ESET Threat Intelligence APT reports PREMIUM

THREAT RESEARCH

ACTIVITY SUMMARY

Issue:

AS-2021-0007

1 April – 15 April, 2021

LAZARUS GROUP

Group overview

The Lazarus Group, active since at least 2009, is responsible for high-profile incidents such as the Sony Pictures Entertainment hack in 2016, tens-of-millions-of-dollar cyberheists in 2016, the WannaCryptor (aka WannaCry) outbreak in 2017 and a long history of disruptive attacks against South Korean public and critical infrastructure at least since 2011 until today. The diversity, number, and eccentricity in implementation of Lazarus campaigns define this group, as well as that they perform all three pillars of cybercriminal activities: cyberespionage, cybersabotage and pursuit of financial gain.

Activity summary

Operation In(ter)ception

Operation In(ter)ception is ESET's name for a series of attacks attributed to the Lazarus group. These attacks have been ongoing at least since September 2019, targeting aerospace, military, and defense companies. The operation is notable for using LinkedIn-based spearphishing and employing effective tricks to stay under the radar. Its main goal appears to be corporate espionage.

A new version of the Stage 1 downloader surfaced on VirusTotal at the beginning of April 2021. The main functionality and the structure of the malware remain the same, however the authors introduced 1-Byte XOR encryption of important strings such as URLs, User-Agent, and HTTP headers, so they cannot be easily read during static analysis.

Victimology / Business verticals

Aerospace, military, and defense companies.

Infection vector

N/A

Post-compromise activity

N/A

IoCs

Operation In(ter)ception

Date	**2021-04-07 00:08:38**
MD5	2CBE0BEA035DB9240CEB338CF9EA7FE6
SHA-1	9A8B7F11104156F0DF4F07827EC12E5C2300C4EE
SHA-256	40B6CBCC594D3696952E90FA15CCD733EBC2777554092E8C15694334274E5B90
Filename	c.exe
Description	Stage 1 loader.
C&C	*https://kehot.com[.]ar/Pubs/menus.jpg* https://www.meisami[.]net/css/search.css https://www.sfaonweb[.]com/pdf/{A76E7D01-6BAF-4FE4-98E0-.pdf *https://amon-werbeartikel[.]de/Media/Uploaded/chrisen.png*
Detection	Win64/Interception.G
PE compilation timestamp	2020-02-04 18:01:33 (Timestomped)

ESET Threat Intelligence APT reports PREMIUM

THREAT RESEARCH

TECHNICAL ANALYSIS

NETVULTURE & TURLACHOPPER

Issue:

TA-2021-0002

12 March, 2021

EXECUTIVE SUMMARY

Turla is an infamous cyberespionage group active for more than a decade. It mainly focuses on high-profile targets, such as governments and diplomatic entities, in Europe, Central Asia and the Middle East. It is known for having breached major organizations such as the US Department of Defense in 2008 and the Swiss defense company RUAG in 2014. During the past few years, we *have documented* a *large part* of the *group's arsenal* in order to raise awareness about its activities.

In January 2021, we spotted suspicious activity on a Microsoft Exchange server belonging to a Ministry of Foreign Affairs in Eastern Europe. We discovered two new malware families that we attribute to Turla: TurlaChopper and NETVulture.

Key points in this report:

- The Microsoft Exchange Outlook Web Access server was compromised likely using CVE-2020-0688.
- On this server, the attackers deployed a custom webshell, that we named TurlaChopper.
- Two months later, the attackers deployed a previously unknown backdoor, which we have named NETVulture, on another Windows server of the same organization. It was probably installed using TurlaChopper.
- NETVulture is a backdoor developed in .NET and that uses Microsoft OneDrive as its C&C server.
- The NETVulture and TurlaChopper instances had been actively used for malicious purposes from early 2020 to the beginning of January 2021.

TURLA PROFILE

Turla, also known as Snake, is an infamous cyberespionage group active for at least a decade. The group is well known for its advanced custom tools and its ability to run highly targeted operations.

For more than a decade, Turla has been responsible for numerous high-profile breaches. The targets include the *United States Central Command in 2008*, the *Finnish Ministry of Foreign Affairs* in 2013, the Swiss military company RUAG in 2014 and the *German Foreign Office* in 2017. More recently, it allegedly compromised the *French Armed Forces* in 2018 and the *Austrian Foreign Ministry* in 2019. The timeline in Figure 1 presents some of the major attacks publicly attributed to Turla.

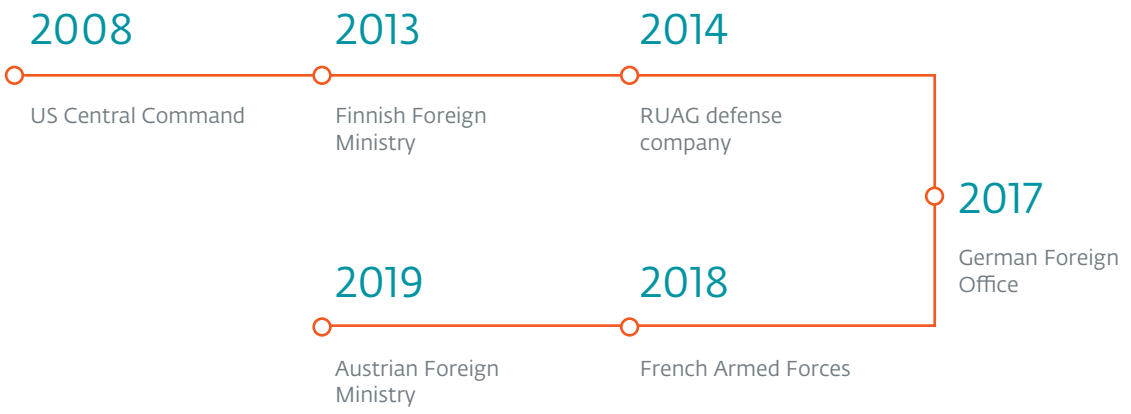

Figure 1. Timeline of attacks publicly attributed to Turla

The verticals targeted by the group have been quite consistent over the past years:

- Ministries of Foreign Affairs and diplomatic representations (embassies, consulates, etc.)
- Military organizations
- Regional political organizations
- Defense contractors

The group operates a large arsenal of malware families: from Skipper, which is often seen in *watering hole campaigns*, to sophisticated backdoors such as *ComRAT v4*, a backdoor using Gmail for C&C communications, *LightNeuron*, an implant specially designed for Microsoft Exchange email servers, and *Crutch*, a backdoor using Dropbox as its C&C server.

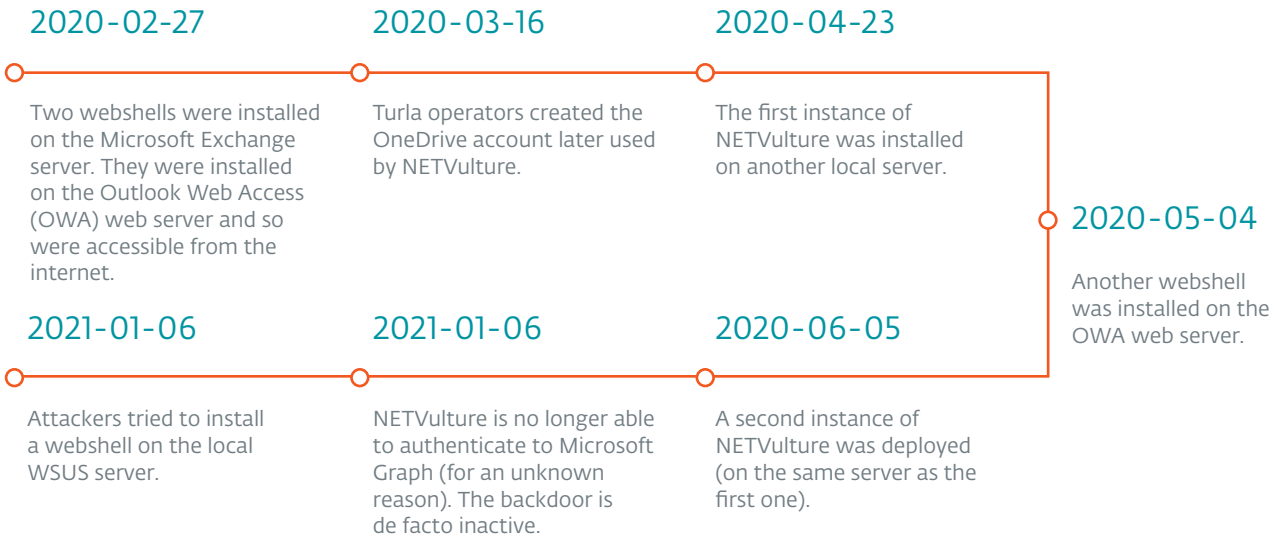

Figure 2. Timeline of important events related to the NETVulture incident

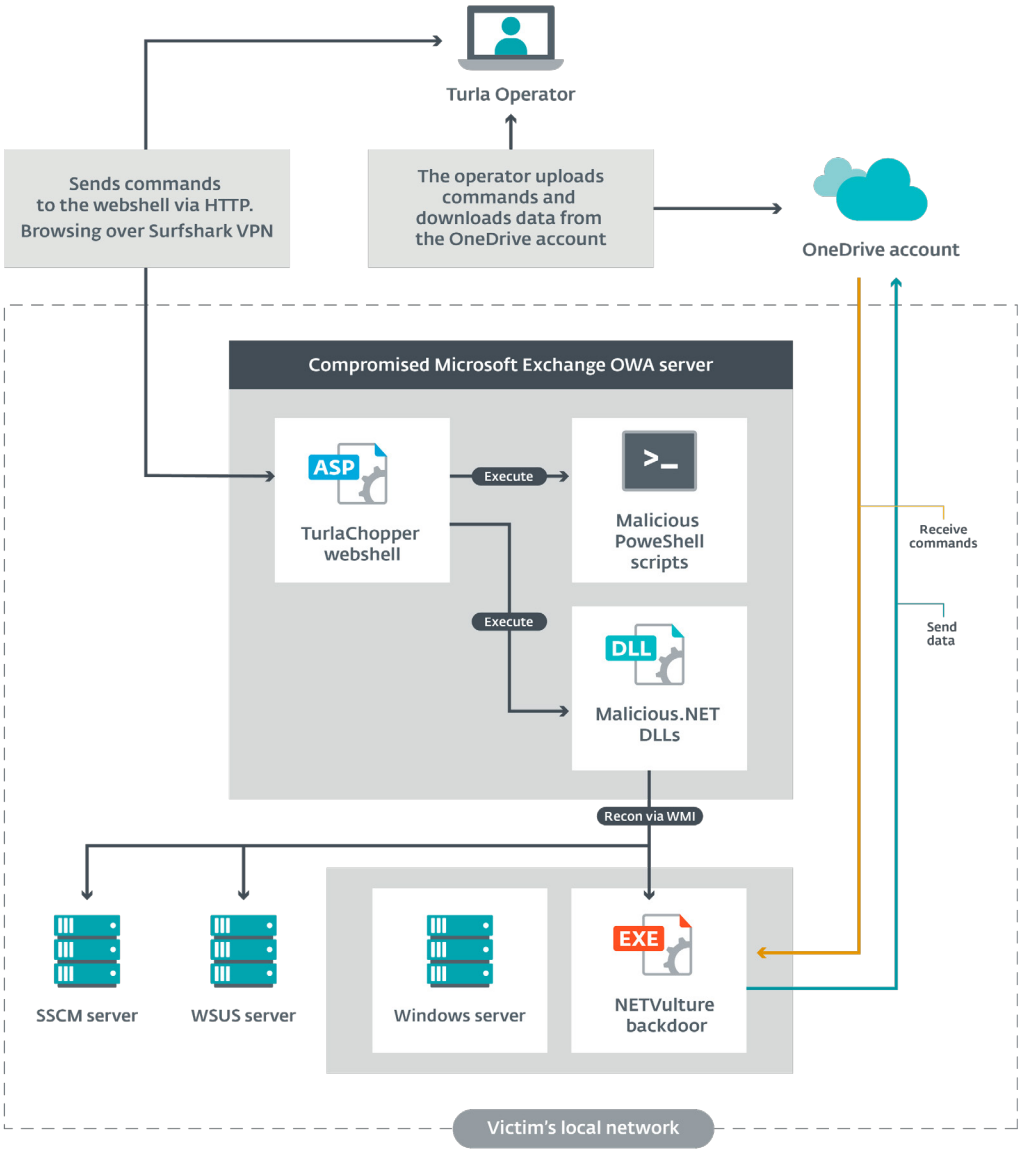

Figure 3. Overview of TurlaChopper and NETVulture usage