

akp.exe

Is DLL

Packer

Anti Debug

Anti VM

Signed

XOR

MalFamily: Razy

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	280.00 KB (286720 bytes)
Compile time:	2018-07-08 06:20:54
MD5:	16c1238a0b0a66ba81ce61eeb5747570
SHA1:	16609ede5b03d3be00ec4f6c8f3c8cce213562f8
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-07-12 12:33:03

URL(s) file hosting

<http://unitedbnkonline.com/panel/akp.exe>

Antivirus Report

Report date	Detection Ratio	Permalink
2018-07-09 14:36:01	39/68	

Import library

mscoree.dll

17

Behaviors detected by system signatures

Collects information to fingerprint the system

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\9375CFF0413111
d3B88A00104B2A6676
- key:
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111
d3B88A00104B2A6676
```

Harvests information related to installed instant messenger clients

```
- file: C:\Users\Seven01\AppData\Roaming\purple\accounts.xml
```

- key: HKEY_CURRENT_USER\Software\Paltalk

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

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\General Motors Corporation\General Motors Corporation.exe

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

Retrieves Windows ProductID, probably to fingerprint the sandbox

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\General Motors Corporation
- data: C:\Users\Seven01\AppData\Roaming\General Motors Corporation\General Motors Corporation.exe

Sniffs keystrokes

- SetWindowsHookExW: Process: akp.exe(2644)

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Roaming\General Motors Corporation\General Motors Corporation.exe:Zone.Identifier

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

- Injection: akp.exe(2484) -> akp.exe(2644)

Looks up the external IP address

- domain: checkip.dyndns.org

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.96, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00033000, virtual_size: 0x000327b4

Performs some HTTP requests

- url: http://checkip.dyndns.org/
- url: http://unitedbnkonline.com/panel/akp/api.php

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://unitedbnkonline.com/panel/akp/api.php

A process attempted to delay the analysis task.

- Process: akp.exe tried to sleep 1150 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

8

HTTP Request(s) detected



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

Hostname: checkip.dyndns.org

IP Address: 162.88.100.200

Port: 80

Count: 1

<http://unitedbnkonline.com/panel/akp/api.php>

Hostname: unitedbnkonline.com

IP Address: 160.153.128.2

Port: 80

Count: 1

<http://unitedbnkonline.com/panel/akp/api.php>

Hostname: unitedbnkonline.com

IP Address: 160.153.128.2

Port: 80

Count: 5

<http://unitedbnkonline.com/panel/akp/api.php>

Hostname: unitedbnkonline.com

IP Address: 160.153.128.2

Port: 80

Count: 1

<http://unitedbnkonline.com/panel/akp/api.php>

Hostname: unitedbnkonline.com

IP Address: 160.153.128.2

Port: 80

Count: 18

<http://unitedbnkonline.com/panel/akp/api.php>

Hostname: unitedbnkonline.com

IP Address: 160.153.128.2

Port: 80

Count: 1

<http://unitedbnkonline.com/panel/akp/api.php>



Hostname: unitedbnkonline.com
IP Address: 160.153.128.2
Port: 80
Count: 1

http://unitedbnkonline.com/panel/akp/api.php
Hostname: unitedbnkonline.com
IP Address: 160.153.128.2
Port: 80
Count: 1