aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois de décembre 2023

2023-12-31 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. Synthèse

Ce mois ci, le CERT aDvens vous propose trois vulnérabilités présentant un intérêt, en complément de celles déjà publiées.

Au travers de deux articles, les analystes du CERT présentent une analyse sur les diverses méthodes d'extorsion utilisées lors d'attaques rançongiciel, suivie d'un état des lieux de l'emploi des applications **OAuth** servant à mener des activités cybercriminelles.

2. Vulnérabilités

Ce mois-ci, le CERT aDvens met en exergue **trois** vulnérabilités affectant des technologies fréquemment utilisées au sein des entreprises.
Elles sont présentées par ordre de gravité (preuves de concept disponibles, exploitation …). L'application de leurs correctifs ou contournements est fortement recommandée.

Le CERT aDvens recommande de tester les mesures de contournement proposées dans un environnement dédié avant leur déploiement en production afin de prévenir tout effet de bord.

2.1. Apache OFBiz - CVE-2023-49070

Le 4 décembre 2023, Apache alerte dans son bulletin de sécurité, d'une vulnérabilité critique (CVE-2023-49070) affectant sa solution *OFBiz*.

Apache OFBiz est un logiciel Open-Source de gestion de ressources, utilisé par des entreprises de plus de 10000 employés.

Cette faille est due à la présence d'un composant XML-RPC déprécié. Elle permet à un attaquant non authentifié, d'injecter du code arbitraire dans des application vulnérables.

2.1.1. Risque

- Exécution de code arbitraire

2.1.2. Type de vulnérabilité

- **CWE-94** : Improper Control of Generation of Code ('Code Injection')

2.1.3. Criticité

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.1.4. Composants vulnérables

- Apache OFBiz versions 18.12.09 et antérieures

2.1.5. Recommandations

- Mettre à jour Apache OFBiz vers la version 18.12.10 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin d'Apache.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. Unitronics - CVE-2023-6448

Le 28 novembre 2023, le CISA a publié une alerte concernant une vulnérabilité dans les API (Automate Programmable Industriel) Unitronics. Ces API sont fréquemment utilisés dans le secteur du traitement des eaux, de l'énergie, de l'agroalimentaire et de la santé.

L'utilisation d'un mot de passe administrateur par défaut permet à un attaquant, diposant d'un accès à ces API, de prendre le contrôle du système vulnérable.

Cette vulnérabilité est actuellement exploitée par le groupe Iranien CyberAv3ngers.
Le CISA a ajoutée cette CVE à son référentiel de vulnérabilités exploitées (KEV), le 12 décembre 2023.

2.2.1. Risque

- Compromission du système

2.2.2. Types de vulnérabilités

- **CWE-798** : Use of Hard-coded Credentials
- **CWE-1188** : Initialization of a Resource with an Insecure Default

2.2.3. Criticité

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.2.4. Composants vulnérables

- Unitronics VisiLogic versions antérieures à 9.9.00

2.2.5. Recommandations

- Mettre à jour Unitronics VisiLogic vers la version 9.9.00 ou ultérieure.
- Ne pas exposer les APIs sur internet.
- Des informations complémentaires sont disponibles dans le bulletin d'Unitronics ou du CISA.

2.2.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

2.2.7. Indicateurs de compromission

TLP	TYPE	VALEUR
TLP:CLEAR	MD5	BA284A4B508A7ABD8070A427386E93E0
TLP:CLEAR	SHA1	66AE21571FAEE1E258549078144325DC9DD60303
TLP:CLEAR	SHA256	440b5385d3838e3f6bc21220caa83b65cd5f3618daea676f271c3671650ce9a3
TLP:CLEAR	IP	178.162.227.180
TLP:CLEAR	IP	185.162.235.206

2.3. QNAP - CVE-2023-47565

Le 11 décembre 2023, la société QNAP alerte sur une vulnérabilité affectant *VioStor NVR (Network Video Recorder)*, une solution de vidéosurveillance en réseau de caméras IP.

Un défaut de contrôle des données envoyées par l'utilisateur permet à un attaquant, distant et authentifié, de modifier les paramètres NTP pour exécuter du code.

Cette vulnérabilité est actuellement exploitée par le variant Mirai InfectedSlurs.
Le CISA a ajoutée cette CVE à son référentiel de vulnérabilités exploitées (KEV), le 21 décembre 2023.

2.3.1. Risque

- Exécution de code arbitraire

2.3.2. Type de vulnérabilité

- **CWE-78** : Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.3.3. Criticité

Vecteur d'attaque	Adjacent	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Faible	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.3.4. Composants vulnérables

- QVR versions de firmware 4.X

2.3.5. Recommandations

- Mettre à jour le firmware de QVR vers la version 5.x ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de QNAP ou du CISA.

2.3.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

2.3.7. Indicateurs de compromission

TLP	TYPE	VALEUR
TLP:CLEAR	SHA256 I Payload	dabdd4b5a3a70c64c031126fad36a4c45feb69a45e1028d79da6b443291addb8 I arm
TLP:CLEAR	SHA256 I Payload	3f3c2e779f8e3d7f2cc81536ef72d96dd1c7b7691b6e613f5f76c3d02909edd8 I arm5
TLP:CLEAR	SHA256 I Payload	75ef686859010d6164bcd6a4d6cf8a590754ccc3ea45c47ace420b02649ec380 I arm6
TLP:CLEAR	SHA256 I Payload	f8abf9fb17f59cbd7381aa9f5f2e1952628897cee368defd6baa6885d74f3ecc I arm7
TLP:CLEAR	SHA256 I Payload	8777f9af3564b109b43cbcf1fd1a24180f5cf424965050594ce73d754a4e1099 I kdvrarm7
TLP:CLEAR	SHA256 I Payload	ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1 I mips
TLP:CLEAR	SHA256 I Payload	a4975366f0c5b5b52fb371ff2cb034006955b3e3ae064e5700cc5365f27a1d26 I mpsl
TLP:CLEAR	SHA256 I Payload	cd93264637cd3bf19b706afc19944dfb88cd27969aaf0077559e56842d9a0f87 I nigga.sh
TLP:CLEAR	SHA256 I Payload	8e64de3ac6818b4271d3de5d8e4a5d166d13d12804da01ce1cdb7510d8922cc6 I ok.sh
TLP:CLEAR	SHA256 I Payload	35fcc2058ae3a0af68c5ed7452e57ff286abe6ded68bf59078abd9e7b11ea90a I ppc
TLP:CLEAR	SHA256 I Payload	7cc62a1bb2db82e76183eb06e4ca84e07a78cfb71241f21212afd1e01cb308b2 I sh4
TLP:CLEAR	SHA256 I Payload	29f11b5d4dbd6d06d4906b9035f5787e16f9e23134a2cc43dfc1165127c89bff I spc
TLP:CLEAR	SHA256 I Payload	cfbcbb876064c2cf671bdae61544649fa13debbbe58b72cf8c630b5bfc0649f9 I x86
TLP:CLEAR	SHA256 I Payload	a3b78818bbef4fd55f704c96c203765b5ab37723bc87aac6aa7ebfcc76dfa06d I mpsl
TLP:CLEAR	SHA256 I Payload	ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1 I mips
TLP:CLEAR	domaine C2	opewu[.]homes
TLP:CLEAR	domaine C2	wu[.]qwewu[.]site
TLP:CLEAR	domaine C2	dfvzfvd[.]help
TLP:CLEAR	domaine C2	husd8uasd9[.]online
TLP:CLEAR	domaine C2	homehitter[.]tk
TLP:CLEAR	domaine C2	shetoldmeshewas12[.]oss
TLP:CLEAR	domaine C2	shetoldmeshewas12[.]geek
TLP:CLEAR	domaine C2	shetoldmeshewas12[.]pirate
TLP:CLEAR	domaine C2	shetoldmeshewas12[.]dyn
TLP:CLEAR	domaine C2	shetoldmeshewas12[.]libre
TLP:CLEAR	domaine C2	shetoldmeshewas12[.]gopher
TLP:CLEAR	domaine C2	shetoldmeshewas12[.]parody
TLP:CLEAR	domaine C2	shetoldmeshewas13[.]oss
TLP:CLEAR	domaine C2	shetoldmeshewas13[.]geek
TLP:CLEAR	domaine C2	shetoldmeshewas13[.]pirate
TLP:CLEAR	domaine C2	shetoldmeshewas13[.]dyn
TLP:CLEAR	domaine C2	shetoldmeshewas13[.]libre

TLP	TYPE	VALEUR
TLP:CLEAR	domaine C2	shetoldmeshewas13[.]gopher
TLP:CLEAR	domaine C2	shetoldmeshewas13[.]parody
TLP:CLEAR	domaine C2	hujunxa[.]cc
TLP:CLEAR	domaine C2	skid[.]uno
TLP:CLEAR	domaine C2	dogeating[.]monster
TLP:CLEAR	domaine C2	chinkona[.]buzz
TLP:CLEAR	domaine C2	dogeatingchink[.]uno
TLP:CLEAR	domaine C2	infectedchink[.]cat
TLP:CLEAR	domaine C2	infectedchink[.]online
TLP:CLEAR	domaine C2	sdfsd[.]xyz
TLP:CLEAR	domaine C2	gottalovethe[.]indy
TLP:CLEAR	domaine C2	pqahzam[.]ink
TLP:CLEAR	domaine C2	cooldockmantoo[.]men
TLP:CLEAR	domaine C2	chinks-eat-dogs[.]africa
TLP:CLEAR	domaine C2	cnc[.]kintaro[.]cc
TLP:CLEAR	domaine C2	fuckmy[.]site
TLP:CLEAR	domaine C2	fuckmy[.]store
TLP:CLEAR	domaine C2	hbakun[.]geek
TLP:CLEAR	domaine C2	ksarpo[.]parody
TLP:CLEAR	domaine C2	rwziag[.]pirate
TLP:CLEAR	domaine C2	metbez[.]gopher
TLP:CLEAR	domaine C2	rmdtqq[.]libre
TLP:CLEAR	domaine C2	pektbo[.]libre
TLP:CLEAR	domaine C2	mqcgbs[.]gopher
TLP:CLEAR	domaine C2	cbdgzy[.]pirate
TLP:CLEAR	domaine C2	czbrwa[.]geek
TLP:CLEAR	domaine C2	edrnhe[.]oss
TLP:CLEAR	domaine C2	hfoddy[.]dyn
TLP:CLEAR	domaine C2	fawzpp[.]indy
TLP:CLEAR	domaine C2	hxqytk[.]geek
TLP:CLEAR	domaine C2	iaxtpa[.]parody
TLP:CLEAR	domaine C2	mfszki[.]gopher
TLP:CLEAR	domaine C2	qhedye[.]oss
TLP:CLEAR	domaine C2	wnisyi[.]libre
TLP:CLEAR	domaine C2	asdjjasdhioasdia[.]online
TLP:CLEAR	domaine C2	jiggaboojones[.]tech

2.3.8. Règles de détections

Règles Snort

Règle pour détecter des tentatives d'intrusion

```
alert tcp any any -> any any (msg:"QNAP VioStor - CVE-2023-47565 (InfectedSlurs exploitation attempt)";
flow:to_server,established; content:"POST"; http_method; content:"/cgi-bin/server/server.cgi";
content:"func="; content:"counter="; content:"APPLY="; http_uri; content:"time_mode="; content:"time_YEAR=";
content:"time_MONTH="; content:"time_DAY="; content:"time_HOUR="; content:"time_MINUTE=";
content:"time_SECOND"; content:"enable_rtc="; content:"TIMEZONE="; content:"year="; content:"month=";
content:"day="; content:"CONFIGURE_NTP="; content:"SPECIFIC_SERVER="; http_client_body; sid:1000002;)
```

Règle Snort utilisé pour détecter des communications vers l'infrastructure C2 d'InfectedSlurs

```
alert ip any any -> 45.95.147.226 any (msg:"InfectedSlurs C2 communications"; sid:1000001;)
alert ip any any -> 45.142.182.96 any (msg:"InfectedSlurs C2 communications"; sid:1000002;)
alert ip any any -> 5.181.80.53 any (msg:"InfectedSlurs C2 communications"; sid:1000003;)
alert ip any any -> 5.181.80.54 any (msg:"InfectedSlurs C2 communications"; sid:1000004;)
alert ip any any -> 5.181.80.55 any (msg:"InfectedSlurs C2 communications"; sid:1000005;)
alert ip any any -> 5.181.80.59 any (msg:"InfectedSlurs C2 communications"; sid:1000006;)
alert ip any any -> 5.181.80.81 any (msg:"InfectedSlurs C2 communications"; sid:1000007;)
alert ip any any -> 5.181.80.72 any (msg:"InfectedSlurs C2 communications"; sid:1000008;)
alert ip any any -> 5.181.80.77 any (msg:"InfectedSlurs C2 communications"; sid:1000009;)
alert ip any any -> 5.181.80.102 any (msg:"InfectedSlurs C2 communications"; sid:1000010;)
alert ip any any -> 5.181.80.126 any (msg:"InfectedSlurs C2 communications"; sid:1000011;)
alert ip any any -> 5.181.80.127 any (msg:"InfectedSlurs C2 communications"; sid:1000012;)
alert ip any any -> 91.92.254.4 any (msg:"InfectedSlurs C2 communications"; sid:1000013;)
alert ip any any -> 185.225.74.161 any (msg:"InfectedSlurs C2 communications"; sid:1000014;)
alert ip any any -> 185.150.26.226 any (msg:"InfectedSlurs C2 communications"; sid:1000015;)
alert ip any any -> 194.180.48.202 any (msg:"InfectedSlurs C2 communications"; sid:1000016;)
alert ip any any -> 85.217.144.207 any (msg:"InfectedSlurs C2 communications"; sid:1000017;)
alert ip any any -> 45.139.105.145 any (msg:"InfectedSlurs C2 communications"; sid:1000018;)
alert ip any any -> 162.220.166.114 any (msg:"InfectedSlurs C2 communications"; sid:1000019;)
alert ip any any -> 89.190.156.145 any (msg:"InfectedSlurs C2 communications"; sid:1000020;)
alert ip any any -> 162.246.20.236 any (msg:"InfectedSlurs C2 communications"; sid:1000021;)
alert ip any any -> 194.153.216.164 any (msg:"InfectedSlurs C2 communications"; sid:1000022;)
alert ip any any -> 95.214.27.10 any (msg:"InfectedSlurs C2 communications"; sid:1000023;)
alert ip any any -> 62.113.113.168 any (msg:"InfectedSlurs C2 communications"; sid:1000024;)
alert ip any any -> 194.38.21.42 any (msg:"InfectedSlurs C2 communications"; sid:1000025;)
```

Règles YARA

```
rule infected_slurs_scripts_1 {
   meta:
      description = "infected-slurs-scripts-1"
      author = "Akamai SIRT"
      date = "2023-11-20"
   strings:
      $s1 = "ftpget.sh ftpget.sh && sh ftpget.sh;curl http://" fullword ascii
      $s2 = "chinese family" fullword ascii
      $s3 =
"\\x23\\x21\\x2F\\x62\\x69\\x6E\\x2F\\x73\\x68\\x0A\\x0A\\x66\\x6F\\x72\\x20\\x70\\x72\\x6F\\x63\\x5F\\x64\\
x69\\x72\\x20\\x69\\x6E\\x20\\x2F\\x70\\x72\\x6F\\x63\" fullword ascii
      $s4 = "/bin/busybox hostname TBOT" fullword ascii
   condition:
      3 of them
}
```

```
rule infected_slurs_scripts_2 {
   meta:
      description = "infected-slurs-scripts-2"
      author = "Akamai SIRT"
      date = "2023-11-20"
   strings:
      $s1 = ";<=>?@ABCDEFGJIMOPQRSTUVWX[\\^_`abcxyz{|}~" fullword ascii
      $s2 = "#$%&'()*+,234567" fullword ascii
      $s3 = "BOOOOOOONS_" fullword ascii
      $s4 = "npxXoudifFeEgGaACScs" fullword ascii
   condition:
      3 of them
}
```

```
rule infected_slurs_bins {
   meta:
      description = "infected-slurs-bins"
      author = "Akamai SIRT"
      date = "2023-11-20"
   strings:
      $s1 = "attack_gre.c" fullword ascii
      $s2 = "attack_ongoing" fullword ascii
      $s3 = "ensure_single_instance" fullword ascii
      $s4 = "/home/landley/aboriginal/aboriginal/build/temp-armv7l/gcc-core/gcc/config/arm/pr-support.c"
fullword ascii
      $s5 = "words_left" fullword ascii
      $s6 = "kutil_strncmp" fullword ascii
      $s7 = "fflush_unlocked" fullword ascii
      $s8 = "methods_len" fullword ascii
   condition:
      6 of them
}
```

3. Rançongiciel : comprendre les méthodes d'extorsion

Cet article propose d'explorer les méthodes d'extorsion utilisées par les attaquants dans le contexte d'une cyberattaque par rançongiciel. Dans un souci de simplification, ces méthodes sont regroupées dans deux écosystèmes :

- **Écosystème d'extorsion élémentaire** : ce premier rassemble les méthodes les plus utilisées
- **Écosystème d'extorsion multiple** : ce second rassemble les méthodes supplémentaires

3.1. Écosystème d'extorsion élémentaire

Cet écosystème rassemble trois méthodes.

3.1.1. Pure

Dans le cas d'une extorsion pure, les données de la victime sont exfiltrées par les attaquants sans que celles-ci soient chiffrées. Cette méthode est appliquée dans des campagnes connues sous l'appellation : *attaques sans chiffrement* (*encryption-less ransomware* ou *encryption-less attacks*).

- Cette méthode a été observée chez plusieurs groupes d'attaquants, notamment : Babuk, SnapMC, Karakurt, Donut, RansomHouse, BianLian, Cl0p, et Lapsus$…

3.1.2. Simple

Cette méthode de simple extorsion consiste à chiffrer les données de la victime. Chiffrées, les données sont inutilisables et ne peuvent être déchiffrées qu'à l'aide d'une clé spécifique. Cette méthode peut être appliquée à l'encontre de tout un système ou de manière précise à l'encontre de quelques fichiers. Le chiffrement est réalisé via un logiciel malveillant, un rançongiciel, dont l'un des plus célèbres est nord-coréen : WannaCry.

- Cette méthode a été observée chez plusieurs groupes d'attaquants, notamment : KniveSpider (Ukrainien), UNIT 180 (nord-coréen), APT 38 (nord-coréen)…

3.1.3. Double

Les attaquants exfiltrent les données de la victime avant de les chiffrer. Devenue célèbre en 2019, la double extorsion a été obsérvée pour la première fois chez le collectif cybercriminel TA2101 à l'encontre de la société de sécurité privée *Allied Universal*. Les attaquants ont utilisé le rançongiciel Maze pour chiffrer les données et ont menacé de divulguer les données extorquées.

- Cette méthode a été observée chez plusieurs groupes d'attaquants, notamment : LockBit, Hive, Industrial Spy, Egregor, DarkSide, Avaddon, Ragnar Locker, REvil / Sodinokibi, DoppelPaymer / BitPaymer, Conti…

3.1.4. Synthèse infographique

Ci-dessous, une synthèse infographique. Cette modélisation rassemble les trois méthodes présentées préalablement.

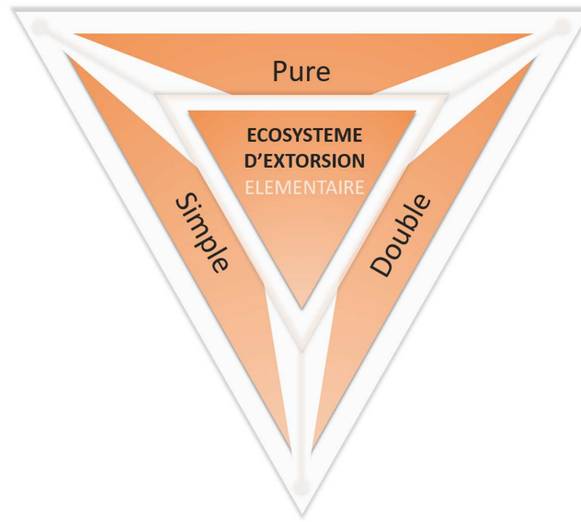

Figure 1. Synthèse infographique de l'écosystème d'extorsion élémentaire.

3.2. Écosystème d'extorsion multiple

Cet écosystème rassemble six méthodes.

3.2.1. L'incapacité opérationnelle

Cette méthode consiste à mener une attaque par déni de service distribué afin de rendre inopérationnels les services de l'organisation victime. Outre les dommages causés par le rançongiciel (le chiffrement des données), les victimes subissent également une perte de revenus due au temps d'arrêt provoqué par l'attaque DDoS. Cette méthode est souvent catégorisée en tant que triple ou quadruple extorsion.

- Cette méthode a été observée chez plusieurs groupes d'attaquants, notamment : LockBit, REvil, Avos Locker, Avaddon…

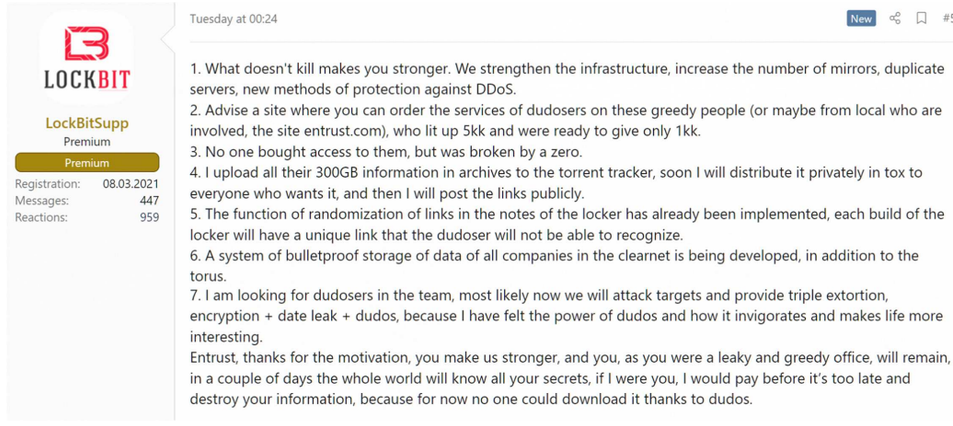

Figure 2. Le syndicat du cybercrime, LockBitSupp, annonce en août 2022 le recours à l'attaque DDoS (voir puce n°7).

3.2.2. La coercition externalisée

Souvent considérée comme étant la quadruple extorsion, cette méthode consiste à inciter au paiement de la rançon en menaçant directement les victimes collatérales. Les clients, les patients ou les partenaires commerciaux de l'organisation victime sont directement contactés par les attaquants. Le contact peut être réalisé via des appels téléphoniques, des courriers, des courriels, et des SMS. Les attaquants menacent de publier les données extorquées et incitent la victime collatérale à payer une micro-rançon. Les attaquants peuvent aussi inciter les victimes collatérales à faire pression sur l'organisation pour payer la rançon dans sa totalité. En 2020, *Vastaamo*, fournisseur de services de psychothérapie privé finlandais, a été victime d'une attaque par rançongiciel.

Le 21 octobre, *Vastaamo* annonce que les données de 36 000 patients ont été extorquées. Le 24 octobre, plusieurs patients ont été contactés par les attaquants pour réaliser des paiements de micro-rançons.

- Cette méthode a été observée chez plusieurs groupes d'attaquants, notamment : REvil, SunCrypt…

Figure 3. VX Underground publie sur la plateforme YouTube un enregistrement audio du collectif cybercriminel SunCrypt dans lequel les attaquants font pression sur une victime pour que l'organisation paie la rançon.

3.2.3. Vilipender via la vitrine

Rare, cette méthode consiste à modifier le site vitrine de l'organisation ciblée de manière à signaler aux visiteurs que celle-ci est victime d'une cyberattaque. La modification peut, par exemple, être un ajout de texte ou d'une image. Cette méthode peut être utilisée par les attaquants lorsque l'organisation ciblée tente de rester discrète afin de ne pas révéler l'incident causé par la cyberattaque. Au cours de l'année 2022, le collectif cybercriminel Industrial Spy à modifié l'index du site d'une organisation en précisant la quantité de données extorquée et une adresse pour communiquer avec les attaquants.

- Cette méthode a été observée chez plusieurs groupes d'attaquants, notamment : Industrial Spy, L4NC34 Ransomware…

Figure 4. Modification d'un site web par le collectif L4NC34 Ransomware.

3.2.4. La dénonciation aux autorités

Récente, cette méthode a fait son apparition au cours du mois de novembre 2023. Celle-ci a pour finalité de faire pression sur l'organisation victime en signalant la cyberattaque aux autorités. En Amérique, la SEC (*Securities and Exchange Commission* : l'organisme fédéral américain de réglementation et de contrôle des marchés financiers) impose aux organisations un délai de notification d'un incident de cybersécurité et donne la posibilité aux particuliers de signaler toute *infraction* constatée. Le non-respect de cette déclaration expose l'organisation victime à une amende. En novembre 2023, le collectif cybercriminel opérant le rançongiciel AlphV / BlackCat à déposé à la SEC une plainte à l'encontre de sa victime : MeridianLink.

- Cette méthode n'a été observée que chez un groupe d'attaquant : AlphV / BlackCat.

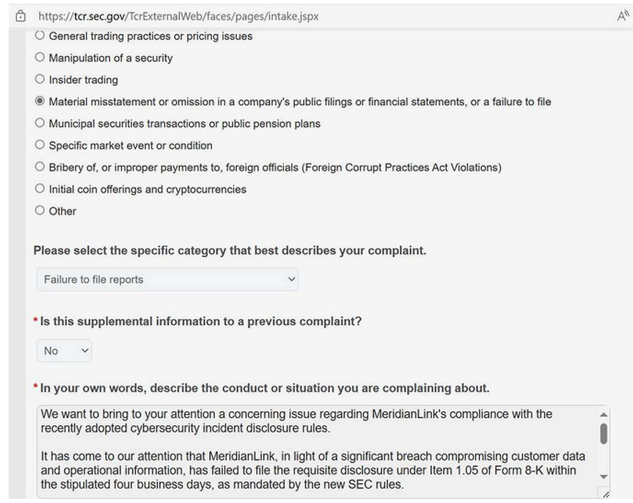

Figure 5. Capture d'écran de la plainte déposée par AlphV / BlackCat à l'encontre de sa victime.

3.2.5. L'atteinte à la réputation

Les attaquants annoncent la cyberattaque aux médias et/ou sur les réseaux sociaux. Industrial Spy a régulièrement publié sur Twitter (*X*) la liste de ses victimes en incluant aussi des captures d'écrans et les logos des enseignes ciblées. Ragnar Locker a diffusé des publicités sur le réseau social *Facebook* pour faire pression sur *Campari* (organisation italienne spécialisée dans l'alcool et spiritueux).

- Cette méthode a été observée chez plusieurs groupes d'attaquants, notamment : Industrial Spy, Ragnar Locker, Bl00dy…

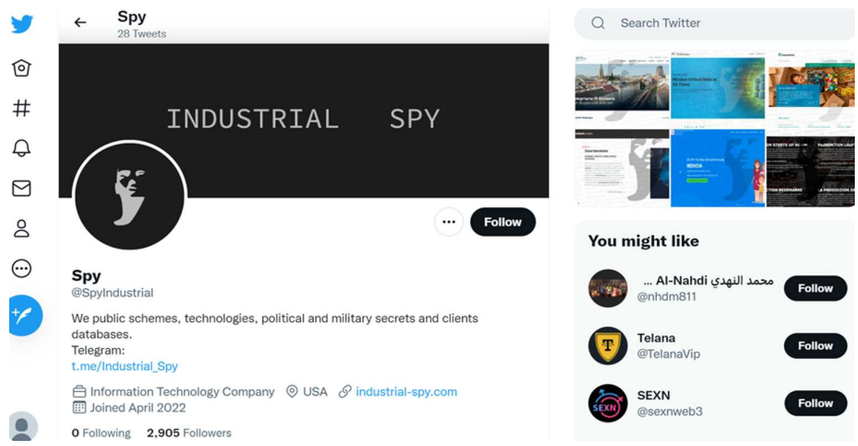

Figure 6. Capture d'écran de l'ancienne page Twiter (X) d'Industrial Spy pour annoncer publiquement leurs victimes.

3.2.6. Menace de mort

Très rare, cette méthode consiste à menacer de mort la vie des familles de l'organisation victime. En septembre 2022, le groupe Bl00dy annonce publiquement sur Telegram des menaces de mort à l'encontre de ceux qui refusent le paiement de la rançon. Les victimes seront "chassées par des assassins".

- Cette méthode n'a été observée que chez un groupe d'attaquant : Bl00dy.

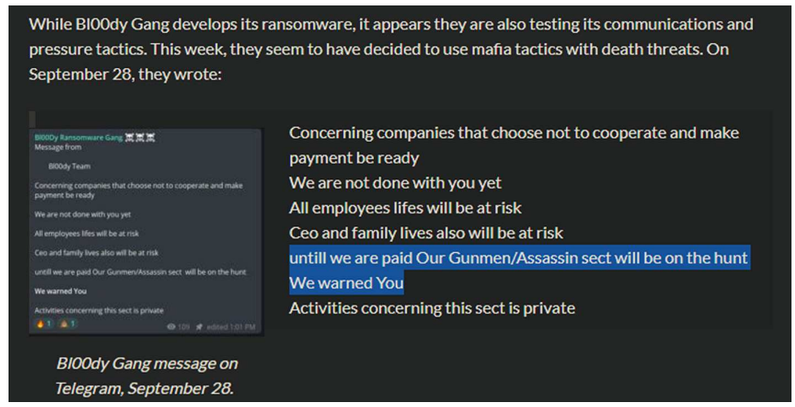

Figure 7. Capture d'écran du site databreach.

3.2.7. Synthèse infographique

Ci-dessous, une synthèse infographique. Cette modélisation rassemble six méthodes présentées préalablement.

Figure 8. Synthèse infographique de l'écosystème d'extorsion multiple.

3.3. Absence de consensus

Il n'existe aucun consensus permettant de catégoriser à l'unisson toutes les méthodes supplémentaires. Ces dernières sont parfois catégorisées en tant que triple extorsion, quadruples extorsions, ou plus.

3.3.1. Exemple 1

Ci-dessous, la société *CloudFlare* ne semble pas considérer l'attaque DDoS comme triple extorsion, mais comme 7e méthode de pression.

7. Adjonction d'une attaque DDoS

Alors que l'entreprise visée croule déjà sous les nombreuses tâches à accomplir (contacter les autorités et les clients, localiser les fichiers de sauvegarde et minimiser les mouvements latéraux), certains acteurs malveillants peuvent également la menacer d'une attaque par déni de service distribué, voire tout bonnement en lancer une. L'engorgement d'un réseau pendant une période mouvementée ajoute du stress et mobilise de nouvelles ressources informatiques.

Figure 9. Extrait de l'article "Les auteurs d'attaques par rançongiciel accentuent leurs tactiques d'extorsion" de CloudFlare.

3.3.2. Exemple 2

Ci-dessous, un modèle de l'écosystème réalisé par *Recorded Future*.

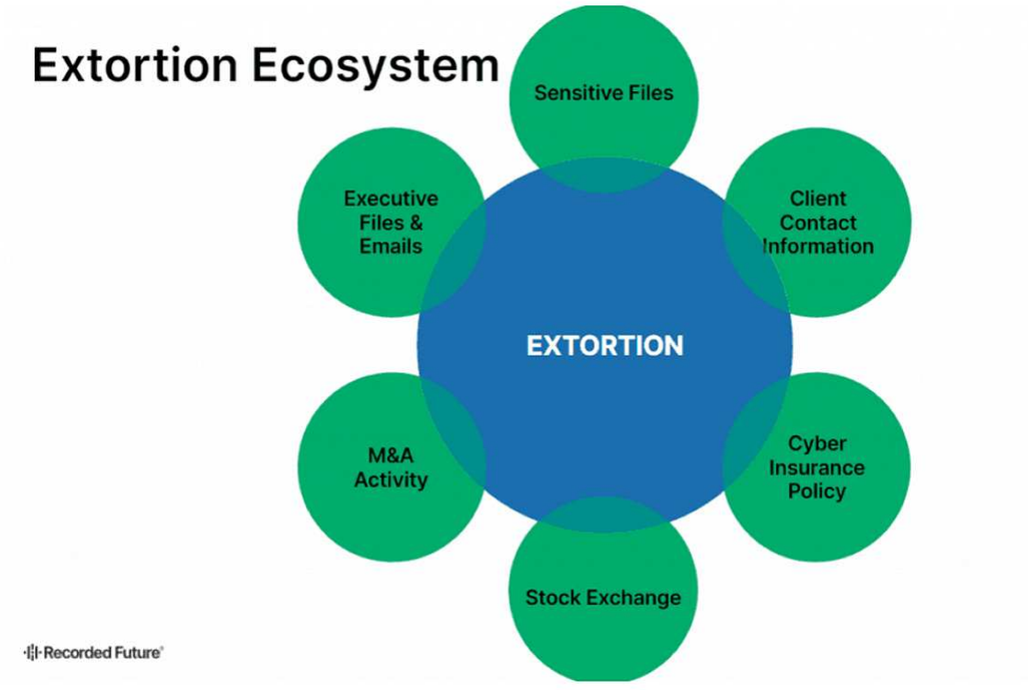

Figure 10. Extrait de l'article "Ransomware gang wants to short the stock price of their victims" de Recorded Future.

3.3.3. Exemple 3

Ci-dessous, la société *PaloAlto* semble considérer l'attaque DDoS comme triple extorsion.

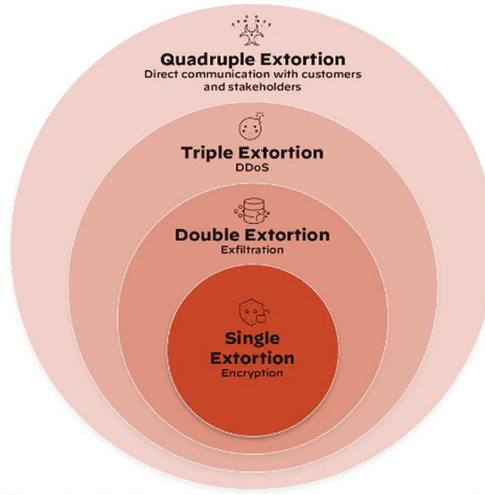

Figure 11. Extrait de l'article "What is Multi-Extortion Ransomware?" de PaloAlto.

3.3.4. Simplification

Pour des raisons de simplicité, le mot composé **extorsion-multiple** est souvent utilisé afin de rassembler toutes ces méthodes supplémentaires.

3.4. Réflexion cyber-psychologique

3.4.1. Une double guerre

Une cyberattaque par rançongiciel constitue une véritable guerre technique en soi : l'utilisation de logiciels malveillants, les technologies de chiffrement, l'infrastructure de l'attaquant…

Cependant, en parallèle de cette guerre technique il y a une autre guerre qui se caractérise par sa subtilité et ses conséquences parfois invisibles. Il s'agit de la guerre psychologique, dont le but ultime de l'attaquant et de réaliser chez sa victime un consentement fabriqué.

Ci-dessous, une infographie qui représente l'écosystème d'extorsion au coeur des deux guerres.

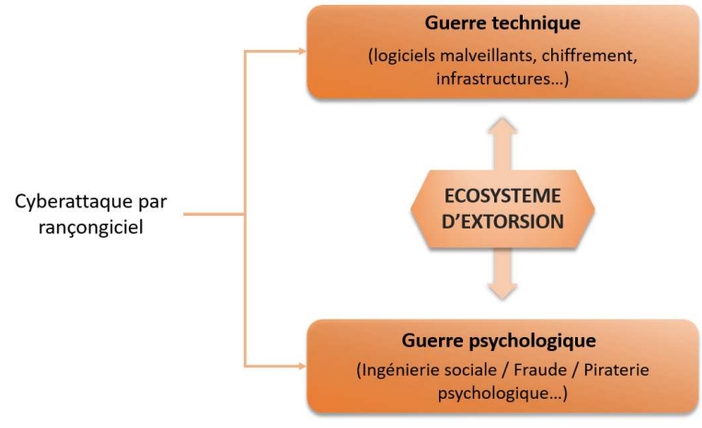

Figure 12. infographie cyber-psychologie : la double inhérence de l'écosystème d'extorsion. La guerre économique n'est pas présentée pour des raisons de simplification.

3.4.2. Une échine complexe

L'échine de l'écosystème d'extorsion est partiellement structurée de divers outils de manipulation mentale. Les outils régulièrement observés chez les collectifs cybercriminels sont le mensonge, l'intimidation, l'isolement et la soumission.

La finalité malveillante, en matière de guerre psychologique, est d'obtenir un consentement fabriqué.

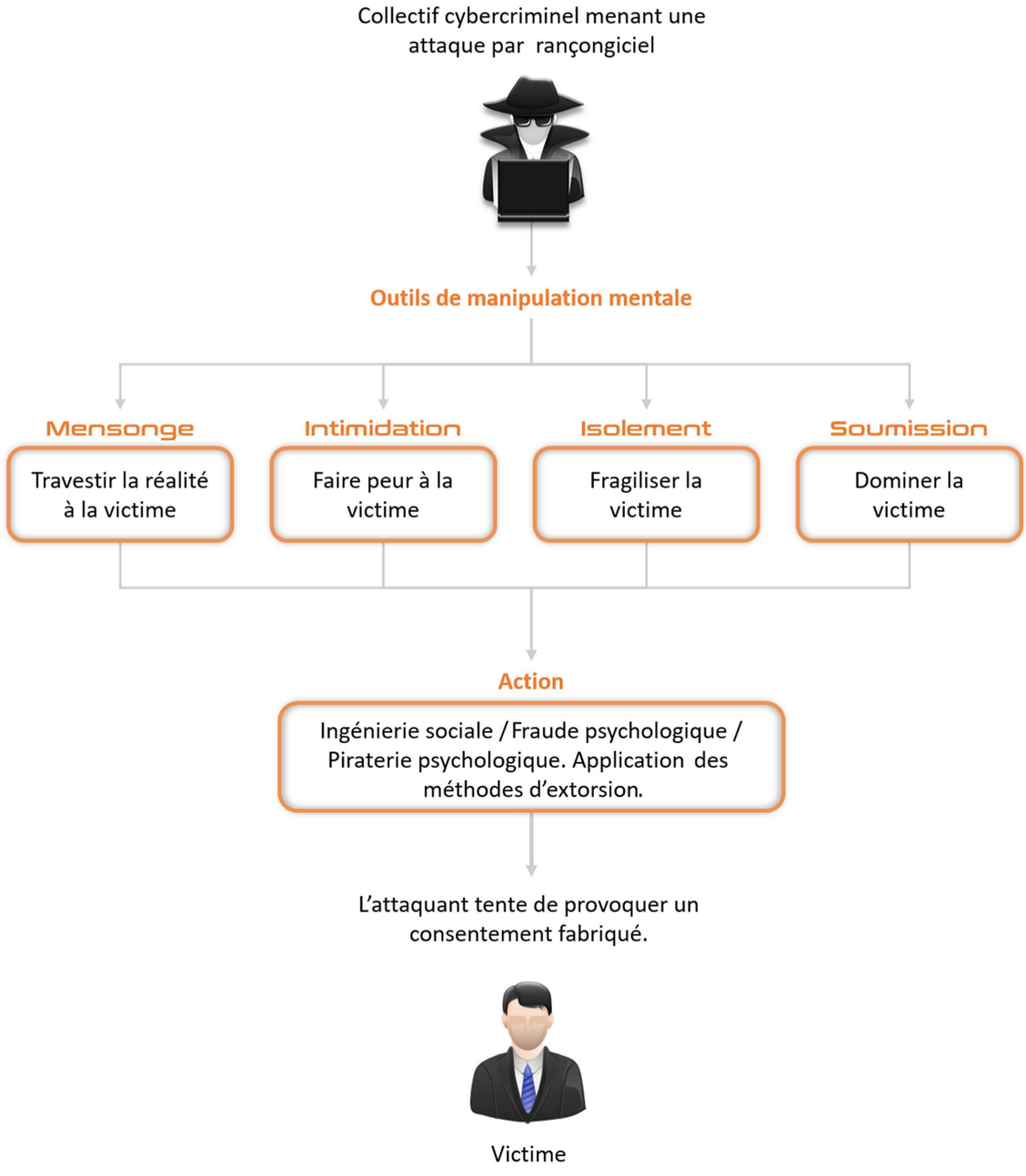

Figure 13. Infographie cyber-psychologie (non exhaustif) : les outils de manipulation mentale constituent partiellement l'échine de l'écosystème d'extorsion.

4. Applications OAuth : Utilisation abusive par les groupes cybercriminels

Le 12 décembre 2023, *Microsoft* alerte sur l'utilisation abusive des applications **OAuth** (Open Authorization) pour automatiser des attaques, dont la motivation est le gain financier. Jusqu'à aujourd'hui, différents types d'utilisation malveillante de ce protocole ont été recensés, allant du phishing au déploiement de machines virtuelles à des fins de cryptomining.

4.1. Historique d'OAuth

OAuth est un protocole qui autorise une application à interagir avec une autre sans transmettre de mots de passe. Ce protocole utilise des jetons d'autorisation pour prouver l'identité des consommateurs et des fournisseurs de services.

Il a été introduit avec *Twitter* en 2007 pour permettre à des applications tierces d'accéder à l'API du réseau social sans avoir besoin d'identifiants. En 2010, c'est au tour de *Google* de proposer ce service à des éditeurs d'applications. De nombreuses grandes entreprises comme *Amazon*, *Netflix*, *PayPal*, *Microsoft*, *LinkedIn* ou *Facebook* offrent aujourd'hui l'intégration de ce protocole.

L'emploi d'**OAuth** semblerait être une garantie de sécurité pour les mots de passe. Toutefois, les groupes d'attaquants continuent de faire évoluer leurs techniques et de s'adapter aux mesures de sécurité. C'est pourquoi, dès 2011, le *SANS* alertait sur la possible utilisation malveillante de ce protocole et comment s'en prémunir.

4.2. L'utilisation d'applications OAuth pour déployer des machines virtuelles pour le cryptomining

Des attaquants ont ciblé des comptes utilisateurs Microsoft grâce à des techniques de *phishing* ou de *pulvérisation de mots passe*. Cette première phase d'accès initial n'était toutefois pas la finalité des attaquants, l'objectif étant par la suite de créer ou modifier des applications **OAuth** pour des actions de plus grande envergure.

Après avoir compromis un premier compte utilisateur Microsoft, le groupe Storm-1283 a modifié une application **OAuth** existante en affectant tous les droits nécessaires pour déployer des machines virtuelles. Celles-ci leur ont, par la suite, permis de miner de la cryptomonnaie. Les attaquants ont réitéré le mode opératoire pour déployer d'autres machines virtuelles à l'aide d'une nouvelle application **OAuth**.

Ces attaques ont engendré des frais aux organisations ciblées allant de **10 000 à 1,5 million de dollars US**, en fonction de l'envergure et de la durée de l'attaque.

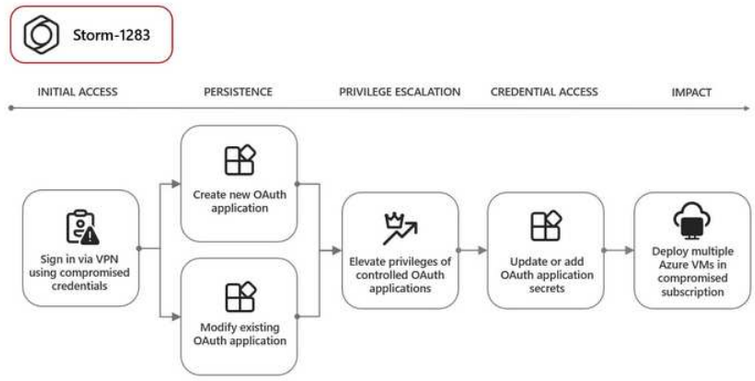

Figure 14. Chaine d'attaque des campagnes de cryptomining - Source : Microsoft.

4.3. L'utilisation d'applications OAuth à des fins de phishing et de compromission d'email

Dans leur rapport, les chercheurs en sécurité de *Microsoft* soulignent l'utilisation d'applications **OAuth** compromises à des fins de campagnes de *phishing*.

Comme dans la campagne précédente, un attaquant a compromis un compte utilisateur Microsoft comme accès initial. Cette fois, l'objectif du cybercriminel n'était pas d'effectuer des opérations de *minage* mais de réaliser des attaques de phishing pour récupérer des tokens **OAuth**.

Le cybercriminel a envoyé, depuis le compte email compris un kit d'hameçonnage à plusieurs cibles de différentes organisations. Ce courrier de phishing contenait une URL qui a redirigé les victimes vers une page d'ouverture de session *Microsoft*. En cliquant sur ce lien, les jetons de cookies de sessions des utilisateurs sont alors récupérés par l'attaquant.

Dans certains cas, l'attaquant a exploité le compte utilisateur compromis pour effectuer des recherches d'informations financières dans les boites aux lettres. Ces informations vont par la suite être utilisées dans des campagnes d'ingénierie sociale plus ciblées.

4.4. L'utilisation d'applications OAuth pour les activités de spamming

Dans son rapport, *Micosoft* met en avant une troisième campagne liée à une utilisation illégitime des applications **OAuth**, attribuée au groupe Storm-1286.

Après une compromission d'un compte ne disposant pas d'authentification multifacteur, les cybercriminels ont ajouter des droits spécifiques aux applications **OAuth** : *email*, *profile*, *openid*, *Mail.Send*, *User.Read* et *Mail.Read*.

Ces permissions ont permis à Storm-1286 de contrôler le compte de messagerie compromis et d'envoyer des milliers de courriels par jour. L'utilisation d'un domaine légitime pour ce type de campagne permet d'éviter les dispositifs de sécurité en charge de la détection de courriels de phishing et de spam.

Dans certains cas, Storm-1286 a attendu plusieurs mois après l'accès initial et la configuration des applications **OAuth** avant de commencer l'activité de spam à l'aide de ces applications.

Les chercheurs en sécurité de *Microsoft* ne sont pas les seuls à observer l'utilisation malveillante de **OAuth**, lors d'attaques. En effet, dès janvier 2023, *Proofpoint* a constaté des campagnes ayant recours à cette utilisation abusive.

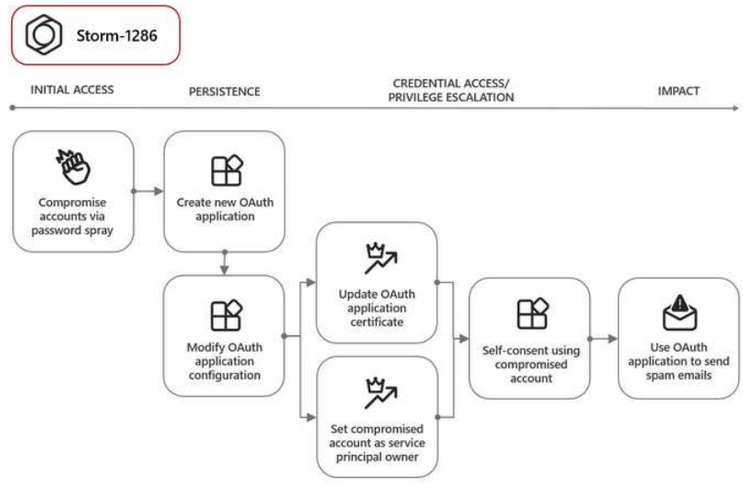

Figure 15. Chaine d'attaque des campagnes de spamming - Source : Microsoft.

4.5. L'utilisation d'applications OAuth malveillantes

En janvier 2023, les chercheurs de *Proofpoint* ont découvert une nouvelle campagne OiVaVoii impliquant des applications **OAuth**. Cette campagne a ciblé des directeurs généraux d' entreprises avec du spear-phishing et des leurres personnalisés.

Les attaquants ont créé des applications **OAuth** satisfaisant les exigences de *Microsoft* pour avoir le statut d'*éditeur vérifié* et donc inspirer confiance aux utilisateurs de cette application. Ils ont alors utilisé un compte Office 365 compromis **OAuth** pour envoyer des emails de phishing en demandant aux utilisateurs d'accorder des droits sur ces applications **OAuth** malveillantes.

Les cybercriminels ont alors pu exfiltrer des données, avoir accès à des messageries ou encore utilisé de façon malveillante des domaines légitimes.

Le statut d'*éditeur vérifié* d'une application **OAuth** ne garantit donc pas la légitimité de celle-ci et la vigilance de chaque utilisateur reste de mise.

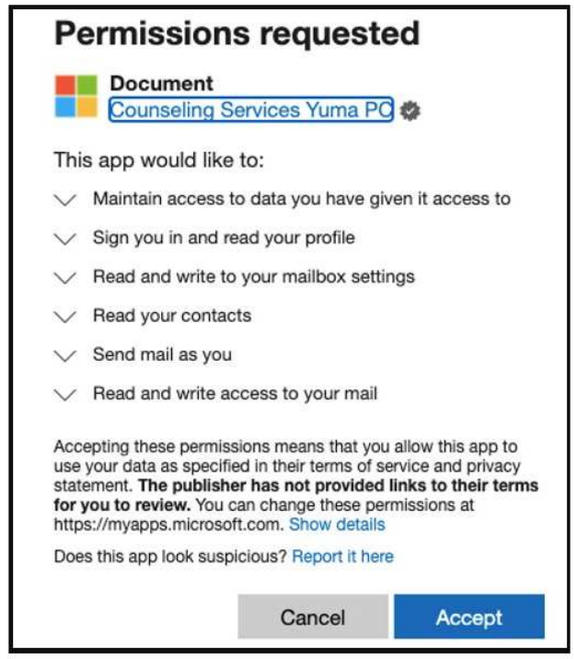

Figure 16. Application **OAuth** *utilisant le logo Microsoft et un éditeur vérifié - Source : ProofPoint.*

4.6. Matrice Mitre ATT&CK

INITIAL ACCESS

T1078 Valid Account. T1566 Phishing.

PERSISTENCE

T1098 Account Manipulation.

PRIVILEGE ESCALATION

T1548 Abuse Elevation Control Mechanism. T1134 Access Token Manipulation. T1528 Steal Application Access Token.

CREDENTIAL ACCESS

T1557 Adversary-in-the-Middle. T1110 Brute Force. T1528 Steal Application Access Token.

IMPACT

T1496 Resource Hijacking. T1657 Financial Theft.

4.7. Recommandations

Les recommandations pour atténuer les risques associés à ce mode opératoire sont :

- Mettre en place l'authentification multifacteur (MFA)
- Empêcher les e-mails malveillants d'atteindre les utilisateurs. Pour ce faire, les serveurs de messageries proposent des fonctionnalités de sécurités qui peuvent être activées et aider à la détection des mails de spam ou de phishing.
- Vérifier toutes les applications et les autorisations consenties pour s'assurer que les applications n'accèdent qu'aux données nécessaires et qu'elles respectent les principes de l'accès au moindre privilège.

4.8. Pistes de détection Microsoft 365 Defender

Il est possible de s'assurer de l'absence de compromission par l'analyse des journaux d'activité grâce aux règles suivantes :

Détection de tentatives de connexion suspectes

```
IdentityLogonEvents
| where Timestamp > ago(3d)
| where ActionType == "LogonFailed" and LogonType == "OAuth2:Token" and Application == "Microsoft Exchange
Online"
| summarize count(), dcount(IPAddress), dcount(CountryCode) by AccountObjectId, AccountDisplayName,
bin(Timestamp, 1h)
```

Détection de création d'applications OAuth

```
CloudAppEvents
| where ActionType in ("Add application.", "Add service principal.")
| mvexpand modifiedProperties = RawEventData.ModifiedProperties
| where modifiedProperties.Name == "AppAddress"
| extend AppAddress = tolower(extract('\"Address\": \"(.*)\",',1,tostring(modifiedProperties.NewValue)))
| mvexpand ExtendedProperties = RawEventData.ExtendedProperties
| where ExtendedProperties.Name == "additionalDetails"
| extend OAuthApplicationId = tolower(extract('\"AppId\":\"(.*)\"',1,tostring(ExtendedProperties.Value)))
| project Timestamp, ReportId, AccountObjectId, Application, ApplicationId, OAuthApplicationId, AppAddress
```

5. Références

Vulnérabilités

- https://nvd.nist.gov/vuln/detail/CVE-2023-49070
- https://lists.apache.org/thread/jmbqk2lp4t4483whzndp5xqlq4f3otg3
- https://nvd.nist.gov/vuln/detail/CVE-2023-6448
- https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf
- https://downloads.unitronicsplc.com/Sites/plc/Visilogic/Version_Changes-Bug_Reports/VisiLogic%209.9.00%20Version%20changes.pdf
- https://nvd.nist.gov/vuln/detail/CVE-2023-47565
- https://www.cisa.gov/news-events/ics-advisories/icsa-23-355-02
- https://www.qnap.com/en/security-advisory/qsa-23-48
- https://www.akamai.com/blog/security-research/qnap-viostor-zero-day-vulnerability-spreading-mirai-patched
- https://www.akamai.com/blog/security-research/new-rce-botnet-spreads-mirai-via-zero-days

Rançongiciel : comprendre les méthodes d'extorsion

- https://www.cloudflare.com/fr-fr/the-net/ransomware-extortion/
- https://fr.wikipedia.org/wiki/Ran%C3%A7ongiciel_en_tant_que_service
- https://www.01net.com/actualites/ransomware-les-pirates-de-blackcat-testent-un-nouveau-moyen-de-pression.html
- https://www.silicon.fr/ransomwares-triple-extorsion-408946.html
- https://en.wikipedia.org/wiki/Vastaamo_data_breach
- https://www.youtube.com/watch?v=htsSaPNgm8s
- https://blog.sucuri.net/2020/04/analyzing-decrypting-l4nc34s-simple-ransomware.html
- https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/
- https://www.01net.com/actualites/ransomware-les-pirates-de-blackcat-testent-un-nouveau-moyen-de-pression.html
- https://www.malwarebytes.com/blog/news/2023/11/ransomware-gang-files-sec-complaint-about-target
- https://www.it-connect.fr/le-gang-de-ransomware-blackcat-denonce-sa-victime-aux-autorites-pour-lui-mettre-la-pression/
- https://www.lemondeinformatique.fr/actualites/lire-le-ransomware-ragnar-locker-s-offre-des-pubs-sur-facebook-81003.html
- https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims
- https://www.databreaches.net/leaked-lockbit-3-0-builder-used-by-bl00dy-ransomware-gang-in-attacks/
- https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware

Application OAuth : Utilisation abusive par les groupes cybercriminels

- https://www.proofpoint.com/fr/threat-reference/OAuth
- https://www.proofpoint.com/us/blog/cloud-security/dangerous-consequences-threat-actors-abusing-microsofts-verified-publisher
- https://www.microsoft.com/en-us/security/blog/2023/12/12/threat-actors-misuse-oauth-applications-to-automate-financially-driven-attacks/
- https://www.sans.org/blog/four-attacks-on-oauth-how-to-secure-your-oauth-implementation/