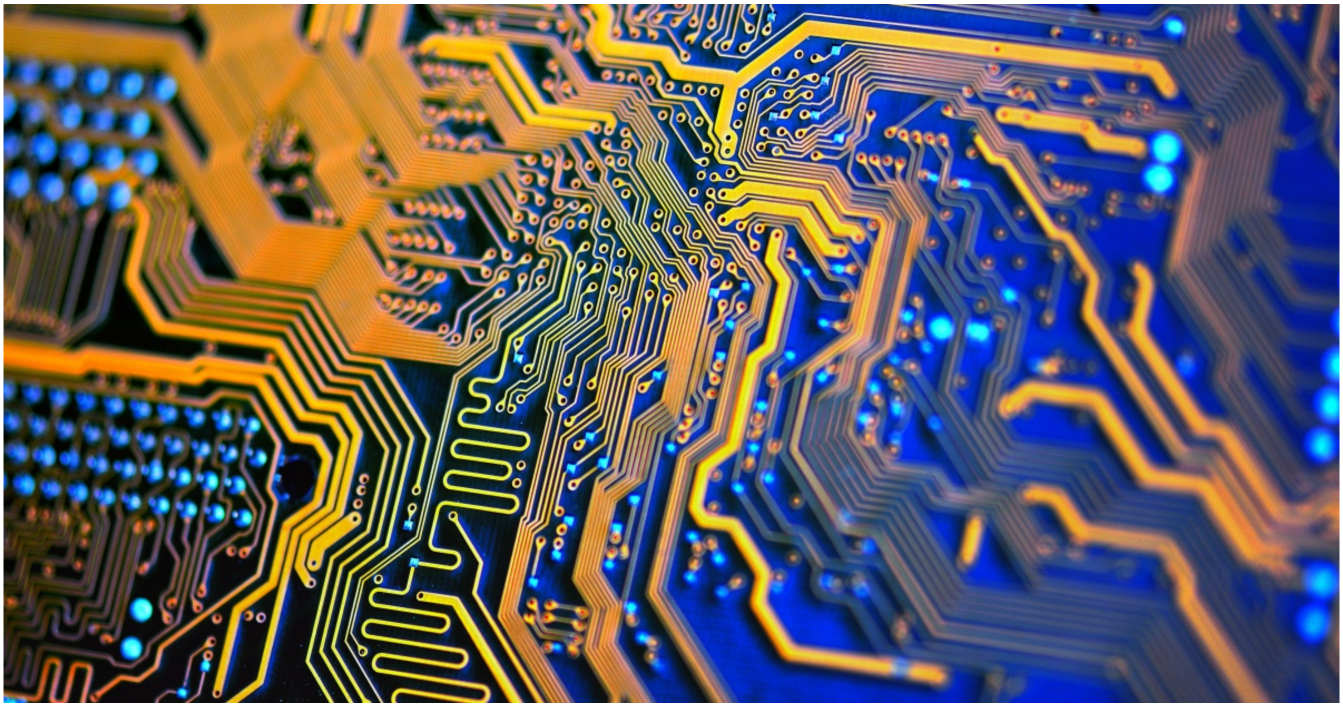
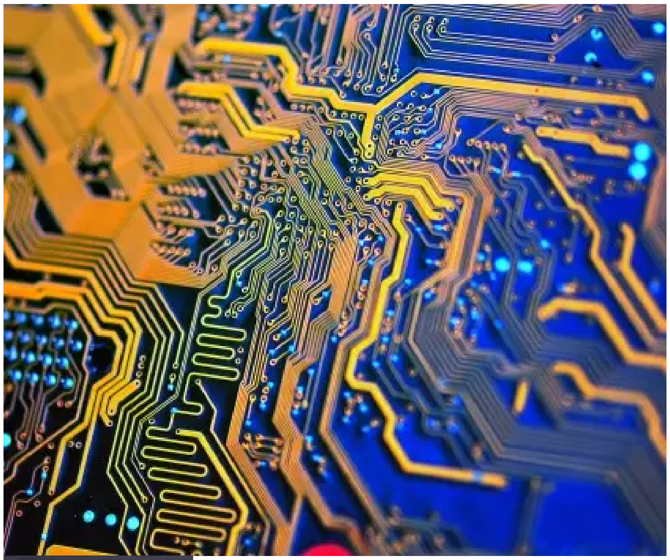
Raindrop: New Malware Discovered in SolarWinds Investigation

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware





Threat Hunter TeamSymantec

Tool was used to spread onto other computers in victims' networks.

Symantec, a division of Broadcom (NASDAQ: AVGO), has uncovered an additional piece of malware used in the SolarWinds attacks which was used against a select number of victims that were of interest to the attackers.

Raindrop (Backdoor.Raindrop) is a loader which delivers a payload of Cobalt Strike. Raindrop is very similar to the already documented Teardrop tool, but there are some key differences between the two. While Teardrop was delivered by the initial Sunburst backdoor (Backdoor.Sunburst), Raindrop appears to have been used for spreading across the victim's network. Symantec has seen no evidence to date of Raindrop being delivered directly by Sunburst. Instead, it appears elsewhere on networks where at least one computer has already been compromised by Sunburst.

Raindrop attacks

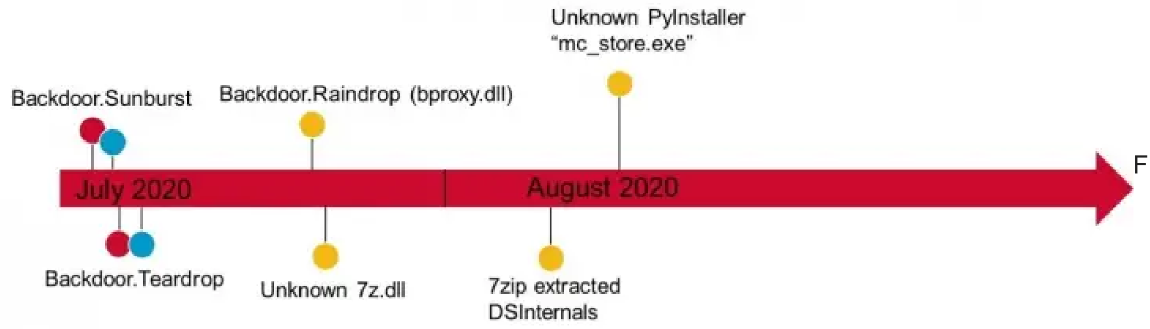
In one victim, in early July 2020, Sunburst was installed through the SolarWinds Orion update, as has been well documented. Two computers were compromised.

The following day, Teardrop was subsequently installed on one of these computers. That computer was found to have an active directory query tool, as well as a credential dumper designed specifically for SolarWinds Orion databases. The credential dumper was similar to, but not the same as, the open source Solarflare tool.

Eleven days later, on a third victim computer in the organization, where no previous malicious activity had been observed, a copy of the previously unseen Raindrop was installed under the name bproxy.dll. This computer was running computer access and management software. The attackers could have used this software to access any of the computers in the compromised organization.

One hour later, the Raindrop malware installed an additional file called "7z.dll". We were unable to retrieve this file, however, within hours a legitimate version of 7zip was used to extract a copy of what appeared to be Directory Services Internals (DSInternals) onto the computer. DSInternals is a legitimate tool which can be used for querying Active Directory servers and retrieving data, typically passwords, keys, or password hashes.

An additional tool called mc_store.exe was later installed by the attackers on this computer. The tool is an unknown PyInstaller packaged application. No further activity was observed on this computer.



Example of Raindrop victim timeline

In a second victim where the Raindrop loader was seen, it was installed in a file called astdrvx64.dll in late May. Several days later, in early June, PowerShell commands were executed on that computer, attempting to execute further instances of Raindrop on additional computers in the organization.

"Invoke-Command -ComputerName REDACTED -ScriptBlock { rundll32 c:\Packages\Plugins\Microsoft.Powershell.DSC\2.77.0.0\bin\TelemetryStatus.dll Tk_CreateItemType}"

"Invoke-WMIMethod win32_process -name create -argumentlist 'rundll32 c:\windows\Speech_OneCore\Engines\TTS\en-US\enUS.Media.dll TkChangeEventWindow' -ComputerName REDACTED"

In a third victim, where Raindrop was seen, the instance of Cobalt Strike that was extracted did not have a HTTP-based command and control server, but was rather configured to use a network pipe over SMB (\\.\pipe\protected_storage[REDACTED]). It's possible that in this instance, the victim computer did not have direct access to the internet, and so command and control was routed through another computer on the local network.

Raindrop technical analysis

Raindrop is similar to Teardrop in that both pieces of malware act as a loader for Cobalt Strike Beacon. Raindrop uses a custom packer to pack Cobalt Strike. This packer is different to the one used by Teardrop.

Raindrop is compiled as a DLL, which is built from a modified version of 7-Zip source code. The 7-Zip code is not utilized and is designed to hide malicious functionality added by the attackers. The DLL is compiled where the Name file of the Export Directory Table is “"7-zip.dll" and the Export Names are:

- DllCanUnloadNow
- DllGetClassObject
- DllRegisterServer
- DllUnregisterServer

And one of the following, selected at random:

- Tk_DistanceToTextLayout
- Tk_GetScrollInfoObj
- Tk_MainLoop
- XGetGeometry

The Export Names used seem to overlap with names used by Tcl/Tk projects (see here and here).

Custom packer

Whenever the DLL is loaded, it starts a new thread from the DllMain subroutine that executes the malicious code. This malicious thread performs the following actions:

- Executes some computation to delay execution. This does not affect functionality.
- Locates start of the encoded payload which is embedded within legitimate 7-Zip machine code.

In order to locate the start of the encoded payload, the packer uses steganography by scanning the bytes starting from the beginning of the subroutine and skipping any bytes until the first occurrence of the following bytes that represent operation codes (opcodes) of interest:

```
.data:0000000180053008 opcodes        db 5, 0Dh, 15h, 1Dh, 25h, 2Dh, 35h, 3Dh, 0B8h
```

The malware will then perform the following actions:

- Extract the encoded payload. This involves simply copying data from pre-determined locations that happen to correspond to immediate values of the relevant machine instructions.
- Decrypt the extracted payload. This uses the AES algorithm in CBC mode.
- Decompress the decrypted payload. This uses the LZMA algorithm.
- Decrypt the decompressed payload. This is simple XOR with byte key and as such does not impact compression ratio.
- Execute the decrypted payload as shellcode.

Raindrop and Teardrop comparison

Although Raindrop is very similar to Teardrop, there are some key differences between the tools. As mentioned previously, Raindrop uses a different packer. The packers differ in the following ways:

	TEARDROP	**RAINDROP**
PAYLOAD FORMAT	Custom, reusing features from PE format. It may be possible to reuse the packer with a range of different payloads supplied as PE DLLs with automatic conversion.	Shellcode only.

	TEARDROP	**RAINDROP**
PAYLOAD EMBEDDING	Binary blob in data section.	Steganography, stored at pre-determined locations within the machine code.
PAYLOAD ENCRYPTION	visualDecrypt combined with XOR using long key.	AES layer before decompression; separate XOR layer using one byte key after decompression.
PAYLOAD COMPRESSION	None.	LZMA.
OBFUSCATION	Reading JPEG file. Inserted blocks of junk code, some could be generated using a polymorphic engine.	Non-functional code to delay execution.
EXPORT NAMES	Export names vary, in some cases names overlapping with Tcl/Tk projects.	Export names overlap with Tcl/Tk projects.
STOLEN CODE	Byte-copy of machine code from pre-existing third-party components. The original code is distributed in compiled format only.	Recompiled third-party source code.

While both malware families are designed to deploy Cobalt Strike Beacon, there are differences in Cobalt Strike configuration. To date, Symantec has seen four samples of Raindrop. In three cases, Cobalt Strike was configured to use HTTPS as a communication protocol. In the fourth it was configured to use SMB Named Pipe as a communication protocol.

All three Raindrop samples using HTTPS communication follow very similar configuration patterns as previously seen in one Teardrop sample (b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07).

The most important similarities are highlighted below.

	TEARDROP
SHA256	b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
URLs	https(://)infinitysoftwares(.)com/files/information_055.pdf
	https(://)infinitysoftwares(.)com/wp-admin/new_file.php
POST FORM	name="uploaded_1";filename="33139.pdf" Content-Type: text/plain

	RAINDROP
SHA256	be9dbbec6937dfe0a652c0603d4972ba354e83c06b8397d6555fd1847da36725
URLs	https(://)bigtopweb(.)com/files/page_306.pdf
	https(://)bigtopweb(.)com/wp-admin/admin-ajax.php
POST FORM	name="uploaded_1";filename="84921.pdf" Content-Type: text/plain

	RAINDROP
SHA256	f2d38a29f6727f4ade62d88d8a68de0d52a0695930b8c92437a2f9e4de92e418
URLs	https(://)panhardware(.)com/files/documentation_076.pdf
	https(://)panhardware(.)com/wp-admin/new_file.php
POST FORM	name="uploaded_1";filename="18824.pdf" Content-Type: text/plain

All of the aforementioned domains use a common Registrar, NameSilo, LLC and, except for panhardware[.]com, which is currently sinkholed, have common name servers:

- ns1.dnsowl.com
- ns2.dnsowl.com
- ns3.dnsowl.com

Clearer picture

The discovery of Raindrop is a significant step in our investigation of the SolarWinds attacks as it provides further insights into post-compromise activity at organizations of interest to the attackers. While Teardrop was used on computers that had been infected by the original Sunburst Trojan, Raindrop appeared elsewhere on the network, being used by the attackers to move laterally and deploy payloads on other computers.

Protection/Mitigation

Tools associated with these attacks will be detected and blocked on machines running Symantec Endpoint products.

File-based protection:

- Backdoor.Raindrop
- Backdoor.Teardrop
- Backdoor.Sunburst
- Backdoor.Sunburst!gen1
- Backdoor.SuperNova

Network-based protection:

System Infected: Sunburst Malware Activity

For the latest protection updates, please visit the Symantec Protection Bulletin.

Yara Rules

The Yara rules are also available for download on GitHub.

Indicators of Compromise

SHA256	DESCRIPTION
f2d38a29f6727f4ade62d88d8a68de0d52a0695930b8c92437a2f9e4de92e418	astdrvx64.dll & sddc.dll (Raindrop)
be9dbbec6937dfe0a652c0603d4972ba354e83c06b8397d6555fd1847da36725	bproxy.dll (Raindrop)
955609cf0b4ea38b409d523a0f675d8404fee55c458ad079b4031e02433fdbf3	cbs.dll (Raindrop)
N/A	Telemetry.Settings.dll (Likely Raindrop)
N/A	enUS.Media.dll (Likely Raindrop)
N/A	TelemetryStatus.dll (Likely Raindrop)
240ef5b8392b8c7a5a025c36a7e5b0e03e5bb0d0d1a28703bb22e6159a4fd10e	mc_store.exe (Unknown)
f2d38a29f6727f4ade62d88d8a68de0d52a0695930b8c92437a2f9e4de92e418	panhardware[.]com
955609cf0b4ea38b409d523a0f675d8404fee55c458ad079b4031e02433fdbf3	\\.\pipe\protected_storage[REDACTED]
be9dbbec6937dfe0a652c0603d4972ba354e83c06b8397d6555fd1847da36725	bigtopweb[.]com

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?