hono.exe

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

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	2247.00 KB (2300928 bytes)
Compile time:	2018-05-08 01:25:18
MD5:	5f6adfd8adc46a9195b1ee20d37b3984
SHA1:	3ddb85f46259436e6dfa4eeff2cfb2d92d7f25af
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-18 15:45:03

URL(s) file hosting

http://qualityoflife-lb.com/crypted/hono.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-09 15:45:13	14/67	

Import library

mscoree.dll

25 Behaviors detected by system signatures

Collects information to fingerprint the system

Sniffs keystrokes

- SetWindowsHookExW: Process: kvskvmk.exe(2920)

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

- Spam: services.exe (488) called API GetSystemTimeAsFileTime 534305 times

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\jlcjlcn
- data: cmd /c type C:\Users\Seven01\AppData\Local\Temp\jlcjlcn.txt | cmd
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Coventry Health Care Inc
- data: C:\Users\Seven01\AppData\Local\Temp\Coventry Health Care Inc\Coventry Health Care Inc.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\kvskvmk.exe

Retrieves Windows ProductID, probably to fingerprint the sandbox

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

Checks the system manufacturer, likely for anti-virtualization

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Local\Temp\Coventry Health Care Inc\Coventry Health Care Inc.exe

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

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Local\Temp\Coventry Health Care Inc\Coventry Health Care Inc.exe:Zone.Identifier

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

- Injection: kvskvmk.exe(2672) -> kvskvmk.exe(2920)

Deletes its original binary from disk

Creates RWX memory

Possible date expiration check, exits too soon after checking local time

- process: sppsvc.exe, PID 1212

A process attempted to delay the analysis task.

- Process: kvskvmk.exe tried to sleep 743 seconds, actually delayed analysis time by 0 seconds
- Process: svchost.exe tried to sleep 330 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 361 seconds, actually delayed analysis time by 0 seconds

Reads data out of its own binary image

- self_read: process: Q08.exe, pid: 2764, offset: 0x00000000, length: 0x00001000
- self_read: process: Q08.exe, pid: 2764, offset: 0x00000080, length: 0x00000200
- self_read: process: Q08.exe, pid: 2764, offset: 0x00000178, length: 0x00000200
- self_read: process: Q08.exe, pid: 2764, offset: 0x00001fb8, length: 0x00000200
- self_read: process: Q08.exe, pid: 2764, offset: 0x00001fd4, length: 0x00000200
- self_read: process: Q08.exe, pid: 2384, offset: 0x00000000, length: 0x00001000

- self_read: process: Q08.exe, pid: 2384, offset: 0x00000080, length: 0x00000200
- self_read: process: Q08.exe, pid: 2384, offset: 0x00000178, length: 0x00000200
- self_read: process: Q08.exe, pid: 2384, offset: 0x00001fb8, length: 0x00000200
- self_read: process: Q08.exe, pid: 2384, offset: 0x00001fd4, length: 0x00000200
- self_read: process: Q08.exe, pid: 2964, offset: 0x00000000, length: 0x00001000
- self_read: process: Q08.exe, pid: 2964, offset: 0x00000080, length: 0x00000200
- self_read: process: Q08.exe, pid: 2964, offset: 0x00000178, length: 0x00000200
- self_read: process: Q08.exe, pid: 2964, offset: 0x00001fb8, length: 0x00000200
- self_read: process: Q08.exe, pid: 2964, offset: 0x00001fd4, length: 0x00000200
- self_read: process: Q08.exe, pid: 1828, offset: 0x00000000, length: 0x00001000
- self_read: process: Q08.exe, pid: 1828, offset: 0x00000080, length: 0x00000200
- self_read: process: Q08.exe, pid: 1828, offset: 0x00000178, length: 0x00000200
- self_read: process: Q08.exe, pid: 1828, offset: 0x00001fb8, length: 0x00000200
- self_read: process: Q08.exe, pid: 1828, offset: 0x00001fd4, length: 0x00000200
- self_read: process: Q08.exe, pid: 1772, offset: 0x00000000, length: 0x00001000
- self_read: process: Q08.exe, pid: 1772, offset: 0x00000080, length: 0x00000200
- self_read: process: Q08.exe, pid: 1772, offset: 0x00000178, length: 0x00000200
- self_read: process: Q08.exe, pid: 1772, offset: 0x00001fb8, length: 0x00000200
- self_read: process: Q08.exe, pid: 1772, offset: 0x00001fd4, length: 0x00000200

A process created a hidden window

- Process: hono.exe -> "cmd"
- Process: kvskvmk.exe -> "cmd"

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Local\Temp\Q08.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/

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: 0x000c8e00, virtual_size: 0x000c8d14

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

1 HTTP Request(s) detected

http://checkip.dyndns.org/
Hostname: checkip.dyndns.org
IP Address: 131.186.113.136
Port: 80
Count: 1