

okilo.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

**MalFamily: Ispy**

**MalScore: 100**

<b>File type:</b>	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
<b>File size:</b>	240.00 KB (245760 bytes)
<b>Compile time:</b>	2018-03-21 23:13:57
<b>MD5:</b>	2b9ae643a92a909eed70bfa83fc27f6f
<b>SHA1:</b>	dfc03d579aded43750730e8a8a836f72b5ba6849
<b>Import hash:</b>	f34d5f2d4577ed6d9ceec516c1f5a744
<b>Submitted:</b>	2018-03-23 17:00:03

### URL(s) file hosting

<http://lashawnbarber.com/images/files/okilo.exe>

### Antivirus Report

Report date	Detection Ratio	Permalink
2018-03-23 12:06:25	17/67	

### Import library

mscoree.dll

**20**

## Behaviors detected by system signatures

Collects information to fingerprint the system

Exhibits behavior characteristic of iSpy Keylogger



- C2: 192.168.56.1
- C2: okilo.cyber-pk.com/api.php
- C2: okilo.cyber-pk.com/api.php/api.php
- C2: okilo.cyber-pk.com/api.php/api.php/api.php
- C2: okilo.cyber-pk.com/api.php/api.php/api.php/api.php

Installs itself for autorun at Windows startup

- key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\First Data Corp
- data: C:\Users\Seven01\AppData\Local\Temp\First Data Corp\First Data Corp.exe

Creates a hidden or system file

- 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

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\lpswitch\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

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

- Process: okilo.exe tried to sleep 2510 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 421 seconds, actually delayed analysis time by 0 seconds

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Local\Temp\First Data Corp\First Data Corp.exe:Zone.Identifier

Sniffs keystrokes

- SetWindowsHookExW: Process: okilo.exe(2544)

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

- Injection: okilo.exe(2368) -> okilo.exe(2544)

Creates RWX memory

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://okilo.cyber-pk.com/api.php

Performs some HTTP requests

- url: http://checkip.dyndns.org/
- url: http://okilo.cyber-pk.com/api.php

Unconventional language used in binary resources: Divehi

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 6.99, characteristics: IMAGE\_SCN\_CNT\_CODE|IMAGE\_SCN\_MEM\_EXECUTE|IMAGE\_SCN\_MEM\_READ, raw\_size: 0x00036000, virtual\_size: 0x000355e4

Looks up the external IP address

- domain: checkip.dyndns.org

Attempts to connect to a dead IP:Port (1 unique times)

- IP: 192.168.56.1:80

## 13 HTTP Request(s) detected

<http://checkip.dyndns.org/>

Hostname: checkip.dyndns.org

IP Address: 91.198.22.70

Port: 80

Count: 1

<http://okilo.cyber-pk.com/api.php>

Hostname: okilo.cyber-pk.com

IP Address: 185.217.94.157

Port: 80

Count: 9

<http://okilo.cyber-pk.com/api.php>

Hostname: okilo.cyber-pk.com

IP Address: 185.217.94.157

Port: 80

Count: 23

<http://okilo.cyber-pk.com/api.php>

Hostname: okilo.cyber-pk.com

IP Address: 185.217.94.157

Port: 80

Count: 1

<http://okilo.cyber-pk.com/api.php>

Hostname: okilo.cyber-pk.com

IP Address: 185.217.94.157

Port: 80

Count: 1

<http://okilo.cyber-pk.com/api.php>



Hostname: okilo.cyber-pk.com
IP Address: 185.217.94.157
Port: 80
Count: 80

<b>http://okilo.cyber-pk.com/api.php</b>
Hostname: okilo.cyber-pk.com
IP Address: 185.217.94.157
Port: 80
Count: 1

<b>http://okilo.cyber-pk.com/api.php</b>
Hostname: okilo.cyber-pk.com
IP Address: 185.217.94.157
Port: 80
Count: 1

<b>http://okilo.cyber-pk.com/api.php</b>
Hostname: okilo.cyber-pk.com
IP Address: 185.217.94.157
Port: 80
Count: 1

<b>http://okilo.cyber-pk.com/api.php</b>
Hostname: okilo.cyber-pk.com
IP Address: 185.217.94.157
Port: 80
Count: 1

<b>http://okilo.cyber-pk.com/api.php</b>
Hostname: okilo.cyber-pk.com
IP Address: 185.217.94.157
Port: 80
Count: 3

<b>http://okilo.cyber-pk.com/api.php</b>
Hostname: okilo.cyber-pk.com



IP Address: 185.217.94.157
Port: 80
Count: 1

<b><a href="http://okilo.cyber-pk.com/api.php">http://okilo.cyber-pk.com/api.php</a></b>
Hostname: okilo.cyber-pk.com
IP Address: 185.217.94.157
Port: 80
Count: 1