TLP:WHITE

CAMPAGNES D'HAMEÇONNAGE DU MODE OPÉRATOIRE D'ATTAQUANTS NOBELIUM

Version 1.1

06 décembre 2021

TLP:WHITE

Sommaire

Résumé

L'ANSSI a observé plusieurs campagnes d'hameçonnage contre des entités françaises depuis février 2021. Le mode opératoire d'attaquants (MOA) employé au cours de ces activités malveillantes a permis de compromettre des comptes de messagerie d'organisations françaises, et d'envoyer à partir de ces comptes des courriels piégés à des institutions étrangères. Par ailleurs, des organisations publiques françaises ont également été destinataires de messages piégés provenant d'institutions étrangères supposément compromises.

Les marqueurs techniques observés par l'ANSSI correspondent aux activités associées au mode opératoire *Nobelium*. Ce MOA aurait été employé en parallèle durant d'autres campagnes d'attaques dirigées contre des entités diplomatiques et des organisations internationales en Europe et en Amérique du Nord. Des recoupements de tactiques, techniques & procédures (TTP) entre les campagnes d'hameçonnage suivies par l'ANSSI et l'attaque par chaîne d'approvisionnement *via* SolarWinds de 2020 ont également été établis.

Ce rapport détaille les informations techniques liées aux campagnes d'hameçonnage, en présentant la nature des activités malveillantes observées (section 1), les tactiques, techniques & procédures (section 2), et l'infrastructure (section 3) des attaquants. Les similarités constatées avec des modes opératoires documentés en source ouverte sont décrites à la section 4. Des recommandations (section 5) et indicateurs de compromission (annexe A) sont disponibles à la fin du document afin de permettre une meilleure protection contre ce type d'attaque et faciliter la recherche d'une éventuelle compromission.

1. Contexte

Depuis février 2021, l'ANSSI a traité une série de campagnes d'hameçonnage dirigée contre des entités françaises, qui se sont intensifiées durant le mois de mai 2021. Ces activités malveillantes sont le fait d'un même mode opératoire d'attaquants (MOA).

Le MOA a notamment permis de compromettre des comptes de messagerie d'organisations françaises, puis s'est servi de ces accès pour envoyer des courriels piégés à des institutions étrangères du secteur de la diplomatie. La méthode d'intrusion initiale demeure inconnue.

Des organisations publiques françaises ont par ailleurs été destinataires de messages piégés. Ces messages provenaient d'institutions étrangères apparemment compromises par le même MOA.

N.B. : un groupe d'attaquants est un ensemble délimité, constitué d'individus identifiés ou identifiables revendiquant une appartenance à une organisation. Un groupe d'attaquants met en œuvre un ou plusieurs modes opératoires. Un mode opératoire d'attaquants est défini comme l'ensemble des outils, tactiques, techniques, procédures et caractéristiques mis en œuvre par un ou plusieurs groupes d'attaquants dans le cadre d'une ou plusieurs attaques informatiques.

2. Tactiques, techniques & procédures

Catégorie	Technique ID	Nom de la technique	Commentaire
Resource development	T1584.001	Compromise Infrastructure : Domains	Le MOA utilise des domaines compromis pour héberger des informations de *fingerprinting* récupérées par **VaporRage** [1].
	T1586.002	Compromise Accounts : Email Accounts	Le MOA compromet des comptes de messagerie pour envoyer ses courriels d'hameçonnage.
	T1583.001	Acquire Infrastructure : Domains	Le MOA utilise principalement les registraires NameCheap et NameSilo pour constituer son infrastructure C2.
	T1583.003	Acquire Infrastructure : Virtual Private Server	L'infrastructure C2 est constituée de *virtual private servers* de plusieurs fournisseurs.
Reconnaissance	T1590.005	Gather Victim Network Information : IP Addresses	Le code malveillant **EnvyScout** collecte des informations sur la victime et les exfiltre vers un serveur contrôlé par l'attaquant [1].
	1589.001	Gather Victim Identity Information : Credentials	Le code **EnvyScout** tente de se connecter en SMB à un serveur contrôlé par l'attaquant, exfiltrant potentiellement des identifiants NTLM [1].
Initial Access	T1199	Trusted Relationship	Les courriels d'hameçonnage sont envoyés depuis des adresses compromises d'entités de confiance. Le mode opératoire usurpe l'identité de l'entité correspondant à l'adresse courriel compromise.
	T1566.001	Phishing : Spearphishing Attachment	Dans le courriel d'hameçonnage du MOA se trouve une pièce-jointe HTML malveillante, nommée **EnvyScout** [1].
	T1566.002	Phishing : Spearphishing Link	Le MOA a hébergé un code malveillant sur la plateforme Google Drive. Un des courriels d'hameçonnage envoyés par le mode opératoire contenait un lien pour télécharger ce code malveillant.
	T1566.003	Phishing : Spearphishing via Service	Le MOA a utilisé le service de marketing en ligne Constant Contact pour distribuer des courriels d'hameçonnage à plusieurs centaines de destinataires.
Execution	T1204.001	User Execution : Malicious Link	Un courriel d'hameçonnage du MOA contenait un lien Google Drive, que l'utilisateur devait cliquer pour télécharger le code malveillant [2].
	T1204.002	User Execution : Malicious File	Pour exécuter la charge Cobalt Strike, la victime doit ouvrir la pièce jointe HTML du courriel d'hameçonnage.
	T1059.003	Command and Scripting Interpreter : Windows Command Shell	Le mode opératoire a effectué des actions de reconnaissance *via* des commandes Windows.
Defense Evasion	T1036.005	Masquerading : Match Legitimate Name or Location	Le MOA a renommé l'exécutable d'ADFind pour le faire passer pour un exécutable légitime. Cette technique a déjà été observée par Microsoft dans le cadre de l'attaque par chaîne d'approvisionnement de SolarWinds [3].
	T1070.004	Indicator Removal on Host : File Deletion	Une fois les résultats récupérés, l'attaquant a supprimé les outils utilisés pour faire de la reconnaissance (BloodHound et ADFind) et les fichiers de sortie de ses outils.
Discovery	T1087.002	Account Discovery : Domain Account	Le MOA recueille des informations sur le domaine *via* des commandes Windows, **BoomBox** [1], ADFind, et BloodHound.
	T1482	Domain Trust Discovery	Le MOA utilise des outils comme ADFind ou nltest pour récupérer des informations sur les Domain Trusts.
Exfiltration	T1567.002	Exfiltration Over Web Service : Exfiltration to Cloud Storage	Le code malveillant **BoomBox** exfiltre les informations recueillies *via* DropBox [1].
	T1041	Exfiltration Over C2 Channel	Utilisation du canal C2 HTTP de Cobalt Strike.

Table 2.1. – Liste des TTP selon le référentiel MITRE ATT&CK

3. Infrastructure de contrôle et de commande

La charge finale déposée par le mode opératoire est un implant Cobalt Strike. Il est configuré pour contacter ses serveurs de commande et de contrôle (C2) en HTTPs sur le port 443.

Les noms de domaine et adresses IP correspondant à l'infrastructure C2 sont disponibles en annexe A.

3.1. Serveurs du mode opératoire

L'infrastructure C2 du mode opératoire est constituée de *virtual private servers* (VPS), situés chez différents hébergeurs. Le mode opératoire semble privilégier des serveurs proches des pays ciblés. Plus particulièrement, plusieurs adresses IP de l'infrastructure C2 appartiennent à OVH.

La répartition est la suivante :

Numéro d'AS	Nom d'AS	Occurrences
AS16276	OVH SAS	7
AS25369	Hydra Communications Ltd	2
AS9009	M247 Ltd	2
AS20207	Gigared S.A.	1
AS31400	Accelerated IT Services Consulting GmbH	1
AS201206	Droptop GmbH	1
AS202448	MVPS LTD	1
AS269070	Hostzone Tecnologia LTDA	1
AS207560	Zubritska Valeriia Nikolaevna	1
AS43641	SOLLUTIUM	1
AS62282	UAB Rakrejus	1
AS197226	sprint S.A.	1
AS204641	HOSTGW SRL	1
AS51852	Private Layer INC	1
AS49981	WorldStream B.V.	1

TABLE 3.1. – Répartition des AS utilisés par le mode opératoire

3.2. Noms de domaine

Les noms de domaine utilisés par le MOA comme C2 Cobalt Strike ressemblent à des noms de domaine légitimes. Plusieurs noms de domaine enregistrés par le mode opératoire imitent des sites d'information et d'actualités. Le MOA enregistre majoritairement ses noms de domaines chez NAMESILO et NAMECHEAP.

3.3. Profils Cobalt Strike

Les échantillons Cobalt Strike utilisés par l'attaquant sont configurés pour contacter des URL spécifiques sur les serveurs de contrôle. Parmi les URI utilisées, on retrouve : « `/jquery-3.3.1.min.js` » et « `/jquery-3.3.2.min.js` ».

Ces deux URI correspondent à des profils Malleable Cobalt Strike disponibles en source ouverte [1], bien que certaines modifications aient été effectuées.

1. https://github.com/threatexpress/malleable-c2.

4. Liens avec des modes opératoires documentés en source ouverte

Les marqueurs techniques observés par l'ANSSI dans les sections 2 & 3 correspondent aux activités associées au MOA *Nobelium* décrites notamment par les équipes de recherche en cybersécurité de Microsoft [4, 1, 5], Volexity [6], Sentinel Labs [7], IstroSec [8] et ESET [9].

D'après Microsoft, *Nobelium* était toujours actif en octobre 2021. Le MOA aurait été utilisé au cours d'autres campagnes d'attaques visant notamment, depuis avril 2021, des serveurs *Active Directory Federation Services* afin de compromettre des entités gouvernementales, des *think tanks* et des entreprises privées aux États-Unis et en Europe [10, 11].

En outre, les campagnes d'hameçonnage décrites dans ce document présentent des TTP analogues [T1036.005, T1087.002 & T1482] à celles employées durant l'attaque par chaîne d'approvisionnement *via* SolarWinds révélée en décembre 2020 [3].

5. Recommandations

5.1. Limiter l'exécution des pièces jointes

Au vu de la chaîne de compromission détaillée plus haut, qui s'appuie sur l'ouverture d'une pièce jointe malveillante lors des campagnes d'hameçonnage, il est recommandé de ne pas exécuter de fichiers douteux.

5.2. Renforcer la sécurité de l'Active Directory

Le mode opératoire s'intéresse particulièrement aux serveurs d'*Active Directory* (AD). Il convient de leur appliquer des mesures de sécurité renforcée. L'ANSSI a produit un guide de recommandations sur ce sujet disponible sur le site du CERT-FR [12].

A. Annexe : Indicateurs de compromission

Domaine	Registraire	Adresse IP	Numéro d'AS	Nom d'AS	Première observation	Dernière observation
hanproud.com	NameSilo	45.179.89.37	AS269070	Hostzone Tecnologia LTDA	2020-10-01	2020-12-01
cbdnewsandreviews.net	NameSilo	139.99.167.177	AS16276	OVH SAS	2021-02-15	2021-05-01
cityloss.com	NameCheap	51.38.85.225	AS16276	OVH SAS	2021-02-15	2021-06-25
businesssalaries.com	NameCheap	190.183.61.30	AS20207	Gigared S.A.	2021-03-01	2021-05-10
trendignews.com	NameCheap	185.243.215.198	AS202448	MVPS LTD	2021-03-01	2021-04-01
worldhomeoutlet.com	NameCheap	192.99.221.77	AS16276	OVH SAS	2021-03-01	2021-09-01
giftbox4u.com	NameCheap	37.120.247.135	AS9009	M247 Ltd	2021-03-01	2021-04-25
myexpertforum.com	NameCheap	45.80.148.166	AS204641	HOSTGW SRL	2021-03-25	2021-07-01
doggroomingnews.com	NameSilo	45.135.167.27	AS207560	Zubritska Valeriia Nikolaevna	2021-04-01	2021-05-20
alifemap.com	NameCheap	188.68.250.182	AS197226	sprint S.A.	2021-04-10	2021-09-15
enpport.com	NameCheap	54.38.137.218	AS16276	OVH SAS	2021-04-15	2021-06-25
theyardservice.com	NameCheap	83.171.237.173	AS201206	Droptop GmbH	2021-04-15	2021-06-24
celebsinformation.com	NameSilo	37.59.225.51	AS16276	OVH SAS	2021-04-20	2021-09-01
dailydews.com	NameSilo	31.42.177.114	AS43641	SOLLUTIUM	2021-02-20	2021-06-10
ideasofbusiness.com	NameSilo	81.17.30.46	AS51852	Private Layer INC	2021-06-01	2021-06-15
newminigolf.com	NameSilo	79.143.87.166	AS25369	Hydra Communications Ltd	2021-02-15	2021-08-15
rchosts.com	NameSilo	51.89.50.153	AS16276	OVH SAS	2021-06-15	2021-10-25
stockmarketon.com	NameCheap	51.254.241.158	AS16276	OVH SAS	2021-02-20	2021-03-15
stonecrestnews.com	NameCheap	91.234.254.144	AS49981	WorldStream B.V.	2021-03-10	2021-09-05
teachingdrive.com	NameCheap	194.135.81.18	AS62282	UAB Rakrejus	2021-05-01	2021-09-25
newstepsco.com	NameCheap	185.158.250.239	AS9009	M247 Ltd	2021-03-15	2021-06-04
tacomanewspaper.com	Epik	195.206.181.169	AS25369	Hydra Communications Ltd	2021-02-25	2021-06-10

B. Bibliographie

[1] MSTIC - Microsoft. *Breaking down NOBELIUM's Latest Early-Stage Toolset*. 28 mai 2021.
URL : https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/.

[2] Alex Lanstein. *Another big wave from unc2652/Nobelium*. 15 juillet 2021.
URL : https://www.twitter.com/alex_lanstein/status/1415761111891148800.

[3] MSTIC - Microsoft. *Deep Dive into the Solorigate Second-Stage Activation : From SUNBURST to TEARDROP and Raindrop*. 20 janvier 2021.
URL : https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/.

[4] MSTIC - Microsoft. *New Sophisticated Email-Based Attack from NOBELIUM*. 27 mai 2021.
URL : https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/.

[5] MRSC - Microsoft. *New Nobelium Activity – Microsoft Security Response Center*. 25 juin 2021.
URL : https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/.

[6] Volexity. *Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns*. 27 mai 2021.
URL : https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/.

[7] Sentinel Labs. *NobleBaron - New Poisoned Installers Could Be Used In Supply Chain Attacks*. 1er juin 2021.
URL : https://labs.sentinelone.com/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/.

[8] IstroSec. *APT Cobalt Strike Campaign Targeting Slovakia (DEF CON Talk)*. 9 août 2021.
URL : https://www.istrosec.com/blog/apt-sk-cobalt/.

[9] ESET. *#ESETresearch investigated this spear-phishing campaign*. 13 août 2021.
URL : https://twitter.com/ESETresearch/status/1426204524553846785.

[10] MSTIC - Microsoft. *FoggyWeb : Targeted NOBELIUM Malware Leads to Persistent Backdoor*. 27 septembre 2021.
URL : https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/.

[11] MSTIC - Microsoft. *NOBELIUM Targeting Delegated Administrative Privileges to Facilitate Broader Attacks*. 25 octobre 2021.
URL : https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/.

[12] CERT-FR. *Points de Contrôle Active Directory*.
URL : https://www.cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/.

Version 1.1 - 06 décembre 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN