"Crystal Attack" analysis

UPD – behavior analysis of the "load.exe" sample

After execution, "load.exe" is migrating to "explorer.exe" – it creates a process in suspended mode, overwrites the code with malicious code and then executes.

CreateProcessInternalW	thread_handle: 0x000002e8 process_identifier: 3756 current_directory: filepath: track: 1 command_line: explorer.exe filepath_r: creation_flags: 4 (CREATE_SUSPENDED) inherit_handles: 0 process_handle: 0x000002f0

Within the new process it copies the original file from the path:

C:\Users\%user name%\AppData\Roaming\Microsoft\fbufwrbe\siaeesws.exe

After that, it deletes the old file.

Aug. 22, 2017, 4:52 p.m. **CopyFileW**	fail_if_exists: 0 oldfilepath_r: C:\Users\Пользователь\AppData\Local\Temp\load.exe newfilepath_r: C:\Users\Пользователь\AppData\Roaming\Microsoft\fbufwrbe\siaeesws.exe newfilepath: C:\Users\Пользователь\AppData\Roaming\Microsoft\fbufwrbe\siaeesws.exe oldfilepath: C:\Users\Пользователь\AppData\Local\Temp\load.exe
Aug. 22, 2017, 4:52 p.m. **DeleteFileW**	filepath_r: C:\Users\Пользователь\AppData\Local\Temp\load.exe filepath: C:\Users\Пользователь\AppData\Local\Temp\load.exe

Also, malicious sample creates autorun Key in the Registry:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\jack1024

It writes the path to a newly created file to this Registry Key:

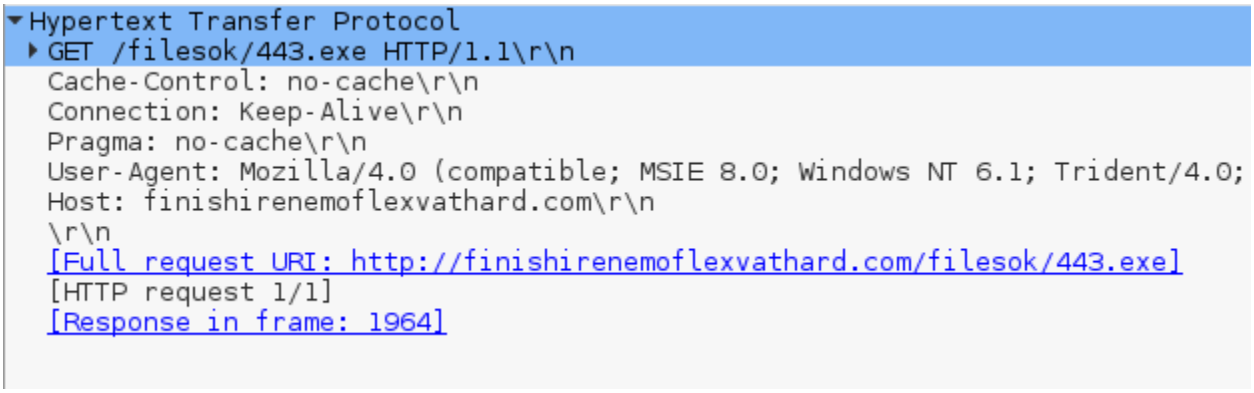
C:\Users\%user_name%\AppData\Roaming\Microsoft\fbufwrbe\siaeesws.exe

RegSetValueExW	regkey_r: jack1024 reg_type: 1 (REG_SZ) value: C:\Users\Пользователь\AppData\Roaming\Microsoft\fbufwrbe\siaeesws.exe regkey: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\jack1024

After, it scans through the list of executed processes. We found the following configuration block in a memory stack of the sample:

procmon_rules=runner.exe|0?2,node.exe|0?3,cb193w.exe|0?4,ifobsclient.exe|0?5,tiny.exe|0?6,mtbclient.exe|0?7,clibankonlineru.exe|0?8,upp_4.exe|0?9,clibankonlineua.exe|0?10,srclbclient.exe|0?11,pionner.exe|0?12,java.exe|0?13,jp2launcher.exe|0?23,javaw.exe|0?24,eximclient.exe|0?25,start.corp2.exe|0?26,|:||:|keylog_rules=start.corp2.exe,node.exe,runner.exe,MTBClient.exe,CliBankOnlineUa.exe,CliBankOnlineRu.exe,CliBank.exe,SRCLBClient.exe,upp_4.exe,tiny.exe,cb193w.exe,bank.exe,jp2launcher.exe,eximclient.exe,javaw.exe|:|

This configuration block has 2 lists of the processes: “procmon_rules” and “keylog_rules”. When it detects files from the “procmon_rules” list, it downloads additional executable file, using HTTP from the following address *http[:]//finishirenemoflexvathard[.]com/filesok/443.exe*



The Domain Name *finishirenemoflexvathard[.]com* had the same IP address as C&C server *kantslerinborisinafrolova[.]ru - 47.88.52.220* at the time of analysis.

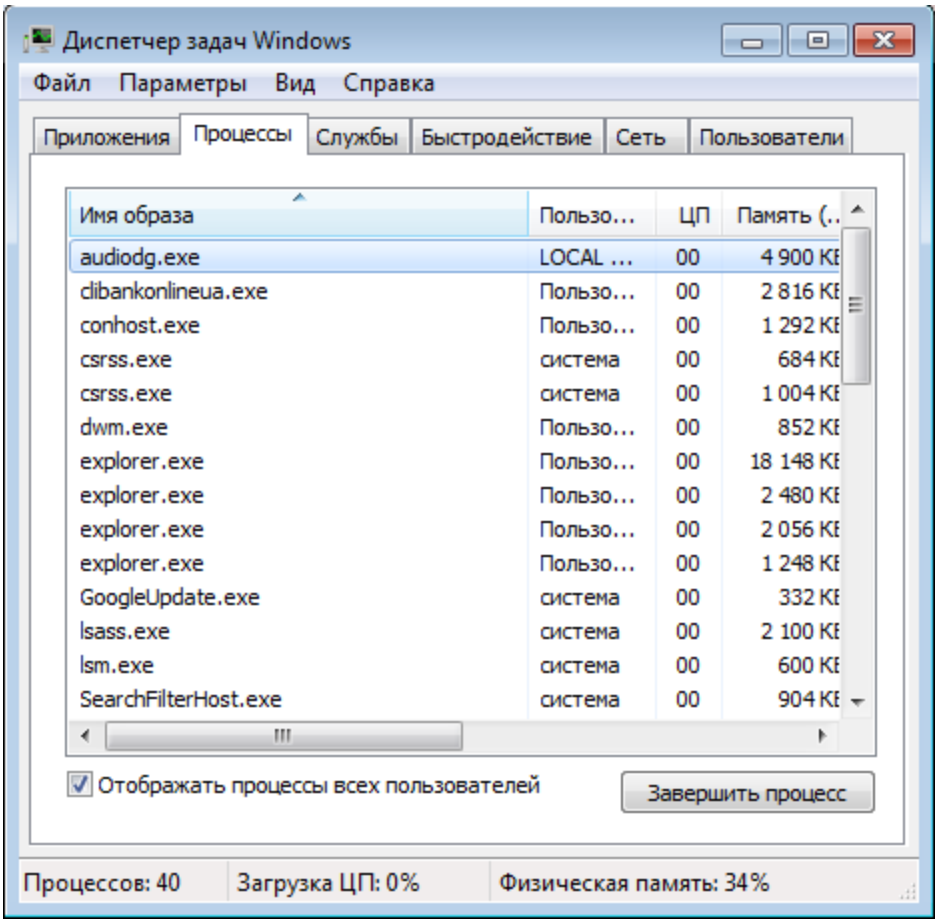
The other list – “keylog_rules” consist of the processes names, for which keylogger should be active.

The sample writes the data to the encrypted file:

C:\Users\%user_name%\AppData\Roaming\Microsoft\fbufwrbe\fbufwrbe

Aug. 22, 2017, 4:55 p.m. **NtCreateFile**	create_disposition: 5 (FILE_OVERWRITE_IF) file_handle: 0x000004b8 filepath: C:\Users\Пользователь\AppData\Roaming\Microsoft\fbufwrbe\fbufwrbe desired_access: 0x40100080 (FILE_READ_ATTRIBUTES|SYNCHRONIZE|GENERIC_WRITE) file_attributes: 128 (FILE_ATTRIBUTE_NORMAL) filepath_r: \??\C:\Users\Пользователь\AppData\Roaming\Microsoft\fbufwrbe\fbufwrbe create_options: 96 (FILE_NON_DIRECTORY_FILE|FILE_SYNCHRONOUS_IO_NONALERT) status_info: 2 (FILE_CREATED) share_access: 2 (FILE_SHARE_WRITE)
Aug. 22, 2017, 4:55 p.m. **NtWriteFile**	buffer: BûÀÏ♂~□2Ü◙□ÇeÐ» 1e□(¯☼◙□×□Î£"$□◄Å?"qm□ÊÀéÈFV!♫5òoG□£¸□♪Ì□□UO/,ö=+j×♀K☊¾ eÍj£ûAP|□]ÉÂ>K¾□ ©õ:ÛE7}\ï□Qõ□+□WQ¾c'□G□á RÕØö¤õD5#□fq□p©ádçk9□Ù§W□¹)ì□ÿ.ôa¹^#@¯Jó□□à½w:+@□):!R:ø³õä;V□êOv□Ù9°□□æùÎ7CýmÊ!□¹□Ì□□OZ×□q*Y7□û{ÁÉÙ ´✓ûóYû½□◄□h□xhíÎPN±SÆÍçm -AXÀ?bø□¾"Ðo*S„h½&Jú[□2Ðfie>)l&ç©Ä4□_eêMÏª4^4´¨□□£□e□□t□□`□□□É□□n□_ Ó►®□·.½2hf±□3|³åöÇ[¥-î_§Õ{ªøP#D□yï³¶úh&□_è»ð□□□S¨ÚíDV|W□Ô□m□coÉ□□Þ·□□çì¢□Ad/

During its operation, the sample creates several running copies of “explorer.exe” processes. We detected 3-4 copies of it on the infected computer.



Another sample – “443.exe” seems to be a remote control system (Backdoor) with additional capabilities.

When launching, it migrates to “svchost.exe” process, replacing its code.

Aug. 23, 2017, 12:06 a.m. **CreateProcessInternalW**	thread_identifier: 2940 thread_handle: 0x00000248 process_identifier: 3536 current_directory: filepath: track: 1 command_line: C:\Windows\system32\svchost.exe -k netsvcs filepath_r: creation_flags: 134217740 (CREATE_NO_WINDOW|CREATE_SUSPENDED|DETACHED_PROCESS) inherit_handles: 0 process_handle: 0x0000024c

It copies the file content to the new file:

C:\Users\%user name%\AppData\Roaming\Microsoft\Windows\dllcache\logagent.exe

Adds itself to Autorun by adding the following values to the Registry:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\logagent
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\logagent
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Control Panel\Desktop\SCRNSAVE.EXE

Also, creates the same Keys in a Registry branch with Local System account parameters:

\REGISTRY\USER\.DEFAULT

Additionally, it creates the shortcut in a autorun directory:

C:\Users\%user name%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\logagent.lnk

Creates the following files in Temporary directory, like:

C:\Users\%user name%\AppData\Local\Temp\tmp3EC8.tmp

Creates additional files in *dllcache* directory:

C:\Users\%user name%\AppData\Roaming\Microsoft\Windows\dllcache\RCX4012.tmp
C:\Users\%user name%\AppData\Roaming\Microsoft\Windows\dllcache\RCX4497.tmp

The sample establishes permanent connection with the adversary's host: *46.20.33.219* port# *666*

Analyzing the behavioristic pattern of the Samples and files being created, we concluded that Samples are similar to **Buhtrap** Malware and particular absolute versions of Trojan.Winlock, Trojan.Inject and others.

Based on the processes list within the Configuration Block, examined malware samples were designed to attack various banking client`s applications.

IOC`s

http[:]//finishirenemoflexvathard[.]com/filesok/443.exe
finishirenemoflexvathard[.]com

47.88.52.220
46.20.33.219

C:\Users\%user_name%\AppData\Roaming\Microsoft\fbufwrbe\siaeesws.exe
C:\Users\%user_name%\AppData\Roaming\Microsoft\fbufwrbe\fbufwrbe
C:\Users\%user_name%\AppData\Roaming\Microsoft\Windows\dllcache\logagent.exe
C:\Users\% user_name%\AppData\Roaming\Microsoft\Windows\dllcache\RCX4012.tmp
C:\Users\% user_name%\AppData\Roaming\Microsoft\Windows\dllcache\RCX4497.tmp
C:\Users\% user_name %\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\logagent.lnk

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\jack1024
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\logagent
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\logagent

Process list, for downloading additional executable

- runner.exe
- node.exe
- cb193w.exe
- ifobsclient.exe
- tiny.exe
- mtbclient.exe
- clibankonlineru.exe
- upp_4.exe
- clibankonlineua.exe
- srclbclient.exe
- pionner.exe
- java.exe
- jp2launcher.exe
- javaw.exe
- eximclient.exe
- start.corp2.exe

Process list for keylogger activation

- start.corp2.exe
- node.exe
- runner.exe
- MTBClient.exe
- CliBankOnlineUa.exe
- CliBankOnlineRu.exe
- CliBank.exe
- SRCLBClient.exe
- upp_4.exe
- tiny.exe
- cb193w.exe
- bank.exe
- jp2launcher.exe
- eximclient.exe
- javaw.exe