BankSlip.exe

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

MalFamily: Ispy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	464.00 KB (475136 bytes)
Compile time:	2017-10-30 15:22:47
MD5:	776cdb53808fd8430d89d16b6c91c490
SHA1:	e24ba42b66c3ce72cade40c6eccfd17edd494ab3
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-10-30 21:09:04

URL(s) file hosting

http://dugunmalzemeleri.org/wp-content/uploads/BankSlip.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-10-30 19:20:50	16/67	

Import library

mscoree.dll

24 Behaviors detected by system signatures

Collects information to fingerprint the system

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Travel
- data: C:\Users\Seven01\AppData\Roaming\Terry\TPO.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\Terry\TPO.exe
- file: C:\Users\Seven01\AppData\Roaming\ScreenShot

Retrieves Windows ProductID, probably to fingerprint the sandbox

Checks the CPU name from registry, possibly for anti-virtualization

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\Terry\TPO.exe

Attempts to disable System Restore

Harvests credentials from local FTP client softwares

- file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentservers.xml
- file: C:\Users\Seven01\AppData\Roaming\SmartFTP\Client 2.0\Favorites\Quick Connect\
- file: C:\Users\Seven01\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini
- key: HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites

Harvests information related to installed instant messenger clients

- file: C:\Users\Seven01\AppData\Roaming\.purple\accounts.xml
- key: HKEY_CURRENT_USER\Software\Paltalk

Harvests information related to installed mail clients

- file: C:\Users\Seven01\AppData\Roaming\Thunderbird\profiles.ini
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676

The sample wrote data to the system hosts file.

- added: 127.0.0.1

Exhibits behavior characteristic of iSpy Keylogger

- C2: 192.168.56.1
- C2: lallahomes.com/api.php
- C2: lallahomes.com/api.php/api.php
- C2: lallahomes.com/api.php/api.php/api.php
- C2: lallahomes.com/api.php/api.php/api.php/api.php

Deletes its original binary from disk

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Roaming\Terry\TPO.exe:Zone.Identifier

Sniffs keystrokes

- SetWindowsHookExW: Process: BankSlip.exe(2432)

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

- Injection: BankSlip.exe(2104) -> BankSlip.exe(2432)

A process attempted to delay the analysis task.

- Process: BankSlip.exe tried to sleep 618 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 301 seconds, actually delayed analysis time by 0 seconds

A process created a hidden window

- Process: explorer.exe -> "cmd"

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Local\Temp\S7g.exe
- binary: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Templates\explorer.exe

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

- get_no_useragent: HTTP traffic contains a GET request with no user-agent header
- suspicious_request: http://checkip.dyndns.org/
- suspicious_request: http://lallahomes.com/api.php

Performs some HTTP requests

- url: http://checkip.dyndns.org/
- url: http://lallahomes.com/api.php

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.98, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0006e000, virtual_size: 0x0006d6a4

Looks up the external IP address

- domain: checkip.dyndns.org

Creates RWX memory

12 HTTP Request(s) detected

http://checkip.dyndns.org/
Hostname: checkip.dyndns.org
IP Address: 91.198.22.70
Port: 80
Count: 1

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 1

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 14

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 1

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 1

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 94

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 1

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 1

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 5

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 1

http://lallahomes.com/api.php

Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 1

http://lallahomes.com/api.php
Hostname: lallahomes.com
IP Address: 51.254.15.108
Port: 80
Count: 1