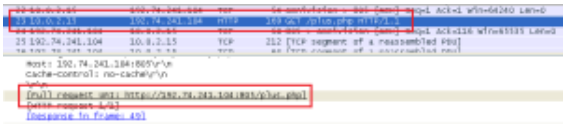
Trojan banking 47d18761d46d8e7c4ad49cc575b0acc2bb3f49bb56a3d29fb1ec600447cb89a4

By Posted by zairon on April 15, 2014

Published: 2014-04-15 · Archived: 2026-04-05 16:11:12 UTC

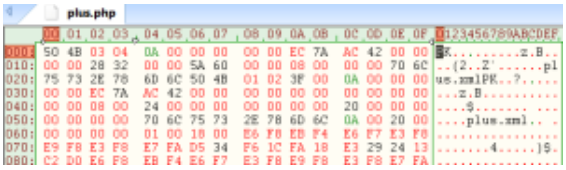
Two days ago I blogged about the approach I used to start analysing the malware, today I spent some more time on the target trying to get an idea of its behaviours. According to VirusTotal the file has a 21/51 revelation rate, it was 6/51 six days ago.
It has been designed for the Asian part of the world and, among all the malicious features, I noted an interesting data exchanges between the infected machine and a server behind 192.74.241.104/192.74.241.105 addresses.

From server to infected machine



Get

File *plus.php* is saved inside the infected machine. Wireshark marks the new file as an “application/zip” file, and I have to admit that at a first glance I thought the same thing:



Misleading header

I was wrong, the file is a not valid archive. To better understand what kind of file is this I put my hands on a debugger. All the bytes starting from offset 0x68 are decrypted by a simple piece of code:

```
10007F10 decrypt_part_of_the_downloaded_file:
10007F10 mov eax, ecx
10007F12 push 2
10007F14 cdq
10007F15 pop edi
10007F16 idiv edi
10007F18 test edx, edx
10007F1A jz short loc_10007F22
10007F1C add byte ptr [ecx+esi], 3Ah
10007F20 jmp short loc_10007F26
10007F22 add byte ptr [ecx+esi], 4Bh
10007F26 inc ecx
```

```
10007F27 cmp ecx, [ebp+var_4]
10007F2A jl short decrypt_part_of_the_downloaded_file
```

It's basically decrypted by an *add* operation, but the result is something I didn't expect, here is a small part of the entire file:

```
126.11.242.224 nAVER.coM
126.11.242.224 kIsA.hoNabenk.coM
126.11.242.224 kIsA.kcB.co.kR
126.11.242.224 kIsA.kfoc.co.kR
126.11.242.224 www.nAVER.co.KR
126.11.242.224 nAVER.cO.kR
126.11.242.224 www.nONGhyup.coM
126.11.242.224 BaNKiNg.nONGhyup.coM
126.11.242.224 iBz.nONGhyup.coM
126.11.242.224 www.nAVER.coM
126.11.242.224 nAVER.kR
```

The file is moved under "*C:\Windows\System32\drivers\etc*" directory with the new name *hosts.ics*. It seems to be the same list described inside three articles by Nshc Security. You can find the mentioned pdf report files inside the Red Alert Reports section:

– Internet Bank Pharming – BlackMoon

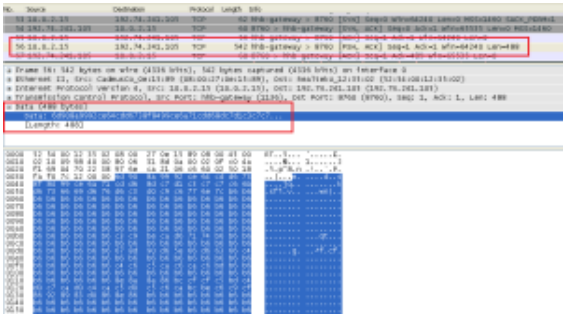
– Internet Bank Pharming with CVE-2013-3897

– Internet Banking Malware

The malware I'm checking has a lot of common things with the samples used to write the reports: it deletes antivirus exe related files, use a link file to run the malware at startup, create the hosts.ics file, steal certificates searching for NPKI folders sending them to a specific server in an encrypted format.

On the other hand the infection has slightly changed: dll file runs from rundll32 camouflaged into ctfmon.exe and not csrss.exe, start link has a different name V2LiteExp (the name comes from AhnLab V3 Internet Security suite), plus.php file is available in the recent samples only. Little things of course, but these are relevant in the removal process.

From infected machine to server



Send

A series of bytes are sent away, what's behind this obscure sequence?

Again, a simple xor encryption is used to hide the real information to send. The message in clear view contains some strings revealing info about the infected machine and the infection itself:

– processor type, something like "Intel(R) Core(TM) i7-3770K CPU @ 3.50GHz"

– physical free memory : "3584 MB"

– running OS: "Win XP SP2"

– date of infection: “20140415”
– location of hosts file: “http://192.74.241.104:805/plus.php”
These information are sent following a precise time line.

192.74.241.104 and 192.74.241.105

These addresses are under “PEG TECH INC” organization. There are many spam related complaints around the web from this organization, pay attention to 192.74.241.96/192.74.241.111 range addresses.
To end this post, look at the advice of a company named PegTech.

Source: https://zairon.wordpress.com/2014/04/15/trojan-banking-47d18761d46d8e7c4ad49cc575b0acc2bb3f49bb56a3d29fb1ec600447cb89a4/