a.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:	638.00 KB (653312 bytes)
Compile time:	2016-04-06 16:56:35
MD5:	96485e7338ca6441b3cf3b603949b2b3
SHA1:	ecff355e2e2f57c43cfa4004b5bf4cfa0263d709
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-12-22 12:18:02

URL(s) file hosting

http://193.124.117.153/crypt/a.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-09-16 16:35:33	40/64	

Import library

mscoree.dll

8 Behaviors detected by system signatures

Detects Avast Antivirus through the presence of a library

Steals private information from local Internet browsers

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@agkn[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@nexac[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@tim[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@adscale[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@tapad[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@dpm.demdex[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@tubemogul[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@adform[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@rubiconproject[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@doubleclick[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@abmr[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@creativecdn[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@liverail[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@adnxs[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@ih.adscale[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@demdex[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@exelator[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@atemda[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@casalemedia[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@track.adform[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@rlcdn[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@pixel.rubiconproject[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@quantserve[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@mathtag[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@ru4[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@rfihub[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@openx[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@mythings[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@onetag-sys[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@onetag-sys[2].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@ibillboard[1].txt
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Cookies\seven01@uk-ox-d.openxadexchange[1].txt

Harvests information related to installed mail clients

- 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\POP3 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\9207f3e0a3b11019908b08002b2a56c2
- 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\32a3dc9c400a4b448b60ab7fe553a392\POP3 User
- 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
- 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\f86ed2903a4a11cfb57e524153480001\POP3 User
- 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}\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\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\13dbb0c8aa05101a9bb000aa002fc45a\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec\POP3 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\7760e21103136b47946c9c80fa097f15\POP3 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\7d19c9e894f20d4780a31c9a9f17da11\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\192e64c97bf3a54488a039619c763627\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd4111\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\POP3 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\6a50d9bd87f9a8478751861a1591a6c2\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook

Anomalous binary characteristics

- anomaly: Actual checksum does not match that reported in PE header

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
- post_no_useragent: HTTP traffic contains a POST request with no user-agent header
- ip_hostname: HTTP connection was made to an IP address rather than domain name
- suspicious_request: http://193.124.117.153/api.php?id=1

Performs some HTTP requests

- url: http://193.124.117.153/api.php?id=1

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.52, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0007d800, virtual_size: 0x0007d704
- section: name: D35EFnvG, entropy: 7.54, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x00010a00, virtual_size: 0x00010828

1 HTTP Request(s) detected

http://193.124.117.153/api.php?id=1
Hostname: 193.124.117.153
IP Address:
Port: 80
Count: 1

1 Host(s) detected

IP Address	Hostname	Reverse DNS
193.124.117.153		ptr.ruvds.com.

1 Countr(y|ies) detected

Hosts	Country
1	Russian Federation