Malicious Telegram Installer Drops Purple Fox Rootkit

blog.minerva-labs.com/malicious-telegram-installer-drops-purple-fox-rootkit



- <u>Tweet</u>
- ٠

We have often observed threat actors using legitimate software for dropping malicious files. This time however is different. This threat actor was able to leave most parts of the attack under the radar by separating the attack into several small files, most of which had very low detection rates by AV engines, with the final stage leading to Purple Fox rootkit infection.

Thanks to the <u>MalwareHunterTeam</u>, we were able to dig deeper into the malicious Telegram Installer. This installer is a compiled Autolt (a freeware BASIC-like scripting language designed for automating Windows GUI and general scripting) script called "Telegram Desktop.exe":



Figure 1 - Malicious Installer's Icon

This Autolt script is the first stage of the attack which creates a new folder named "TextInputh" under C:\Users\Username\AppData\Local\Temp\ and drops a legitimate Telegram installer (which is not even executed) and a malicious downloader (TextInputh.exe).

📙 🛃 🔚 🖛 C:\Users	AppData\Local\Temp\Textinputh				
File Home Share	View				
← → ▾ 📘 → This	PC > Local Disk (C:) > Users	AppData > Local > Temp	> TextInputh		~ i
Local ^	Name	Date modified	Туре	Size	
Applica	🥑 Telegram.exe	11/26/2021 11:37 PM	Application	102,568 KB	
Boxstar	Textinputh.exe	12/8/2021 12:54 AM	Application	171 KB	
Comm					
Connex					
- Country					

Figure 2 - File dropped by compiled AutoIT

TextInputh.exe

When executed, TextInputh.exe creates a new folder named "1640618495" under the C:\Users\Public\Videos\ directory. TextInputh.exe file is used as a downloader for the next stage of the attack. It contacts a C&C server and downloads two files to the newly created folder:

- 1. 1.rar which contains the files for the next stage. 7zz.exe a legitimate 7z archiver.
- 2. The 7zz.exe is used to unarchive 1.rar, which contains the following files:

2 1.rar (evaluation copy)										
File Commands Tools Favorites Options Help										
Add Extract To	Test View	Delete	O 🔍 🤞 Find Wiz	ard Info Vir	o 🗐 usScan Commer	Protect	SFX			
1.rar - R/	1.rar - RAR archive, unpacked size 8,635,521 bytes									
Name	Size	Packed	Туре	Modified	CRC32					
			File folder							
360.tct	41,984	18,766	TCT File	12/7/2021 1:28	48C5D91F					
ojbk.exe	40,960	18,194	Application	12/8/2021 2:51	A8CB5D68					
rundli3222.exe	46,080	18,937	Application	6/14/2017 6:20	D458889D					
svchost.txt	8,506,497	2,416,805	Text Document	12/8/2021 9:32	B9EFA73F					

Figure 3 - The content of 1.rar

Next, TextInputh.exe performs the following actions:

- Copies 360.tct with "360.dll" name, rundll3222.exe and svchost.txt to the ProgramData folder
- Executes ojbk.exe with the "ojbk.exe -a" command line
- Deletes 1.rar and 7zz.exe and exits the process

ojbk.exe

When executed with the "-a" argument, this file is only used to reflectively load the malicious 360.dll file:



Figure 4 - Load of "360.tct" aka 360.dll by ojbk.exe

This DLL is responsible for reading the dropped svchost.txt file. After which, a new HKEY_LOCAL_MACHINE\SYSTEM\Select\MarkTime registry key is created, whose value equals the current time of svchost.exe and then, the svchost.txt payload is executed.

svchost.txt

As the attack flow continues, this file appears to contain the byte code of the next stage of the malicious payload executed by the 360.dll. As the first action of svchost.txt, it checks for the existence of the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\360safe.exe\Path registry key. If the registry key is found, the attack flow will perform an additional step before moving on to the next stage:

The attack drops five more files into the ProgramData folder:

- Calldriver.exe this file is used to shut down and block initiation of 360 AV
- Driver.sys after this file is dropped, a new system driver service named "Driver" is created and started on the infected PC and bmd.txt is created in the ProgramData folder

Processes Services Netw	rok Disk										
Name	Display name	Type	Status	Start type							
DevicesFlowUserSvc	DevicesFlow	User share pro	Stopped	ped Demand start							
DevicesFlowUserS	DevicesFlow_28b212	User share pro	Stopped	Demand start							
DevQueryBroker	DevQuery Background Discovery Broker	Share process	Stopped	ed Demand start (brigger)							
i Dfsc	DFS Namespace Client Driver	FS driver	Running	System start							
C Ohcp	DHCP Client	Unknown	Running	Auto start							
🗖 diagnosticshub.sta	Microsoft (R) Diagnostics Hub Standard Collector Service	Own process	Stopped	Demand start							
diagove	Diagnostic Execution Service	Share process	Stopped	Demand start (tri	gger)						
DiagTrack	Connected User Experiences and Telemetry	Own process	Stopped	Disabled							
📮 disk	Disk Driver	Driver	Running	Boot start							
📮 DispBrokerDeskto	Display Policy Service	Unknown	Running	Auto start (del De	iver Properties						×
DisplayEnhancem	Display Enhancement Service	Share process	Stopped	Demand start							
OmEnrollmentSvc	Device Management Enrollment Service	Own process	Stopped	Demand start	Trigger		Othe	r		Comment	
Ø dmvsc	dmvsc	Driver	Stopped	Demand start	General	Securty	Recovery	Depe	ndencies	Depen	dents
dmwappushservice	Device Management Wireless Application Protocol (WAP) P	Share process	Stopped	Disabled (dela	Denter						
Onscache	DNS Client	Unknown	Running	Auto start	Cover						
a DoSve	Delivery Optimization	Unknown	Running	Auto start (del							
dot3svc	Wired AutoConfig	Share process	Stopped	Demand start							~
	Diagnostic Policy Service	Unknown	Running	Auto start	-				-		_
Oriver	Driver	Driver	Stopped	Demand start	Type: Driver		Ý	Stat type:	Demand	stat	Ŷ
Ormkaud	Microsoft Trusted Audio Drivers	Driver	Stopped	Demand start	Error control:	Ignore	Ŷ	Group:			
DamSve	Device Setup Manager	Unknown	Stopped	Demand start						1.	= 1
DiSve	Data Sharing Service	Unknown	Running	Demand start	Binary path:	VINC Prog	yanData'.Drv	er sys		Bows	e
DusmSvc	Duta Usage	Own process	Running	Auto start	User account:						
DXGKml	LDDM Graphics Subsystem	Driver	Running	System start		-					
😺 e1i65x64	Intel(R) PRO/1000 PCI Express Network Connection Driver I	Driver	Running	Demand start	Paseword:						10
Eaphost	Extensible Authentication Protocol	Share process	Stopped	Demand start	Service DLL:	N/A					
O ebdry	QLogic 10 Gigabit Ethernet Adapter VBD	Driver	Stopped	Demand start	Deland an						_
EFS EFS	Encrypting File System (EFS)	Share process	Stopped	Demand start							
EhStorClass	Enhanced Storage Filter Driver	Driver	Running	Boot start							
EhStorTcgDrv	Microsoft driver for storage devices supporting IEEE 1667 an	Driver	Stopped	Demand start							
embeddedmode	Embedded Mode	Share process	Stopped	Demand start							
EntAppSvc	Enterprise App Management Service	Share process	Stopped	Demand start							
C EnDev	Microsoft Hardware Error Device Driver	Driver	Stopped	Demand start					OK	0	ancel
- EventLog	Windows Event Log	Unknown	Running	Auto start							
😝 EventSystem	COM+ Event System	Unknown	Running	Auto start							
10 A .		66 A.L.	the second second								

Figure 5 - System Driver Service

- dll.dll executed after UAC bypass. The UAC bypass technique used by svchost.txt is a "UAC bypass using CMSTPLUA COM interface" and is well described <u>here</u>. This technique is commonly used by the LockBit and BlackMatter <u>ransomware</u> authors. The dll.dll is executed with the "C:\ProgramData\dll.dll, luohua" command line.
- kill.bat a batch script which is executed after the file drop ends. The script is:

```
"C:\ProgramData\CallDriver.exe" m 360FsFlt
"C:\ProgramData\CallDriver.exe" k 0 ZhuDongFangYu.exe
copy "C:\ProgramData\speedmem2.hg" "C:\Program Files (x86)\360\360Safe\deepscan\speedmem2.hg"
ping -n 1 127.1>nul
del "C:\ProgramData\CallDriver.exe"
del "C:\ProgramData\Driver.sys"
del "C:\ProgramData\speedmem2.hg"
del "C:\ProgramData\speedmem2.hg"
del "C:\ProgramData\speedmem2.hg"
```

Figure 6 - The content of Kill.bat

speedmem2.hg - SQLite file

All these files work together to shut down and block the initiation of 360 AV processes from the kernel space, thus allowing the next stage attack tools (Purple Fox Rootkit, in our case) to run without being detected.

After the file drop and execution, the payload moves to the next step, which is the C&C communication. As mentioned above, if the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\360safe.exe\Path registry key is not found, the flow just skips to this step.

First, the hardcoded C&C address is added as a mutex. Next, the following victim's information is gathered:

- 1. Hostname
- CPU by retrieving a value of HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ ~MHz registry key

- 3. Memory status
- 4. Drive Type
- Processor Type by calling GetNativeSystemInfo and checking the value of wProcessorArchitecture.

debug056:000000180035006	call	query_CPU_registry_key
debug056:00000018003500B	lea	<pre>rcx, [rsp+850h+var_7F8]</pre>
debug056:000000180035010	mov	[rbp+750h+var_6D0], eax
debug056:000000180035016	call	cs:kernel32_GetSystemInfo
debug056:00000018003501C	mov	eax, [rsp+850h+var_7D8]
debug056:000000180035020	lea	rcx, [rbp+750h+var_7B0]
debug056:000000180035024	mov	[rbp+750h+var_6CC], eax
debug056:00000018003502A	mov	[rbp+750h+var_7B0], 40h ; '@'
debug056:000000180035031	call	<pre>cs:kernel32_GlobalMemoryStatusEx</pre>
I I one opposition approximation		

Figure 7 - Part of information gathering function

Next, the malware checks if any of the following processes are running on the victim's PC:

- 360tray.exe 360 Total Security
- 360sd.exe 360 Total Security
- kxetray.exe Kingsoft Internet Security
- KSafeTray.exe Kingsoft Internet Security
- QQPCRTP.exe Tencent
- HipsTray.exe HeroBravo System Diagnostics
- BaiduSd.exe Baidu Anti-Virus
- baiduSafeTray.exe Baidu Anti-Virus
- KvMonXP.exe Jiangmin Anti-Virus
- RavMonD.exe Rising Anti-Virus
- QUHLPSVC.EXE Quick Heal Anti-Virus
- mssecess.exe Microsoft MSE
- cfp.exe COMODO Internet Security
- SPIDer.exe
- acs.exe
- V3Svc.exe AhnLab V3 Internet Security
- AYAgent.aye ALYac Software
- avgwdsvc.exe AVG Internet Security
- f-secure.exe F-Secure Anti-Virus
- avp.exe Kaspersky Anti-Virus
- Mcshield.exe McAfee Anti-Virus
- egui.exe ESET Smart Security
- knsdtray.exe
- TMBMSRV.exe Trend Micro Internet Security
- avcenter.exe Avira Anti-Virus
- ashDisp.exe Avast Anti-Virus
- rtvscan.exe Symantec Anti-Virus
- remupd.exe Panda software
- vsserv.exe Bitdefender Total Security

- PSafeSysTray.exe PSafe System Tray
- ad-watch.exe
- K7TSecurity.exe K7Security Suite
- UnThreat.exe UnThreat Anti-Virus

It seems that after this check is complete, all the collected information, including which security products are running, is sent to the C&C server.

At the time of the investigation, the C&C server was already down, but a quick check of the IP address and other related files all indicate that the last stage of this attack is the download and execution of the Purple Fox Rootkit. Purple Fox uses the msi.dll function, 'MsiInstallProductA', to download and execute its payload. The payload is a .msi file that contains encrypted shellcode including 32-bit and 64-bit versions. Once executed, the system will be restarted with the 'PendingFileRenameOperations' registry to rename its components. In our case the Purple Fox Rootkit is downloaded from hxxp://144.48.243[.]79:17674/C558B828.Png.

DII.dll

This DLL is only used for disabling UAC by setting the three following registry keys to 0:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop

1	
sub	esp, 8
push	esi
lea	eax, [esp+0Ch+phkResult]
push	eax ; phkResult
push	offset SubKey ; "SOFTWARE\\Microsoft\\Windows\\CurrentVe"
push	8000002h ; hKey
mov	[esp+18h+phkResult], 0
call	ds:Reg0penKeyA
mov	edx, [esp+0Ch+phkResult]
mov	esi, ds:RegSetValueExA
push	4 ; cbData
lea	ecx, [esp+10h+Data]
push	ecx ; lpData
push	4 ; dwType
push	0 ; Reserved
push	offset ValueName ; "ConsentPromptBehaviorAdmin"
push	edx ; hKey
mov	dword ptr [esp+24h+Data], 0
call	esi ; RegSetValueExA
mov	ecx, [esp+0Ch+phkResult]
push	4 ; cbData
lea	eax, [esp+10h+Data]
push	eax ; 1pData
push	4 ; dwType
push	0 ; Reserved
push	offset aEnablelua ; "EnableLUA"
push	ecx ; hKey
call	esi ; RegSetValueExA
mov	eax, [esp+0Ch+phkResult]
push	4 ; cbData
lea	edx, [esp+10h+Data]
push	edx ; lpData
push	4 ; dwType
push	0 ; Reserved
push	offset aPromptonsecure ; "PromptOnSecureDesktop"
push	eax ; hKey
call	esi ; RegSetValueExA
mov	ecx, [esp+0Ch+phkResult]
push	ecx ; hKey
call	ds:RegCloseKey
xor	eax, eax
pop	esi
1 A A	

Figure 8 - UAC disabling

Calldriver.exe

Used to shut down and block initiation of 360 AV processes from the kernel space. The technique used is described <u>here</u> under "The ProcessKiller rootkit vs. security products" paragraph.

We found a large number of malicious installers delivering the same Purple Fox rootkit version using the same attack chain. It seems like some were delivered via email, while others we assume were downloaded from phishing websites. The beauty of this attack is that every stage is separated to a different file which are useless without the entire file set. This helps the attacker protect his files from AV detection.



Figure 9 - Purple Fox Rootkit File Creation Flow

Mitigation

Minerva Labs detects malicious process relationships and prevents the malware from writing and executing malicious payloads:

\$	[531 Crea	6] C:\V	Vindows\explo	rer.exe 06:00 pm by	EDESKTOP	-		
\rightarrow	\$	[1356 Creat] C:\Users\ ed on Jan 3rd :	\Desktop\Te 2022 12:57 pm 1	legram des	ktop.exe stop-		
	÷	\$	[5844] C:\User Created on Jan	3rd 2022 12:57	op\Telegran 7 pm by	edesktop.exe		
		-⇒ ([8820] C:N Command: Created o SNA 256:	Users\ 44 "C:\Users\ n Jan 3rd 2022 bael270981c0a	AppData\Loc AppData 12:58 pm by 2d595677a7	al\Temp\Textinp \Local\Temp\T }DESKTOP- Talfefe8087b07	with\TextInputP extInputh\Tex ffea061571d9	h.exe xtInputh.exe" 7b5cd4c0e3edb6e0
			<u>(</u>)	× 📒 c:	Users\Pub	lic\Videos\16412	07494	

Figure 10 - Additional payload download into Videos folder prevented by Minerva Armor

Learn more about Minerva's Ransomware Protection.

IOC's:

Hashes:

- 41769d751fa735f253e96a02d0cccadfec8c7298666a4caa5c9f90aaa826ecd1 Telegram Desktop.exe
- BAE1270981C0A2D595677A7A1FEFE8087B07FFEA061571D97B5CD4C0E3EDB6E0 TextInputh.exe
- af8eef9df6c1f5645c95d0e991d8f526fbfb9a368eee9ba0b931c0c3df247e41 legitimate telegram installer
- 797a8063ff952a6445c7a32b72bd7cd6837a3a942bbef01fc81ff955e32e7d0c 1.rar
- 07ad4b984f288304003b080dd013784685181de4353a0b70a0247f96e535bd56 7zz.exe
- 26487eff7cb8858d1b76308e76dfe4f5d250724bbc7e18e69a524375cee11fe4 360.tct
- b5128b709e21c2a4197fcd80b072e7341ccb335a5decbb52ef4cee2b63ad0b3e ojbk.exe
- 405f03534be8b45185695f68deb47d4daf04dcd6df9d351ca6831d3721b1efc4 rundll3222.exe legitimate rundll32.exe
- 0937955FD23589B0E2124AFEEC54E916 svchost.txt
- e2c463ac2d147e52b5a53c9c4dea35060783c85260eaac98d0aaeed2d5f5c838 Calldriver.exe
- 638fa26aea7fe6ebefe398818b09277d01c4521a966ff39b77035b04c058df60 Driver.sys
- 4bdfa7aa1142deba5c6be1d71c3bc91da10c24e4a50296ee87bf2b96c731b7fa dll.dll
- 24BCBB228662B91C6A7BBBCB7D959E56 kill.bat
- 599DBAFA6ABFAF0D51E15AEB79E93336 speedmem2.hg

IP's:

- 193.164.223[.]77 second stage C&C server.
- 144.48.243[.]79 last stage C&C server.

Url's

hxxp://193.164.223[.]77:7456/h?=1640618495 - contains 1.rar file

• hxxp://193.164.223[.]77:7456/77 - contain 7zz.exe file

• hxxp://144.48.243[.]79:17674/C558B828.Png – Purple Fox Rootkit

Resources:

https://malpedia.caad.fkie.fraunhofer.de/details/win.purplefox