Chanitor Downloader Actively Installing Vawtrak | Zscaler

By ThreatLabz

Published: 2015-01-09 · Archived: 2026-04-06 00:34:47 UTC

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:\

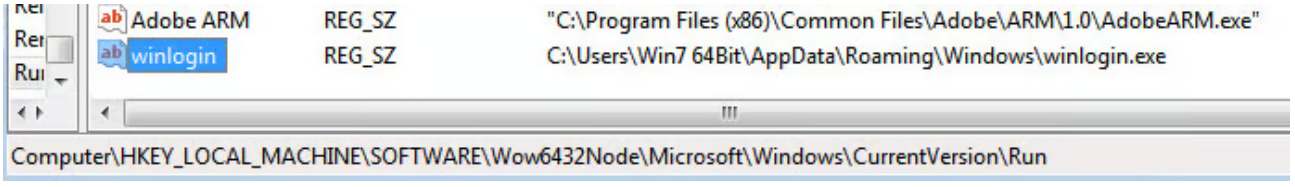
\winlogin.exe" > ___ && move /Y ___ "C:\Users\\AppData\Roaming\Windows\winlogin.exe"

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:\

" && start /B "" "C:\Users\\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:

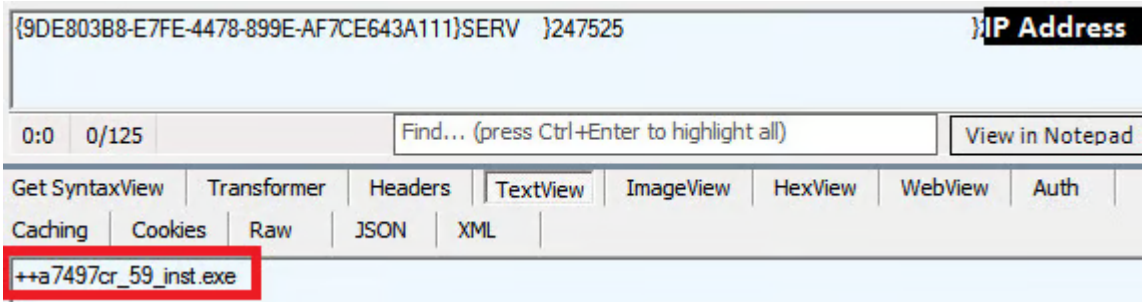
```
00402271  $  55            PUSH EBP
00402272  .  8BEC          MOV EBP,ESP
00402274  .  33C0          XOR EAX,EAX
00402276  .  56            PUSH ESI
00402277  .  8B75 08       MOV ESI,DWORD PTR SS:[ARG.1]
0040227A  .  3945 0C       CMP DWORD PTR SS:[ARG.2],EAX
0040227D  .v 76 0F         JBE SHORT 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

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.

	200	HTTP	Tunnel to	api.ipify.org:443	733			winlogin:1644
#1	200	HTTPS	api.ipify.org	/	13		text/plain	winlogin:1644
	200	HTTP	Tunnel to	svcz25e3m4mwlauz.tor2web.org:443	640			winlogin:1644
#2	200	HTTPS	svcz25e3m4mwlauz...	/gate.php	27		text/html	winlogin:1644
	200	HTTP	Tunnel to	svcz25e3m4mwlauz.tor2web.org:443	640			winlogin:1644
#3	200	HTTPS	svcz25e3m4mwlauz...	/gate.php	385,769	Expires: 0	application/octet-stream	winlogin:1644
	200	HTTP	Tunnel to	svcz25e3m4mwlauz.tor2web.org:443	640			winlogin:1644
#4	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:



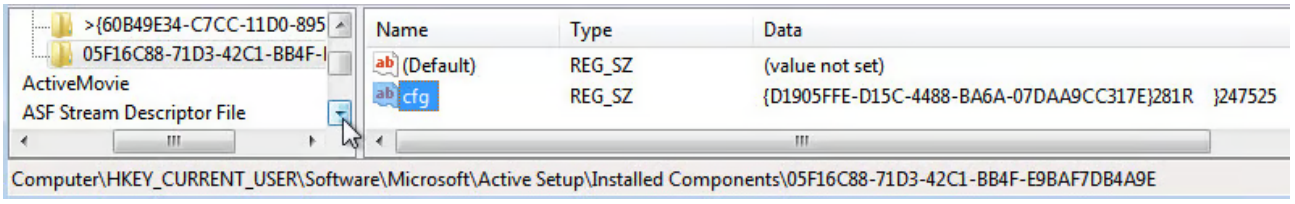
Each beacon takes the following form:

{

}}}

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 beaconing again:

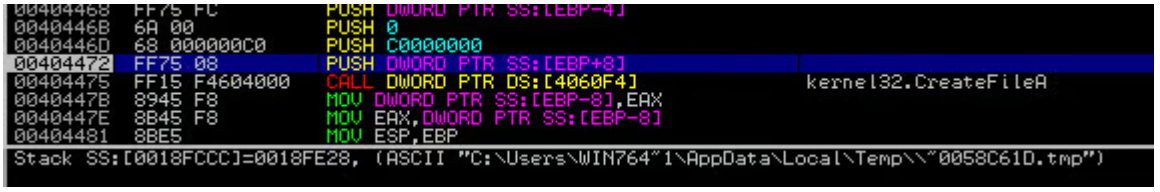
Downloaded Binary

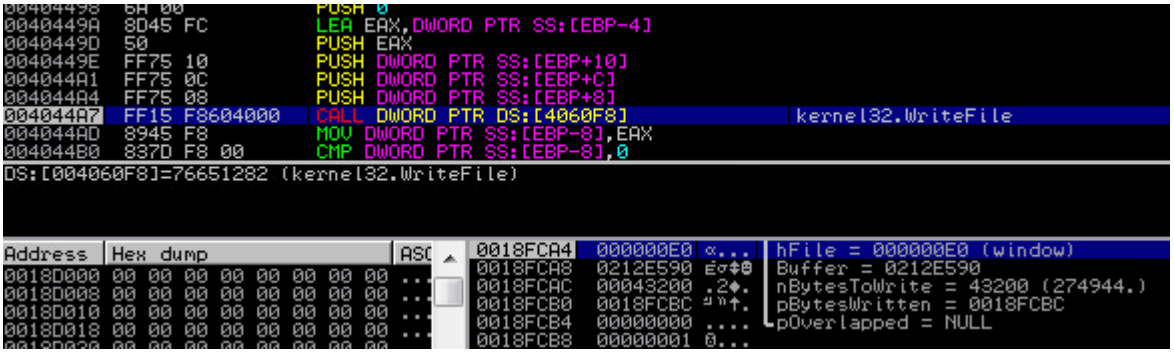
The downloaded binary is a dropper Trojan and is saved as C:\Users\\AppData\Local\Temp__.exe. Chanitor will run the downloaded payload via the following command:

cmd /D /R start /B "" "C:\Users\

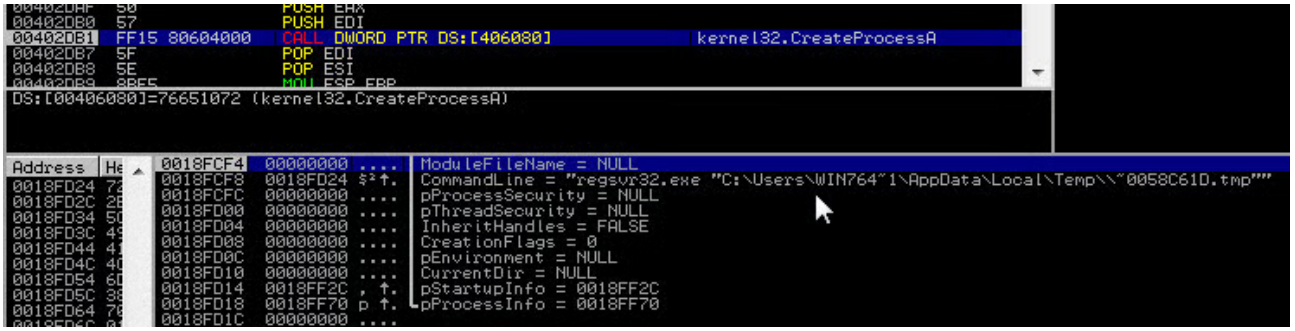
\AppData\Local\Temp___16AE.exe" && exit

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.





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



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:

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://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

abuse@tor2web.org

and at

info@tor2web.org

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.
