Turla Crutch: Keeping the “back door” open

welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open

December 2, 2020

ESET researchers discover a new backdoor used by Turla to exfiltrate stolen documents to Dropbox

Matthieu Faou
2 Dec 2020 - 11:30AM

ESET researchers found a previously undocumented backdoor and document stealer. Dubbed *Crutch* by its developers, we were able to attribute it to the infamous Turla APT group. According to our research, it was used from 2015 to, at least, early 2020. We have seen Crutch on the network of a Ministry of Foreign Affairs in a country of the European Union, suggesting that this malware family is only used against very specific targets as is common for many Turla tools..

Turla is a cyberespionage group active for more than ten years. It has compromised many governments, especially diplomatic entities, all around the world, operating a large malware arsenal that we have described in the last years.

Attribution to Turla

During our research, we were able to identify strong links between a Crutch dropper from 2016 and Gazer. The latter, also known as WhiteBear, was a second-stage backdoor used by Turla in 2016-2017. Our analysis is based on the Crutch dropper with SHA-1 A010D5449D29A1916827FDB443E3C84C405CB2A5 and the Gazer dropper with SHA-1 1AE4775EFF21FB59708E8C2B55967CD24840C8D9. We identified the following similarities:

- Both samples were dropped at C:\Intel\~intel_upd.exe on the same machine with a five-day interval in September 2017
- Both samples drop CAB files containing the various malware components

- The loaders, dropped by the aforementioned samples, share clearly related PDB paths:
  C:\Users\user\Documents\Visual Studio 2012\Projects\MemoryStarter\Release\Extractor.pdb and
  C:\Users\user\Documents\Visual Studio 2012\Projects\MemoryStarter\x64\Release\Extractor.pdb
- The loaders decrypt their payloads using the same RC4 key:
  E8 8E 77 7E C7 80 8E E7 CE CE CE C6 C6 CE C6 68

Given these elements and that Turla malware families are not known to be shared among different groups, we believe that Crutch is a malware family that is part of the Turla arsenal.

Another interesting observation is the presence of FatDuke and Crutch at the same time on one machine. The former is a third-stage backdoor that we attributed to the Dukes/APT29 in our Operation Ghost report. However, we don’t have any evidence of interaction between these two malware families. It is possible that both groups independently compromised the same machine.

Espionage activity

According to ESET LiveGrid® data, Turla used the Crutch toolset against several machines of the Ministry of Foreign Affairs in a country of the European Union. These tools were designed to exfiltrate sensitive documents and other files to Dropbox accounts Turla operators controlled.

We were able to capture some of the commands sent by the operators to several Crutch v3 instances, which is helpful to understand the goal of the operation. The operators were mainly doing reconnaissance, lateral movement and espionage.

The main malicious activity is the staging, compression and exfiltration of documents and various files, as shown in Figure 1. These are commands manually executed by the operators, thus not showing the automated collection of documents by the drive monitor component described in a later section. The exfiltration is performed by another backdoor command and thus not shown in the examples below.

```
1  copy /y \\<redacted>\C$\users\<redacted>\prog\csrftokens.txt c:\programdata\ & dir /x
   c:\programdata\
2
   copy /y \\<redacted>\c$\users\user\Downloads\FWD___~1.ZIP %temp%\
3
   copy /y \\<redacted>\c$\docume~1\User\My Documents\Downloads\8937.pdf
4  %temp%

   "C:\Program Files\WinRAR\Rar.exe" a -hp<redacted> -ri10 -r -y -u -m2 -v30m
   "%temp%\~res.dat" "d:\<redacted>\*.*" "d:\$RECYCLE.BIN\*.doc*" "d:\$RECY-
   CLE.BIN\*.pdf*" "d:\$RECYCLE.BIN\*.xls*" "d:\Recycled\*.doc*" "d:\Recycled\*.pdf*"
   "d:\<redacted>\*.pdf"
```

Figure 1. Manual commands executed by the operators during the espionage phase

Finally, the operators have a certain sense of humor. At some point, they executed the following command:

```
1  mkdir %temp%\lllbeback
```

Operators’ working hours

In order to have a rough idea of the working hours of the operators, we exported the hours at which they uploaded ZIP files to the Dropbox accounts they operate. These ZIP files contain commands for the backdoor and are uploaded to Dropbox by the operators, asynchronously from the time at which the backdoor reads and executes their content. Thus, this should show when the operators are working and not when the victim’s machines are active.

We collected 506 different timestamps and they range from October 2018 to July 2019. They are plotted in Figure 2.

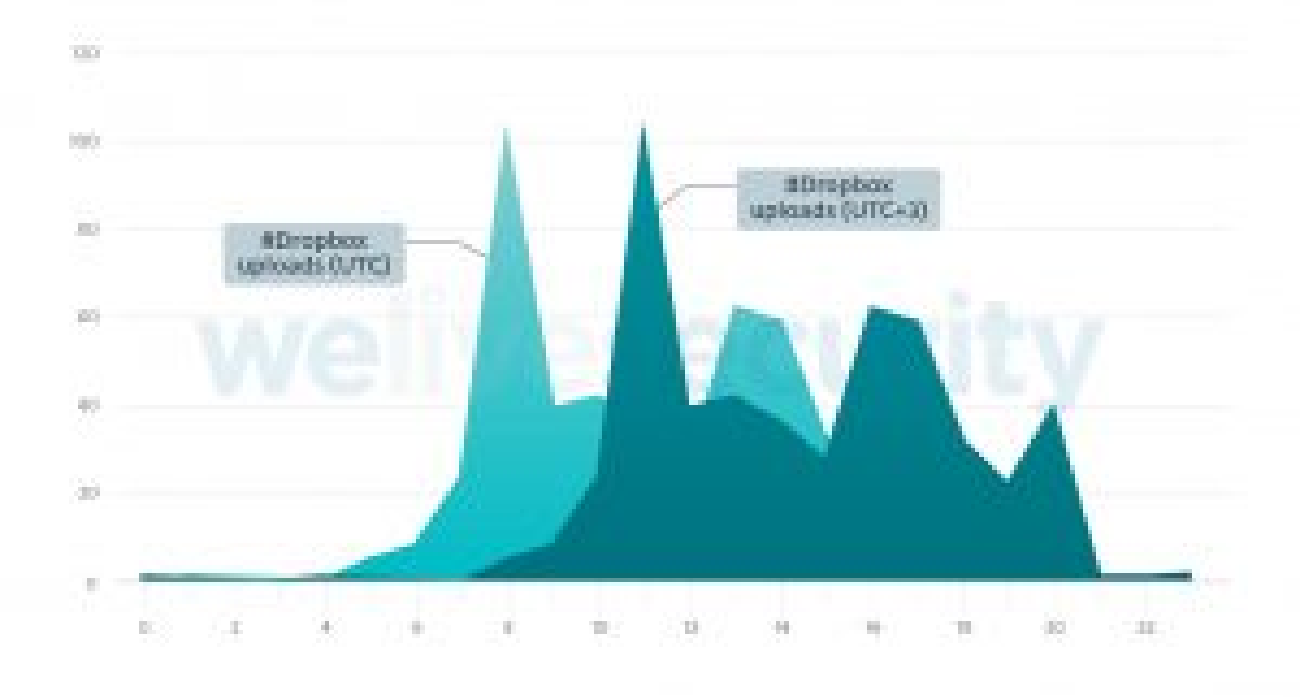

Figure 2. Working hours of Crutch operators based on the uploads to Dropbox

Given the graph, the operators are likely to operate in the UTC+3 time zone.

Compromise / Malware delivery

We believe that Crutch is not a first-stage backdoor and is deployed after the operators have first compromised an organization’s network.

The first method consists in using a first-stage implant such as Skipper. In 2017, we saw Crutch being deployed a few months after the computer was compromised by Skipper. Then, the malware operators also compromised other machines on the local network by moving laterally.

The second method we have witnessed is the use of PowerShell Empire. We were not able to uncover how the malicious script arrived on the machine, but we believe it was through another implant although a phishing document cannot be excluded. It should be noted that the PowerShell Empire scripts were using OneDrive and Dropbox.

Crutch version 1 to 3

From 2015 to mid-2019, the malware architecture used a backdoor communicating with Dropbox and a drive monitor without network capabilities.

Figure 3 outlines the architecture of Crutch version 3. It includes a backdoor that communicates with a hardcoded Dropbox account using the official HTTP API. It can execute basic commands such as reading and writing files or executing additional processes. It persists via DLL hijacking on Chrome, Firefox or OneDrive. In some variants, we noticed the presence of recovery C&C channels using either GitHub or a regular domain.

The second main binary is a removable-drive monitor that searches for files that have an interesting extension (.pdf, .rtf, .doc, .docx). It then stages the files in an encrypted archive.

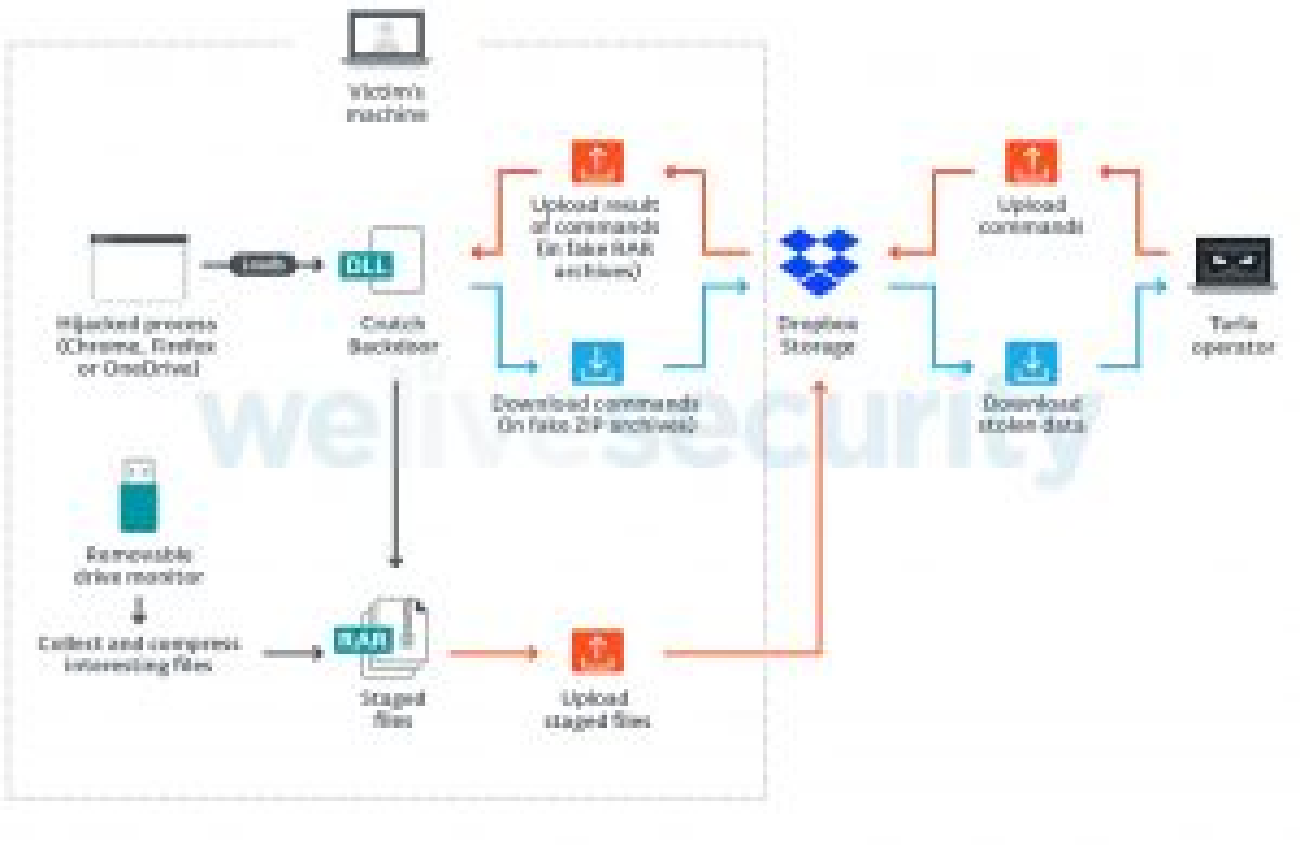

Figure 3. Architecture of Crutch v3

Crutch version 4

In July 2019, we found a new version of Crutch. While we don’t have the developer’s version number, we believe it has evolved enough to qualify as version 4. This new version is an updated version of the removable-drive monitor with networking capabilities.

Figure 4 shows the architecture of Crutch v4. The main difference is that it no longer supports backdoor commands. On the other hand, it can automatically upload the files found on local and removable drives to Dropbox storage by using the Windows version of the Wget utility.

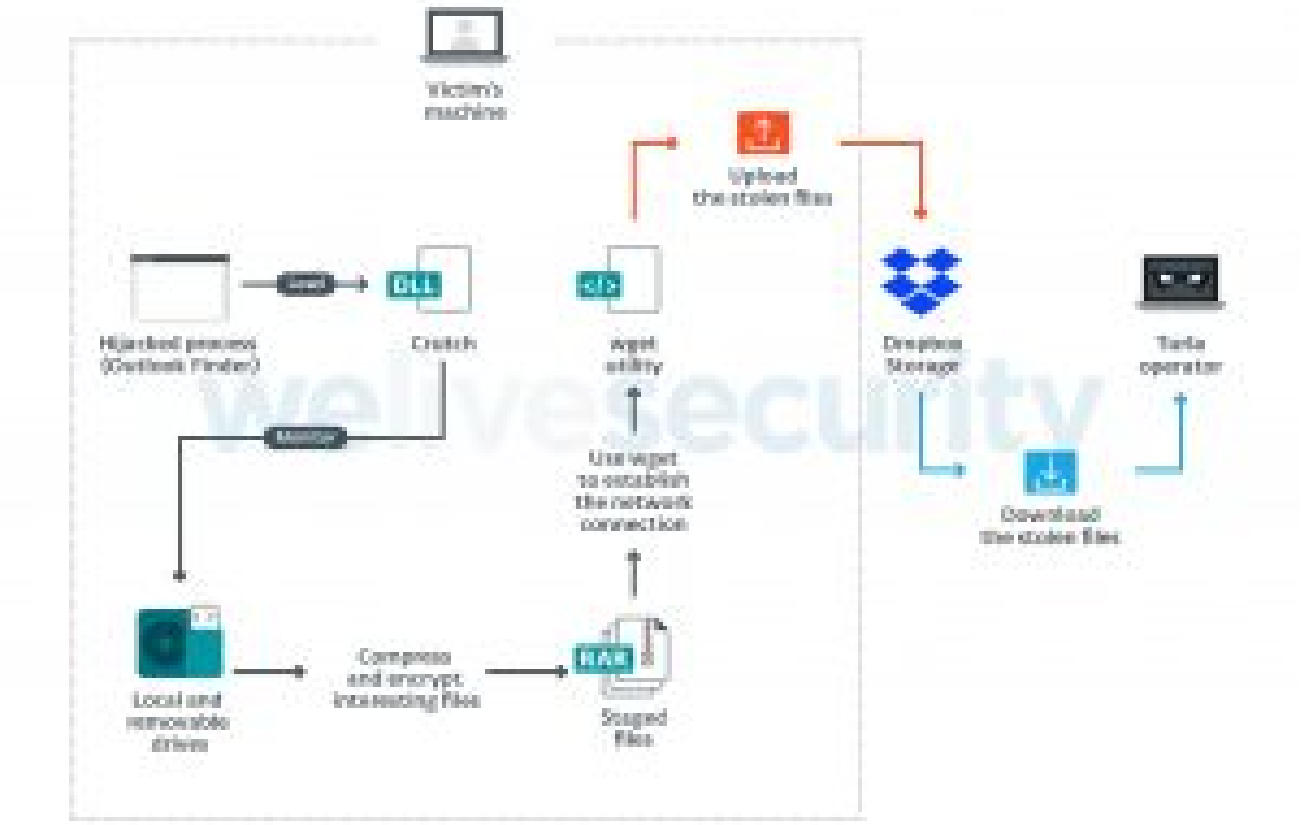

Figure 4. Architecture of Crutch v4

The working directory of this v4 is C:\Intel where the following components are found:

- outllib.dll: The Crutch DLL
- finder.exe: The genuine Outlook Item Finder from Microsoft Outlook (SHA-1: 830EE9E6A1BB7588AA8526D94D2D9A2B491A49FA)
- resources.dll: Genuine DLL that is a dependency of finder.exe (SHA-1: 31D82C554ABAB3DD8917D058C2A46509272668C3)
- outlook.dat: Crutch config file. It contains the Dropbox API token.
- ihlp.exe: The genuine RAR utility (SHA-1: A92C801F491485F6E27B7EF6E52E02B461DBCFAA)
- msget.exe: A clean version of the Wget utility for Windows (SHA-1: 457B1CD985ED07BAFFD8C66FF40E9C1B6DA93753)

As Crutch v3, it persists using DLL hijacking. However, in this case the host application is an old Microsoft Outlook component that is dropped on the compromised system by the operators.

Conclusion

In the past few years, we have publicly documented multiple malware families operated by Turla. Crutch shows that the group is not short of new or currently undocumented backdoors. This discovery further strengthens the perception that the Turla group has considerable resources to operate such a large and diverse arsenal.

Crutch is able to bypass some security layers by abusing legitimate infrastructure – here Dropbox – in order to blend into normal network traffic while exfiltrating stolen documents and receiving commands from its operators.

Indicators of Compromise can also be found on GitHub. For any inquiries, or to make sample submissions related to the subject, contact us at: threatintel@eset.com.

Indicators of Compromise

Hashes

SHA-1	Description	ESET detection name
A010D5449D29A1916827FD-B443E3C84C405CB2A5	Crutch dropper similar to Gazer	Win64/Agent.VX
2FABCF0FCE7F733F45E73B432F413E564B92D651	Crutch v3 backdoor (packed)	Win32/Agent.TQL
A4AFF23B9A58B598524A71F09AA67994083A9C83	Crutch v3 backdoor (unpacked)	Win32/Agent.TQL
778AA3A58F5C76E537B5FE287912CC53469A6078	Crutch v4	Win32/Agent.SVE

Paths

Crutch working directories

- C:\Intel\
- C:\AMD\Temp\

Filenames

- C:\Intel\outllib.dll
- C:\Intel\lang.nls
- C:\Intel\~intel_upd.exe
- C:\Intel\~csrss.exe

- C:\Program Files (x86)\Google\Chrome\Application\dwmapi.dll
- C:\Program Files (x86)\Mozilla Firefox\rasadhlp.dll
- %LOCALAPPDATA%\Microsoft\OneDrive\dwmapi.dll

Network

- hotspot.accesscam[.]org
- highcolumn.webredirect[.]org
- ethdns.mywire[.]org
- theguardian.webredirect[.]org
- https://raw.githubusercontent[.]com/ksRD18pro/ksRD18/master/ntk.tmp

MITRE ATT&CK techniques

Note: This table was built using version 7 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Initial Access	T1078.003	Valid Accounts: Local Accounts	Crutch operators abused local accounts that have the same password across the victim’s network. This was used when compromising additional machines in the network, the initial breach is unknown.
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task	Crutch v4 persists using a Windows scheduled task.
	T1574.001	Hijack Execution Flow: DLL Search Order Hijacking	Crutch v3 persists by doing DLL search order hijacking on Google Chrome, Mozilla Firefox or Microsoft OneDrive.
Defense Evasion	T1036.004	Masquerading: Masquerade Task or Service	Crutch v4 persists using a scheduled task that impersonates the Outlook item finder.
	T1120	Peripheral Device Discovery	Crutch monitors when a removable drive is plugged into the compromised machine.
	T1025	Data from Removable Media	Crutch monitors removable drives and exfiltrates files matching a given extension list.

Tactic	ID	Name	Description
	T1074.001	Data Staged: Local Data Staging	The Crutch v3 removable-drive monitor stages the stolen files in the C:\AMD\Temp directory.
	T1119	Automated Collection	Crutch automatically monitors removable drives in a loop and copies interesting files.
	T1560.001	Archive Collected Data: Archive via Utility	Crutch uses the WinRAR utility to compress and encrypt stolen files.
	T1008	Fallback Channels	Crutch v3 uses a hardcoded GitHub repository as a fallback channel.
	T1071.001	Application Layer Protocol: Web Protocols	The network protocol of Crutch uses the official Dropbox API over HTTP.
	T1102.002	Web Service: Bidirectional Communication	Crutch uses Dropbox to download commands and to upload stolen data.
Exfiltration	T1020	Automated Exfiltration	Crutch v4 automatically exfiltrates the stolen files to Dropbox.
	T1041	Exfiltration Over C2 Channel	Crutch exfiltrates data using the primary C&C channel (Dropbox HTTP API).
	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Crutch exfiltrates stolen data to Dropbox.

2 Dec 2020 - 11:30AM