LoaderBot.exe

Is DLL ✗ | Packer ✓ | Anti Debug ✗ | Anti VM ✗ | Signed ✗ | XOR ✗

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	16.50 KB (16896 bytes)
Compile time:	2018-01-17 14:35:43
MD5:	d53504fbe4e02806a1d9c931ce4e9585
SHA1:	c4a1f3fecdf073b5a078bc52bb26e5efbf4f5a3c
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-01-17 14:51:03

URL(s) file hosting

http://109.234.36.233/bot/Miner/bin/Release/LoaderBot.exe
http://ih803741.myihor.ru/winhost.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-01-17 13:36:02	27/68	

Import library

mscoree.dll

14 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: Traffico Anomalo: Traffico verso host malevolo, GET HTTP Content ".php" (Soc-Rule)

Attempts to interact with an Alternate Data Stream (ADS)

- file: C:\$Extend\$Quota:$Q:$INDEX_ALLOCATION

Checks the system manufacturer, likely for anti-virtualization

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Webhost
- data: C:\Users\Seven01\AppData\Roaming\Windows\LoaderBot.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Webhost.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Webhost.url
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job
- task: "cmd" /C schtasks /create /tn \System\SecurityServiceUpdate /tr %userprofile%\AppData\Roaming\Windows\LoaderBot.exe /st 00:00 /du 9999:59 /sc daily /ri 5 /f

Attempts to repeatedly call a single API many times in order to delay analysis time

- Spam: services.exe (488) called API GetSystemTimeAsFileTime 2339435 times

Deletes its original binary from disk

Performs some HTTP requests

- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
- url: http://akrt6q.ml/cmd.php?hwid=E4BCC4DD
- url: http://akrt6q.ml/cmd.php?timeout=1

A process created a hidden window

- Process: LoaderBot.exe -> "cmd" /C schtasks /create /tn \System\SecurityServiceUpdate /tr %userprofile%\AppData\Roaming\Windows\LoaderBot.exe /st 00:00 /du 9999:59 /sc daily /ri 5 /f
- Process: LoaderBot.exe -> "cmd" /C schtasks /create /tn \System\SecurityServiceUpdate /tr %userprofile%\AppData\Roaming\Windows\LoaderBot.exe /st 00:00 /du 9999:59 /sc daily /ri 5 /f

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: inetsim.org0

A process attempted to delay the analysis task.

- Process: WmiPrvSE.exe tried to sleep 360 seconds, actually delayed analysis time by 0 seconds
- Process: taskeng.exe tried to sleep 360 seconds, actually delayed analysis time by 0 seconds
- Process: svchost.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds

Possible date expiration check, exits too soon after checking local time

- process: schtasks.exe, PID 2588

Creates RWX memory

Attempts to connect to a dead IP:Port (2 unique times)

- IP: 192.168.56.1:443
- IP: 192.168.56.1:80

At least one process apparently crashed during execution

3 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 67.24.27.254
Port: 80
Count: 1

http://akrt6q.ml/cmd.php?hwid=E4BCC4DD
Hostname: akrt6q.ml
IP Address: 94.142.141.150
Port: 80
Count: 1

http://akrt6q.ml/cmd.php?timeout=1
Hostname: akrt6q.ml
IP Address: 94.142.141.150
Port: 80
Count: 1