KDATC.exe

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

MalFamily: Malicious **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	519.55 KB (532016 bytes)
Compile time:	2018-05-29 16:52:53
MD5:	05802c35fefeefc47992d59c053e57e6
SHA1:	b40a62cccebff8098e715ef50a98e46efeeb5453
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-06-01 23:33:05

URL(s) file hosting

http://www.paulocamarao.com/server-log/KDATC.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-06-01 13:38:47	15/65	

Import library

mscoree.dll

21 Behaviors detected by system signatures

Collects information to fingerprint the system

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Roaming\Michaels Stores Inc\Michaels Stores Inc.exe:Zone.Identifier

Sniffs keystrokes

- SetWindowsHookExW: Process: svhost.exe(2600)

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Michaels Stores Inc
- data: C:\Users\Seven01\AppData\Roaming\Michaels Stores Inc\Michaels Stores Inc.exe
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
- data: C:\Users\Seven01\AppData\Local\Temp\FolderN\name.exe.lnk

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Local\Temp\FolderN
- file: C:\Users\Seven01\AppData\Roaming\Michaels Stores Inc\Michaels Stores Inc.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\Local\Temp\FolderN\name.exe

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

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

- Injection: KDATC.exe(2256) -> svhost.exe(2600)

Looks up the external IP address

- domain: checkip.dyndns.org

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.07, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00046000, virtual_size: 0x00045fb8

Creates RWX memory

A process attempted to delay the analysis task.

- Process: svhost.exe tried to sleep 1990 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 304 seconds, actually delayed analysis time by 0 seconds

Reads data out of its own binary image

- self_read: process: KDATC.exe, pid: 2256, offset: 0x00000000, length: 0x00001000
- self_read: process: KDATC.exe, pid: 2256, offset: 0x00000080, length: 0x00000200

A process created a hidden window

- Process: KDATC.exe -> "cmd.exe"

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Local\Temp\svhost.exe

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://checkip.dyndns.org/

Performs some HTTP requests

- url: http://checkip.dyndns.org/

Unconventional language used in binary resources: Korean

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

- IP: 192.168.56.1:587

1 HTTP Request(s) detected

http://checkip.dyndns.org/
Hostname: checkip.dyndns.org
IP Address: 162.88.96.194
Port: 80
Count: 1