PHISHING CAMPAIGNS BY THE NOBELIUM INTRUSION SET

Version 1.1

06 December 2021

Table of contents

Summary

ANSSI (French National Cybersecurity Agency) has observed a number of phishing campaigns directed against French entities since February 2021. Of particular note, the intrusion set involved during this malicious activity has succeeded in compromising email accounts belonging to French organisations, and then using these to send weaponised emails to foreign institutions. Moreover, French public organisations have also been recipients of spoofed emails sent from supposedly compromised foreign institutions.

Technical indicators observed by ANSSI correspond to activities associated with the *Nobelium* intrusion set. This intrusion set would have been used in other attack campaigns targeting diplomatic entities and international organisations across Europe and North America. Overlaps have also been identified in the tactics, techniques & procedures (TTP) between the phishing campaigns monitored by ANSSI and the supply chain attack via SolarWinds in 2020.

This report lays out the technical information related to the phishing campaigns, beginning with details as to the nature of the malicious activities observed (section 1), the tactics, techniques & procedures (section 2) and the attack infrastructure (section 3). Similarities found with publicly documented intrusion sets are detailed in section 4. Recommendations (section 5) and indicators of compromise (appendix A) are available at the end of the document in order to help defenders protect against this type of attack and assess possible compromises.

1. Background

Since February 2021, ANSSI has dealt with a series of phishing campaigns directed against French entities. The campaigns escalated significantly in May 2021. This malicious activity is attributable to one and the same intrusion set.

The intrusion set succeeded in compromising email accounts belonging to French organisations, before using these access points to send weaponised emails to foreign institutions in the diplomatic sector. The initial method of intrusion remains unknown.

French public organisations have also been recipients of spoofed emails. These messages were sent from foreign institutions seemingly compromised by the same intrusion set.

N.B.: a threat actor is a defined set, made up of identified or identifiable individuals claiming to belong to an organisation. A threat actor implements one or more toolsets. An intrusion set is defined as the package of tools, tactics, techniques, procedures and characteristics implemented by one or more threat actors within the context of one or more cyber attacks.

2. Tactics, techniques & procedures

Category	Technique ID	Technique name	Comment
Resource development	T1584.001	Compromise Infrastructure: Domains	The intrusion set uses compromised domains to host fingerprinting information retrieved by **VaporRage** [1].
	T1586.002	Compromise Accounts: Email Accounts	The intrusion set compromises email accounts in order to send its phishing emails.
	T1583.001	Acquire Infrastructure: Domains	The intrusion set mainly uses the registrars NameCheap and NameSilo to create its C2 infrastructure.
	T1583.003	Acquire Infrastructure: Virtual Private Server	The C2 infrastructure is created using virtual private servers from different providers.
Reconnaissance	T1590.005	Gather Victim Network Information: IP Addresses	**EnvyScout** malware collects victim information, which it then exfiltrates to an attacker-controlled server [1].
	1589.001	Gather Victim Identity Information: Credentials	**EnvyScout** code attempts to log into an attacker-controlled server using SMB, potentially exfiltrating NTLM authentication credentials [1].
Initial Access	T1199	Trusted Relationship	Phishing emails are sent using compromised email addresses from trusted entities. The intrusion set masquerades as the trusted entity by using the compromised email address.
	T1566.001	Phishing: Spearphishing Attachment	The intrusion set's phishing email contains a malicious HTML file attachment called **EnvyScout** [1].
	T1566.002	Phishing: Spearphishing Link	The intrusion set hosted malware on the Google Drive platform. One of the phishing emails sent by the intrusion set contained a link to download this malware.
	T1566.003	Phishing: Spearphishing via Service	The intrusion set used the online mass-mailing service Constant Contact to distribute phishing emails to hundreds of recipients.
Execution	T1204.001	User Execution: Malicious Link	One of the intrusion set's phishing emails contained a Google Drive link, which downloaded the malware when the user clicked it [2].
	T1204.002	User Execution: Malicious File	To execute the Cobalt Strike payload, the victim needs to open the HTML file attachment in the phishing email.
	T1059.003	Command and Scripting Interpreter: Windows Command Shell	The intrusion set performed reconnaissance actions via Windows commands.
Defence Evasion	T1036.005	Masquerading: Match Legitimate Name or Location	The intrusion set renamed the ADFind executable file to mimic a legitimate executable file. This technique has previously been observed by Microsoft in the context of the SolarWinds supply chain attack [3].
	T1070.004	Indicator Removal on Host: File Deletion	With its outcome achieved, the attacker then deleted the reconnaissance tools used (BloodHound and ADFind) and the output files generated.
Discovery	T1087.002	Account Discovery: Domain Account	The intrusion set gathers domain information via Windows commands, **BoomBox** [1], ADFind and BloodHound.
	T1482	Domain Trust Discovery	The intrusion set uses tools such as ADFind or nltest to retrieve information about Domain Trusts.
Exfiltration	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	**BoomBox** malware exfiltrates the information gathered via DropBox [1].
	T1041	Exfiltration Over C2 Channel	Use of the Cobalt Strike HTTP C2 channel.

Table 2.1. – List of TTPs documented in the MITRE ATT&CK framework

3. Command and control infrastructure

The payload delivered by the intrusion set is a Cobalt Strike implant. It is configured to contact its command and control (C2) servers using HTTPs over port 443.

The domain names and IP addresses corresponding to the C2 infrastructure are available in appendix A.

3.1. Intrusion set servers

The intrusion set's C2 infrastructure is made up of virtual private servers (VPS) from different hosters. The intrusion set seems to favour servers located close to the target countries. In particular, several IP addresses within the C2 infrastructure belong to OVH.

A breakdown is shown as follows:

AS Number	AS Name	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. – Distribution of the AS used by the intrusion set

3.2. Domain names

The domain names used by the intrusion set as Cobalt Strike C2 resemble legitimate domain names. A number of domain names registered by the intrusion set mimic information and news websites. In the majority of cases, the intrusion set registers its domain names with NameSilo and NameCheap.

3.3. Cobalt Strike profiles

The Cobalt Strike samples used by the attacker are configured to contact specific URLs on control servers. The URIs used include: « `/jquery-3.3.1.min.js` » and « `/jquery-3.3.2.min.js` ».

Both URIs correspond to publicly available Cobalt Strike Malleable profiles[1], albeit with certain modifications made.

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

4. Links with publicly documented intrusion sets

The technical indicators observed by ANSSI in sections 2 & 3 correspond to activity associated with the *Nobelium* intrusion set as detailed in cybersecurity research by MICROSOFT [4, 1, 5], VOLEXITY [6], SENTINEL LABS [7], ISTROSEC [8] and ESET [9].

According to MICROSOFT, *Nobelium* was still active in October 2021. The intrusion set would likely have been used during other attack campaigns including, since April 2021, those targeting Active Directory Federation Services servers in an attempt to compromise government bodies, think tanks and private firms in the USA and in Europe [10, 11].

In addition, the phishing campaigns detailed in this document apply TTPs [T1036.005, T1087.002 & T1482] similar to those used during the supply chain attack via SOLARWINDS exposed in December 2020 [3].

5. Recommendations

5.1. Restrict the execution of file attachments

Given the chain of compromise detailed above, which relies on the opening of a malicious file attachment as part of a phishing campaign, it is recommended that suspicious files are not executed.

5.2. Tightening Active Directory security

The intrusion set tends to focus on Active Directory (AD) servers in particular. Tighter security measures should be applied. ANSSI has produced a guide containing recommendations for security hardening, which can be found on the CERT-FR website [12].

A. Appendix: Indicators of compromise

Domain	Registrar	IP Address	AS Number	AS Name	First seen	Last seen
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. Bibliography

[1] MSTIC - Microsoft. *Breaking down NOBELIUM's Latest Early-Stage Toolset*. May 28, 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*. July 15, 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*. January 20, 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*. May 27, 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*. June 25, 2021.
URL: https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/.

[6] Volexity. *Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns*. May 27, 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*. June 1, 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)*. August 9, 2021.
URL: https://www.istrosec.com/blog/apt-sk-cobalt/.

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

[10] MSTIC - Microsoft. *FoggyWeb: Targeted NOBELIUM Malware Leads to Persistent Backdoor*. September 27, 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*. October 25, 2021.
URL: https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/.

[12] CERT-FR. *Active Directory Security Assessment Checklist*. June 2, 2020.
URL: https://www.cert.ssi.gouv.fr/uploads/guide-ad.html.

Version 1.1 - 06 December 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