas nécessaire pour un motif impérieux, l'ANSSI recommande dans la mesure du possible de les désactiver. À défaut, de les rendre configurables uniquement aux personnes ou services en ayant absolument besoin.

L'ANSSI recommande par ailleurs une revue périodique de ce type de configuration de redirection afin de s'assurer de leur légitimité.

R4

## Réduction des risques de détournement des courriels en transit

Il est important de ne pas oublier qu'un attaquant peut choisir de s'attaquer directement aux passerelles de filtrage de courriels se situant en amont du serveur de réception d'une entité. Ainsi, en cas de soupçon de compromission des courriels et en l'absence de traces suspectes sur le système d'information, il est important d'investiguer sur ces briques amont. Tout d'abord, en vérifiant que leur configuration est cohérente et n'a pas été altérée (filtrage, sélection, redirection, etc.), par exemple pour réaliser une copie de tout ou partie des courriels vers un serveur tiers. Puis, en vérifiant que ces passerelles sont à jour de leurs correctifs de sécurité ou n'exposent pas publiquement d'interface d'administration, susceptibles d'offrir une porte d'entrée à un attaquant. Le cas échéant, il conviendra de procéder à des investigations numériques à la recherche de traces de compromission.

Dans le cas où des services sont externalisés ou opérés par un prestataire, il est nécessaire de s'assurer que le service intègre tous les mécanismes de sécurité et les options de configuration répondant au besoin, en particulier les points suivants :

- chiffrement des communications ;
- cloisonnement, même logiciel, avec les autres clients ;
- journalisation des événements et auditabilité des configurations ;
- capacités de détection des incidents de sécurité ou d'événements inhabituels.

Si des doutes persistent, des investigations numériques complémentaires avec le prestataire sont à réaliser.

R5

## Usurpation d'identité lors de l'envoi de courriels piégés depuis ou vers des interlocuteurs

Sans avoir à compromettre un compte de messagerie, il est aisé pour un attaquant de contrefaire des courriels avec le nom de domaine d'une entité ou de ses interlocuteurs. Ce stratagème peut être utilisé pour tromper la vigilance d'un utilisateur en lui envoyant des courriels qui, d'apparence, semblent provenir d'un contact habituel. Pour limiter la nuisance de ces courriels, en amont de leur réception par les utilisateurs, l'ANSSI encourage à mettre en œuvre certains protocoles ayant pour rôle de vérifier l'authenticité et l'intégrité des courriels. Ils nécessitent une configuration, non seulement par l'entité expéditrice sur les enregistrements DNS de ses noms de domaine, mais aussi par l'entité destinataire sur ses serveurs SMTP de réception. Ces protocoles sont :

- **Sender Policy Framework** (SPF) qui permet de spécifier les adresses IP des serveurs autorisés à émettre les courriels d'un domaine ;
- **DomainKeys Identified Mail** (DKIM) qui permet l'authentification du domaine de messagerie d'un courriel à l'aide d'une signature cryptographique ;
- **Domain-based Message Authentication, Reporting and Conformance** (DMARC) qui permet notamment à une entité de définir une politique de traitement de ses courriels envoyés en fonction des résultats de conformité SPF et DKIM.

R6

## Réduction de la surface d'attaque des interfaces de messagerie web (*webmail*)

Les interfaces de messagerie web sont des cibles de choix en raison de leur surface d'attaque très importante, liée à leur richesse en fonctionnalités. Ces trois dernières années ont été particulièrement marquées par la découverte et la publication de nombreuses vulnérabilités affectant plusieurs de ces services. Nombre de ces vulnérabilités ne nécessitaient aucune authentification préalable et parfois l'accès à un seul compte suffisait pour mettre en péril l'ensemble de l'applicatif. APT28, comme de nombreux autres acteurs, s'est massivement servi de ces brèches. L'ANSSI a traité et continue de traiter de nombreux cas de compromission ayant comme point de départ ce type de service.

Lorsque des interfaces de messagerie web sont mises en œuvre, l'ANSSI recommande fortement de ne pas les exposer publiquement sur Internet et de ne les rendre accessibles qu'en interne ou *via* un VPN pour les personnes en situation de nomadisme ou de télétravail.

Néanmoins, si pour d'impérieuses raisons opérationnelles ces accès doivent être exposés, il est recommandé, sur la base de l'appréciation des risques, de mettre en œuvre une chaîne d'accès avec des ressources dédiées, des restrictions d'accès aux seules boîtes de messagerie concernées et une stratégie renforcée de détection, par exemple :

- un serveur d'exposition (exemple : portail de messagerie web) hébergé au sein de la zone de services exposés ;
- la configuration d'accès aux seules boîtes de messagerie concernées ;
- la protection du serveur d'exposition par un serveur mandataire inverse (*reverse proxy*), voire un pare-feu applicatif, hébergé en zone de services relais ;
- la mise en œuvre d'une authentification double facteur pour les utilisateurs, éventuellement avec la fourniture d'un certificat électronique ;
- la définition d'une stratégie renforcée de détection (géolocalisation des connexions, nombre d'authentifications échouées, volumes de courriels échangés) ;
- une veille rigoureuse sur la publication de vulnérabilités affectant ce type d'application et une réactivité appropriée seront elles aussi déterminantes.

Cependant, il est important de noter que dans le cadre d'une infrastructure Microsoft Exchange, il n'est pas possible de dissocier les fonctionnalités de messagerie Web des autres fonctionnalités d'un serveur ou *cluster* Microsoft Exchange. Or, par nature, un serveur Microsoft Exchange dispose d'une emprise très forte dans un écosystème Microsoft, car il permet notamment la gestion de tous les comptes (à l'exception, de ceux constituant le Tier 0 d'un domaine Active Directory) et ce au-delà du simple périmètre de la fonction de courrier électronique. Par conséquent, la compromission d'un serveur Microsoft Exchange, par exemple au travers de son interface web, mettra en péril le Système d'information.

R7

## Réduction du risque de latéralisation depuis les serveurs Microsoft Exchange

En raison d'une mauvaise configuration ou d'une configuration historique, un serveur Microsoft Exchange peut disposer de droits privilégiés dans un environnement Active Directory (AD). En cas de compromission, un attaquant peut abuser de cette situation pour élever ses privilèges et prendre le contrôle d'un annuaire AD, entrainant de fait la compromission du système d'information associé. Dans une logique de sécurité en profondeur, l'ANSSI encourage à vérifier que l'annuaire AD a été durci pour éviter les risques d'élévation de privilège en cas de compromission d'un serveur Microsoft Exchange [29].

R8

## Architecture de messagerie sécurisée

Afin de protéger le système d'information interne des courriels malveillants (*phishing*, *spear phishing*, etc.), il est recommandé de construire une architecture en s'appuyant sur des serveurs relais de messagerie au sein d'une passerelle sécurisée [25].

Pour les besoins de messagerie externes à l'entité (c'est-à-dire avec une interconnexion à Internet), au moins un serveur SMTP doit être positionné au sein de la passerelle Internet sécurisée. Néanmoins, en tenant compte de la complexité et coûts associés, il est recommandé de dédier un serveur SMTP pour l'envoi et un autre pour la réception de courriels (par exemple : deux machines virtuelles distinctes) au sein de la passerelle Internet sécurisée. Ils doivent être configurés en conséquence :

- un serveur SMTP d'envoi n'accepte les courriels que depuis une liste de serveurs autorisés (serveurs relais internes ou serveurs de boîtes aux lettres) et assure des fonctions de nettoyage des en-têtes afin de limiter la divulgation d'informations pouvant être réutilisées par un attaquant (par exemple, par la suppression des en-têtes « received » ou « X-»);
- un serveur SMTP de réception applique les premières politiques de sécurité, assure des fonctions d'analyse protocolaire et de contenu, qualifie les courriels nécessitant une mise en quarantaine et transmet *in fine* les courriers à un autre serveur relais de l'entité ou à un serveur de boîtes aux lettres;
- un serveur relais au sein du système d'information interne chaîné aux serveurs d'envoi et de réception exposé à Internet au travers de la passerelle sécurisée.

À noter que si finalement un seul serveur est positionné au sein de la passerelle Internet sécurisée pour assurer cette fonction d'interface entre l'interne et l'externe, la logique de configuration des fonctions d'envoi, réception et relais reste applicable.

Pour les besoins de messagerie interne (c'est-à-dire sans interconnexion à Internet), déployer au moins un serveur relais au sein du système d'information interne qui sera dédié au besoin interne uniquement. Ce serveur ne doit être en aucun cas chaîné à un serveur SMTP exposé sur Internet.

R9

## Capacités d'investigation pour identifier des courriels malveillants

Les dispositifs de sécurité et de filtrage disposés en amont des serveurs de messagerie ne sont pas infaillibles, et des messages malveillants peuvent être reçus par les utilisateurs. Il est alors important de connaître les capacités de journalisation et de recherche. Ces mécanismes pourront être mis à contribution lorsque, sur la base d'un signalement, un ou plusieurs courriels suspects et les activités associées devront être recherchés.

Ainsi, lorsque des indicateurs de compromissions (*Indicator of Compromise* ou IoC) sont partagés, ceux-ci portent le plus souvent sur :

- une ou plusieurs adresses émettrices/destinataires ;
- un domaine malveillant ou détourné ;
- l'objet du courriel ;
- le corps du courriel contenant un texte, lien, un ensemble de mots de clés ;
- une période d'émission/réception.

Concernant les pièces jointes, les indicateurs portent le plus souvent sur :

- nom ;
- extension ;
- métadonnées ;
- empreintes MD5/SHA1/SHA256 ;
- contenu.

Ces IoC peuvent être précis ou encore porter sur un schéma caractéristique recherchable par exemple au travers d'une expression rationnelle ou d'une règle Yara.

L'identification d'un courriel malveillant doit être vue comme un point de départ d'une investigation et ne doit pas seulement se résumer à une action de suppression. Dans la mesure du possible, il est recommandé d'essayer de répondre aux questions suivantes :

- est-ce que le courriel malveillant a été bloqué ou non par les dispositifs de filtrage amont ? Dans un cas comme dans l'autre, quelles ont été les conclusions d'analyse de ces solutions amont ?
- est-il possible d'en récupérer une copie ?
- est-ce que plusieurs utilisateurs ont reçu ce même courriel ?
- existe-t-il d'autres variantes de ce courriel dans l'environnement ?
- est-ce que la ou les personnes concernées ont effectivement reçu, ouvert, supprimé, transféré le courriel ou ses pièces jointes ? Si oui quand, comment, à qui ?
- est-ce que des activités système ou réseau suspectes depuis le compte ou le poste de ces utilisateurs ont été observées suite aux actions précédemment identifiées ?

Pour répondre à ces questions, il est nécessaire de disposer de différents points de journalisation collectables et pouvant être corrélés : passerelle de filtrage, serveur de messagerie, poste utilisateur, proxy réseau, pare-feu, annuaire Active Directory (le cas échéant). Ces évènements ayant pu survenir plusieurs mois en arrière, il est donc recommandé, en accord avec les contraintes légales ou réglementaires et les capacités de l'entité, de dimensionner suffisamment la conservation de cette journalisation.

Enfin, échanger avec la ou les personnes concernées sur les actions qu'elles ont pu réaliser autour de ce courriel est également important. En effet, certains courriels ne contiennent parfois aucune charge ou lien malveillant, mais seulement une liste d'instructions à effectuer par l'utilisateur. De plus, celui-ci peut parfois être en mesure d'expliquer le contexte précédant la réception du courriel malveillant.

## 3.2 Sécurité des données d'authentification

R10

### Réduction des risques engendrés par les bases de fuites de données

Comme de nombreux MOA, APT28 exploite des bases de fuites de données à la recherche de mots de passe toujours valides.

Pour faire face à ce type de risque, plusieurs mesures complémentaires sont recommandées [24] :

- mettre en œuvre de l'authentification multifacteur ;
- privilégier l'utilisation d'un mot de passe fort bien mémorisé et pour lequel l'utilisateur est conscient de sa sensibilité, plutôt que le renouvellement à intervalles courts (par exemple, tous les 90 jours) comme recommandé autrefois ;
- sensibiliser à l'utilisation de secrets d'authentification distincts pour accéder à différents services, et encourager à l'utilisation de coffre-forts de mots de passe sécurisés ;
- favoriser la mise en œuvre de service d'authentification unique (Single Sign On) comme Kerberos, afin de limiter le nombre de secrets d'authentification à mémoriser ;
- auditer à intervalles réguliers la robustesse des mots de passe utilisateur et demander un renouvellement si nécessaire.

R11

### Réduction des risques engendrés par les attaques par force brute en ligne

Afin de réduire les risques de compromission des comptes utilisateurs sur des services en ligne, il est recommandé [24] :

- de s'assurer que les comptes et mots de passe par défaut ont été désactivés ou changés ;
- de définir une politique de mots de passe forts, incluant la vérification à la saisie ;
- d'implémenter de l'authentification multifacteur ;
- d'implémenter des mécanismes détectant les essais multiples d'authentification depuis une ou plusieurs adresses IP distinctes, qui soient en mesure de les bloquer ou de réduire le nombre de tentatives possibles ;
- d'auditer à intervalles réguliers la robustesse des mots de passe utilisateurs et de demander un renouvellement si nécessaire.

R12

## Réduction des risques liés aux campagnes d'hameçonnage

L'hameçonnage reste une valeur sûre pour les attaquants. Lorsqu'il est réalisé de manière élémentaire, les taux de réussite peuvent néanmoins être élevés. Lorsqu'il est réalisé avec soin, même un utilisateur expérimenté peut se faire piéger. Si les campagnes d'hameçonnage par courriels malveillants restent une voie classique très prisée, il ne faut pas oublier les autres formes de campagnes d'hameçonnage possibles. Par exemple :

- *via* des messages sur les réseaux sociaux ;
- *via* des messages par SMS ou messageries instantanées (WhatsApp, Signal, Telegram, TikTok, Slack, Discord, Facebook Messenger, etc. ) ;
- *via* des appels téléphoniques ;
- *via* des attaques par redirection de connexion lorsque la navigation Internet est effectuée en HTTP.

Il faut donc former les utilisateurs à savoir reconnaître les différentes formes d'hameçonnage, mais également les éventuelles pages d'hameçonnage. Cette sensibilisation doit tenir compte du scénario où les moyens de communication d'un contact ont été détournés par un attaquant.

La séparation des moyens de communication professionnels et personnels est une mesure de sécurité importante, car elle permet de réduire les risques de confusion entre les canaux de communications susceptibles d'être visés par des campagnes d'hameçonnage.

Même si elle n'est pas infaillible, l'utilisation de mécanismes d'authentification multifacteurs pour protéger l'accès aux services est une mesure de sécurité particulièrement efficace pour lutter contre les scénarios courants de vols de secrets de connexion par hameçonnage.

Le succès de certaines campagnes d'hameçonnage repose sur l'usurpation de l'identité de marque. Mettre en œuvre des moyens techniques, organisationnels et juridiques pour y faire face est souvent nécessaire pour :

- filtrer les courriels usurpant des adresses d'une entité (cf. supra) ;
- détecter, bloquer et faire fermer les domaines malveillants jouant sur les fautes de frappe opportunistes (*typosquatting*) ;
- détecter, bloquer et faire fermer les sites ou pages malveillantes usurpant l'identité d'une entreprise.

R13

## Réduction des risques engendrés par les attaques ciblant NTLM

À l'instar de l'utilisation par le MOA APT28 de la vulnérabilité CVE-2023-23397, les attaques ciblant les secrets et défis-réponses NTLM sont très courantes. Elles ouvrent en effet des possibilités d'attaque hors ligne par force brute en vue d'obtenir des mots de passe utilisateurs et permettent par ailleurs de mener des attaques de type relais NTLM. Dans le cadre de cette vulnérabilité, une hygiène réseau correctement implémentée permet d'invalider l'exploitation telle qu'elle a été décrite plus haut dans ce document. En effet, le MOA a besoin que la victime puisse établir une connexion SMB depuis son poste vers une machine qu'il maîtrise (en l'occurrence, des routeurs compromis). Or, sauf cas très particulier, aucun flux SMB ne devrait être autorisé en sortie d'un réseau d'entreprise. Le pare-feu du poste utilisateur ou en périphérie du réseau doit bloquer cette tentative et attirer l'attention des équipes sécurité. Cependant, si pour des motifs impérieux l'établissement de connexions SMB vers l'extérieur doit être permise, une liste blanche des destinations devrait être établie.

Par ailleurs, les connexions sortantes du système d'information interne ne devraient pas par défaut utiliser l'authentification unique interne (*Single Sign On* / SSO) ; pour ce faire une liste de domaines autorisés à s'appuyer sur le SSO interne devrait être établie et appliquée sur l'ensemble du système d'information.

Les secrets et défis-réponses NTLM sont par nature vulnérables aux attaques par force brute visant à essayer de retrouver les mots de passe associés. Une politique de mots de passe forts et de non-réutilisation de mots de passe doit donc être appliquée [24].

La désactivation globale de l'authentification NTLM au profit d'une utilisation exclusive de Kerberos rend également ces attaques inopérantes. Il s'agit d'une mesure générique particulièrement efficace. Cependant, l'authentification NTLM reste souvent nécessaire au bon fonctionnement de certaines applications non migrées vers Kerberos, et il n'est donc pas toujours possible d'interdire NTLM globalement. Pour tenir compte de cette complexité de mise en œuvre, des évolutions progressives portées par Microsoft (par exemple au travers des versions récentes de Windows 11), et des contraintes d'étalement dans le temps d'une telle migration, l'ANSSI encourage à commencer en priorité par les services les plus critiques ou assurant une fonction de gestion de parc informatique, en désactivant pour ces serveurs les connexions sortantes utilisant NTLM (par exemple pour les serveurs et services suivants : contrôleurs de domaine, Microsoft Exchange, Microsoft Endpoint Configuration Manager, System Center Configuration Manager, etc.).

L'ANSSI tient à disposition sur le site du CERT-FR une page dédiée au sujet [30].
Enfin, Microsoft a mis à disposition un ensemble d'outils et recommandations pour aider à l'investigation d'une potentielle exploitation de la vulnérabilité CVE-2023-23397 [31].

## 3.3 Sécurité des postes utilisateurs

R14

### Logiciels et pilotes malveillants ou détournés à des fins malveillantes

APT28 dispose de son propre arsenal d'outils malveillants. Toutefois, comme de nombreux acteurs malveillants, le MOA emploie aussi dans le cadre de ses attaques des outils légitimes importés par ses soins ou disponibles par défaut sur les systèmes visés. Le détournement de ces derniers à des fins malveillantes vise à complexifier la détection et ainsi à renforcer son niveau de discrétion. Ainsi, plusieurs lignes complémentaires de défense en profondeur sont nécessaires.

En premier lieu, il convient d'utiliser les lignes de défense élémentaires intégrées au système d'exploitation ainsi que les solutions antivirales et d'activer :

- la détection des applications/programmes potentiellement indésirables (*Potentially Unwanted Applications/Programs* (PUA/PUP)) ;
- la détection des pilotes et microprogrammes compromis ;
- l'intégrité de la protection mémoire ;
- *Microsoft Defender Application Guard* [32] ;
- *Credential Guard*.

De plus, le suivi des alertes de détection qui seront levées est indispensable afin d'être en mesure de réagir promptement le cas échéant.

En second lieu, il convient d'utiliser des lignes de défense avancées pour limiter l'efficacité des logiciels malveillants ou détournés non détectés par les solutions antivirales :

- définir et mettre en œuvre une politique de restriction logicielle afin de restreindre l'exécution à une liste de programmes ou emplacements dûment autorisés (par exemple : dans le cadre de la mise en œuvre d'une liste noire en bloquant les répertoires temporaires depuis lesquels sont ouvertes les pièces jointes des courriels) [26] ;
- définir une politique de filtrage réseau rigoureuse au niveau poste utilisateur, afin tout d'abord de bloquer de façon stricte les flux entrants à l'exception des flux dûment autorisés, puis en restreignant les flux sortants en fonction de leur nature et destinations ;
- mettre en place un système de journalisation efficace et sécurisé [27, 28] ;
- mettre en place une supervision de ces journaux et implémenter des heuristiques de détection visant à rechercher des détournements d'applications légitimes à des fins malveillantes.

L'identification et le suivi dans le temps des applications et pilotes détournables à des fins malveillantes peuvent se révéler être une tâche fastidieuse. Des projets communautaires existent [33, 34].

R15

### Limiter les possibilités de latéralisation depuis un poste utilisateur compromis

Lorsque le MOA APT28 parvient à la compromission d'un poste utilisateur, celui-ci ne se contente pas uniquement d'exfiltrer l'information disponible, mais peut aussi chercher à se latéraliser au sein du système d'information. La gestion des risques de l'entité doit inclure un ou plusieurs scénarios sur la compromission de postes utilisateurs et doit prendre en compte l'importance de la résilience de l'infrastructure face à ce risque. Ce travail doit déterminer, de façon cohérente et maintenable, différentes stratégies de segmentation :

- réseau,
- applicatives,
- fonctionnelles (par exemple : utilisateurs, utilisateurs privilégiés, administrateurs, administrateurs AD, etc.)
- physiques et logiques,
- etc.

L'ANSSI rappelle que dans le cadre d'un environnement Microsoft AD, l'annuaire doit au minimum posséder un niveau de sécurité basique non affaibli depuis son installation (ce qui correspond par exemple au niveau 3 du référentiel ANSSI) [29].

## 3.4 Sécurisation de l'accès aux contenus hébergés sur Internet

R16

### Mise en œuvre d'un serveur mandataire et inspection TLS maitrisée

Il est essentiel d'éviter tout accès direct depuis un poste utilisateur ou un serveur vers Internet. Pour cela, un serveur mandataire (proxy) Web doit assurer le rôle de relais et mettre en œuvre des fonctions de sécurité : authentification, contrôle d'accès, analyse de contenus, journalisation, etc. Tous les accès aux contenus hébergés sur le Web doivent être authentifiés de manière individuelle pour les utilisateurs et non ambiguë pour les services.

Le nombre de sites accessibles en HTTPS est en constante augmentation et constitue une avancée majeure dans la sécurisation des communications dans la mesure où la configuration TLS associée est à l'état de l'art. La contrepartie est que, s'il s'agit d'accès à des sites d'hameçonnage (*phishing*) ou d'hébergement de codes malveillants, il est théoriquement impossible de détecter le contenu suspect dans l'ensemble du trafic chiffré. Pour pallier cela, la mise en place d'inspection TLS est une possibilité. Celle-ci doit permettre *in fine* d'analyser le contenu et de s'assurer de la conformité protocolaire des échanges. L'inspection TLS répond donc au besoin de détection de codes malveillants et doit, le cas échéant, être mise en œuvre de façon sécurisée au sein de la zone de services relais. Le choix de l'équipement réalisant cette inspection est structurant ; celui-ci doit notamment permettre une configuration des paramètres cryptographiques à l'état de l'art [25].

R17

## Identifier et limiter l'utilisation détournée de services spécialisés en ligne

Il existe en ligne de nombreux services permettant de simuler des points de terminaison personnalisables (« `mockbin[.]org` », « `mocky[.]io` », « `pipedream[.]com` », « `frge[.]io` », « `webhook[.]site` », etc.). Ces services légitimes spécialisés peuvent être utilisés de façon détournée à des fins malveillantes par exemple pour mener des campagnes de *phishing* ou pour réaliser de l'exfiltration de données. Il est à noter que ces services répondent à des besoins métier très spécialisés. Il convient de s'interroger sur le besoin d'accéder à ce type de service et le cas échéant d'autoriser au cas par cas leur accès.

Les mécanismes de sécurité détaillés dans la recommandation précédente, permettent de mettre en œuvre les politiques de filtrages adéquates ou la recherche *a posteriori* en cas de besoin d'investigation.

# 4 Bibliographie

[1] MalwareBytes. *Russia's APT28 Uses Fear of Nuclear War to Spread Follina Docs in Ukraine*. 21 juin 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. *Attaque informatique du groupe APT28 à l'aide du code malveillant CredoMap*. 20 juin 2022.
URL : https://cert.gov.ua/article/341128.

[3] CERT-UA. *Attaque informatique du groupe APT28 à l'aide du code malveillant CredoMap_V2*. 6 mai 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)*. 15 mars 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*. 5 mai 2023.
URL : https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/.

[6] CERT-UA. *Attaques par hameçonnage du groupe APT28 visant à obtenir des données d'authentification pour des services de messagerie publique*. 8 juillet 2023.
URL : https://cert.gov.ua/article/5105791.

[7] CERT-UA. *Campagne d'hameçonnage utilisant le thème du service UKR.NET et des QR-codes*. 16 mars 2022.
URL : https://cert.gov.ua/article/37788.

[8] CERT-UA. *Attaque informatique d'APT28 : diffusion de courriels contenant des « instructions » pour la « mise à jour du système d'exploitation »*. 28 avril 2023.
URL : https://cert.gov.ua/article/4492467.

[9] Google. *Threat Horizons*. 7 décembre 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*. 20 juin 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*. 23 septembre 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*. 4 juin 2021.
URL : https://blog.cluster25.duskrise.com/2021/06/03/a-not-so-fancy-game-apt28-skinnyboy.

[13] NSA. *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*. 1er juillet 2021.
URL : https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO0158036-21.PDF.

[14] Trellix. *Prime Minister's Office Compromised : Details of Recent Espionage Campaign*. 25 janvier 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*. 28 septembre 2022.
URL : https://securityscorecard.com/research/apt28s-stealer-called-credomap/.

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

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

[18] ANSSI. *Bulletin d'alerte du CERT-FR : vulnérabilité dans Microsoft Outlook*. 15 mars 2023.
URL : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-002/.

[19] MICROSOFT. *Guidance for Investigating Attacks Using CVE-2023-23397*. 24 mars 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.* 21 décembre 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*. 6 juin 2022.
URL : https://www.trellix.com/en-us/about/newsroom/stories/research/growling-bears-make-thunderous-noise.html.

[22] CERT-UA. *Attaque informatique d'APT28 : msedge utilisé comme loader, TOR et les services mockbin.org/website.hook utilisés comme centre de contrôle*. 4 septembre 2023.
URL : https://cert.gov.ua/article/5702579.

[23] ANSSI. *Guide de la méthode EBIOS Risk Manager*.
URL : https://cyber.gouv.fr/ebios-rm.

[24] ANSSI. *Recommandations relatives à l'authentification multifacteur et aux mots de passe*. 8 octobre 2021.
URL : https://cyber.gouv.fr/guide-authentification.

[25] ANSSI. *Recommandations relatives à l'interconnexion d'un système d'information à Internet*. 19 juin 2020.
URL : https://cyber.gouv.fr/guide-interconnexion-si-internet.

[26] ANSSI. *Recommandations-pour la mise en oeuvre dune politique de restrictions logicielles sous windows*. 13 janvier 2017.
URL : https://cyber.gouv.fr/guide-windows-restrictions-logicielles.

[27] ANSSI. *Recommandations de sécurité pour l'architecture d'un système de journalisation*. 28 janvier 2022.
URL : https://cyber.gouv.fr/guide-journalisation.

[28] ANSSI. *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory*. 28 janvier 2022.
URL : https://cyber.gouv.fr/guide-journalisation-windows.

[29] ANSSI. *Points de contrôles Active Directory*. 18 octobre 2022.
URL : https://cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/.

[30] ANSSI. *Classe de vulnérabilités en environnement Active Directory*. 18 octobre 2022.
URL : https://cert.ssi.gouv.fr/dur/CERTFR-2021-DUR-001/.

[31] MICROSOFT. *Guidance for investigating attacks using cve-2023-23397*. 24 mars 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 vue d'ensemble*. 13 juillet 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. *Projet communautaire : Living Off The Land Binaries, Scripts and Libraries*.
URL : https://lolbas-project.github.io/.

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

1.0 - 26 octobre 2023



**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

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

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*