

POSTED: 18 JAN, 2021 | 5 MIN READ |  
THREAT INTELLIGENCE

SUBSCRIBE

FOLLOW

# Raindrop: New Malware Discovered in SolarWinds Investigation

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

Raindrop

key differ

Sunburst

spreading

Raindrop

network

## Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

[Accept Cookies](#)

[Cookies Settings](#)

## 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.

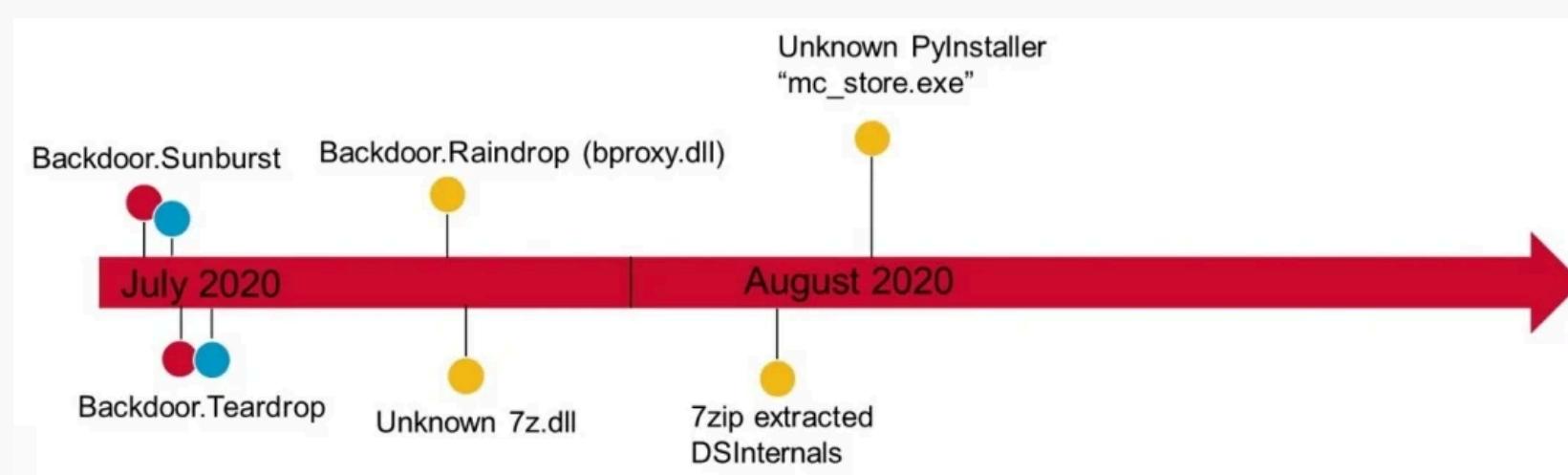


Figure 1. Example of Raindrop victim timeline

In a second victim who had astdrvx64.dll in late May, the same command and control were executed on that computer, but on additional compute

### Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

"Invoke-Command -C

c:\Packages\Plugins\Microsoft.PowerShell.DSC\2.7.0.0\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 pac

Whenever the DLL is loaded, it executes the malicious code.

- Executes some co

### Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

- 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
PAYOUT 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.
PAYOUT EMBEDDING	Binary blob in data section.	Steganography, stored at pre-determined locations within the machine code.
PAYOUT ENCRYPTION	vis us	<b>Cookies</b> By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our <a href="#">Cookie Policy</a> .
PAYOUT COMPRESSION	No	Re ju us
OBFUSCATION	Re ju us	

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	f2d38a	<b>Cookies</b>
URLs	https(:	By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our <a href="#">Cookie Policy</a> .
POST FORM	name=	

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

```
rule RaindropPacker
{
    meta:
        copyright = "Sy
        family = "Raind

    strings:
        $code = {
            41 8B 4F 20
```

## Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

// lea rsi [r15+24h]

89 8D ?? ?? 00 00	//	mov	dword ptr [rbp+0A0h+arg_0]
E8 ?? ?? ?? ??	//	call	sub_180010270
33 D2	//	xor	edx, edx
48 8D 4C 24 ??	//	lea	rcx, [rsp+1A0h+var_160]
44 8D 42 10	//	lea	r8d, [rdx+10h]
E8 ?? ?? ?? ??	//	call	sub_180038610
48 8D 5C 24 ??	//	lea	rbx, [rsp+1A0h+var_150]
F7 DB	//	neg	ebx
48 8D 7C 24 ??	//	lea	rdi, [rsp+1A0h+var_150]
48 C1 EB 02	//	shr	rbx, 2
48 8D 54 24 ??	//	lea	rdx, [rsp+1A0h+var_160]
83 E3 03	//	and	ebx, 3
48 8D 3C 9F	//	lea	rdi, [rdi+rbx*4]
48 8B CF	//	mov	rcx, rdi
E8 ?? ?? ?? ??	//	call	sub_1800101D0
48 8D 4C 24 ??	//	lea	rcx, [rsp+1A0h+var_140]
49 8B D7	//	mov	rdx, r15
48 8D 0C 99	//	lea	rcx, [rcx+rbx*4]
BB 20 00 00 00	//	mov	ebx, 20h
44 8B C3	//	mov	r8d, ebx
E8 ?? ?? ?? ??	//	call	sub_180010ED0
44 8B 85 ?? ?? 00 00	//	mov	r8d, dword ptr [rbp+0A0h+a]
48 8B D6	//	mov	rdx, rsi ; _QWORD
49 C1 E8 04	//	shr	r8, 4 ; _QWORD
48 8B CF	//	mov	rcx, rdi ; _QWORD
FF 15 ?? ?? ?? ??	//	call	cs:qword_180056E90
8B 95 ?? ?? 00 00	//	mov	edx, dword ptr [rbp+0A0h+a]
4C 8D 85 ?? ?? 00 00	//	lea	r8, [rbp+0A0h+dwSize]
48 83 A5 ?? ?? 00 00 00	//	and	[rbp+0A0h+dwSize], 0
48 8B CE	//	mov	rcx, rsi
E8 ?? ?? ?? ??	//	call	sub_180009630
48 8B 95 ?? ?? 00 00	//	mov	rdx, [rbp+0A0h+dwSize] ; d
44 8B CB	//	mov	r9d, ebx ; flProtect
41 B8 00 10 00 00	//	mov	r8d, 1000h ; flAlloc
33 C9	//	xor	ecx, ecx ; lpAddres
FF 15 ?? ?? ?? ??	//	call	cs:VirtualAlloc
48 8B 95 ?? ?? 00 00	//	mov	rdx, [rbp+0A0h+dwSize] ; d
4C 8D 8D ?? ?? 00 00	//	lea	r9, [rbp+0A0h+f1OldProtect]
48 8B C8	//	mov	rcx, rax ; lpAddres
41 B8 04 00 00 00	//	mov	r8d, 4 ; flNewPro
48 8B D8	//	mov	rbx, rax
FF 15 ?? ?? ?? ??	//	call	cs:VirtualProtect
4C 8D 8D ?? ?? 00 00	//	lea	r9, [rbp+0A0h+arg_0]
4C 8B C6	//	mov	r8, rsi
48 8D 95 ?? ?? 00 00	//	lea	rdx, [rbp+0A0h+dwSize]
48 8B CB	//	mov	rcx, rbx
E8 ?? ?? ?? ??	//	call	sub_1800095A0
4D 8B C6	//	mov	r8, r14
33 D2	//	xor	edx, edx
49 8B CF	//	mov	rcx, r15
E8 ?? ?? ?? ??	//	call	sub_180038610
33 D2	//		
41 B8 00 80	//		
49 8B CF	<b>Cookies</b>		
FF 15 ?? ??	By clicking Accept Cookies, you understand that Broadcom and		
48 8B 95 ??	third-party partners use technology, including cookies to, among		
48 85 D2	other things, analyze site usage, improve your experience and help		
74 1B	us advertise. For more details, please see our <a href="#">Cookie Policy</a> .		
48 8B CB	//	mov	rax, rcx
80 31 ??	//		
48 FF C1	//		
48 8B 95 ??	//		
48 8B C1	//		

```
48 2B C3          //    sub    rax, rbx
48 3B C2          //    cmp    rax, rdx
72 E8             //    jb     short l_0
44 8B 85 ?? ?? 00 00 // l_1: mov    r8d, [rbp+0A0h+f1OldProtect
4C 8D 8D ?? ?? 00 00 //      lea    r9, [rbp+0A0h+f1OldProtect
48 8B CB          //      mov    rcx, rbx      ; lpAddress
FF 15 ?? ?? ?? ?? //      call   cs:VirtualProtect
FF D3             //      call   rbx

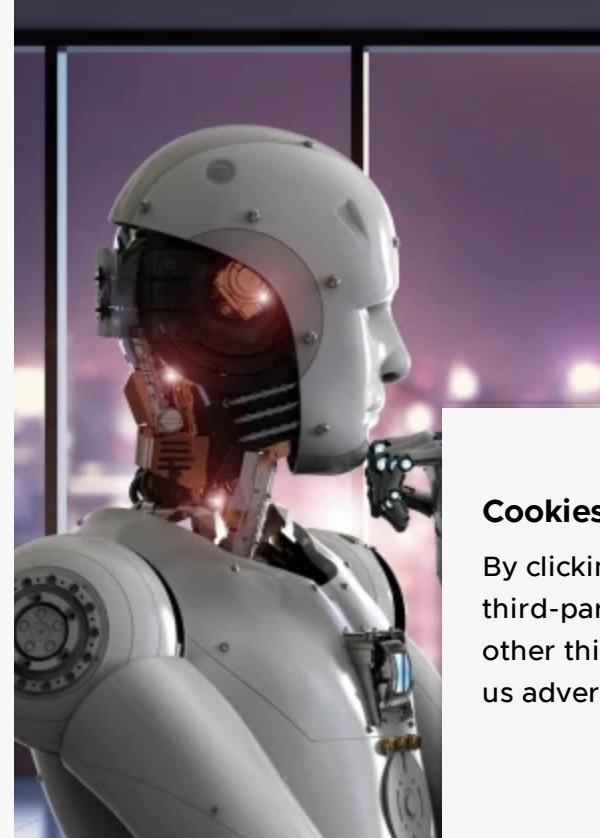
}

condition:
  all of them
}
```

The Yara rules are also [available for download](#) on GitHub.

## Indicators of Compromise

SHA256	DESCRIPTION
f2d38a29f6727f4ade62d88d8a68de0d52a0695930b8c92437a2f9e4de92e418	astdrv64.dll & sddc.dll (Raindrop)
be9dbbec6937dfe0a652c0603d4972ba354e83c06b8397d6555fd1847da36725	bproxy.dll (Raindrop)
955609cf0b4ea38b409d523a0f675d8404fee55c458ad079b4031e02433fdbf3	cbs.dll (Raindrop)
N/A	Telemetry.Settings.dll (Unknown)
N/A	enUS.Media.dll (Likely Raindrop)
N/A	TelemetryStatus.dll (Unknown)
240ef5b8392b8c7a5a025c36a7e5b0e03e5bb0d0d1a28703bb22e6159a4fd10e	mc_store.exe (Unknown)
f2d38a29f6727f4ade62d88d8a68de0d52a0695930b8c92437a2f9e4de92e418	panhardware[.]com
955609cf0b4ea38b409d523a0f675d8404fee55c458ad079b4031e02433fdbf3	\.\pipe\protected\_ (Unknown)
be9dbbec6937dfe0a652c0603d4972ba354e83c06b8397d6555fd1847da36725	bigtopweb[.]com



## About the Author

**Threat Hunter Team**  
Symantec

The Threat Hunter Team is a group of security

### Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).

# Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.



## Related Blog Posts



POSTED: 22 OCT, 2024 |  
5 MIN READ

**Exposing the Danger  
Within: Hardcoded  
Cloud Credentials in  
Popular Mobile Apps**



POSTED: 17 OCT, 2024 |  
3 MIN READ

**Ransomware: Threat  
Level Remains High in  
Third Quarter**



POSTED: 2 OCT, 2024 |  
5 MIN READ

**Stonefly: Extortion  
Attacks Continue  
Against U.S. Targets**



POSTED: 12 SEP, 2024 |  
3 MIN READ

**Ransomware: Attacks  
Once More Nearing  
Peak Levels**

[SUBSCRIBE](#)

[FOLLOW](#)

[Privacy Policy](#) [Cookie Policy](#) [Data Processing and Data Transfers](#) [Supplier Responsibility](#) [Terms of Use](#) [Sitemap](#)  
Copyright © 2005-2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

### Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our [Cookie Policy](#).