94816439312563db982cd038cf77cbc5ef4c7003e3edee86e2b0f99e675ed4ed

Sign in Sign up

54 / 71

Community Score

54/71 security vendors flagged this file as malicious

Reanalyze Similar More

94816439312563db982cd038cf77cbc5ef4c7003e3edee86e…

msimg32.dll

pedll 64bits idle long-sleeps detect-debug-environment

Size 17.00 KB

Last Analysis Date 1 year ago

DLL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 6

Display grouped sandbox reports

C2AE	⚠ 1	0	0	0	0	0
CAPA	⚠ 0	1	0	0	0	0
Zenbox	⚠ 2	5	0	0	0	2

Activity Summary

Download Artifacts Full Reports Help

⚠ 2 Detections
2 MALWARE 1 TROJAN

Mitre Signatures
1 LOW 12 INFO

IDS Rules
NOT FOUND

Sigma Rules
NOT FOUND

Dropped Files
NOT FOUND

Network comms
2 DNS

Behavior Tags
detect-debug-environment idle long-sleeps

Dynamic Analysis Sandbox Detections
⚠ The sandbox Zenbox flags this file as: MALWARE TROJAN

⚠ The sandbox C2AE flags this file as: MALWARE

MITRE ATT&CK Tactics and Techniques
+ Execution TA0002
+ Persistence TA0003
+ Privilege Escalation TA0004
+ Defense Evasion TA0005
+ Discovery TA0007
+ Command and Control TA0011

Capabilities
Open in CAPA explorer

+ Host-Interaction

+ Executable

Network Communication

DNS Resolutions

fp2e7a.wpc.2be4.phicdn.net

+ fp2e7a.wpc.phicdn.net

Memory Pattern Domains

192.168.88.128:23343

Memory Pattern Urls

http://192.168.88.128:23343

http://192.168.88.128:23343/jquery-3.3.2.slim.min.js

Memory Pattern IPs

192.168.88.128

Behavior Similarity Hashes

C2AE	bdf6e36b0e52a3d7631ffb5fed2fea3d
CAPA	d4656e0adc47907618699d38fc575067
Zenbox	2fa0023372d3e1c0d17c02d73915104e

File system actions

Files Opened

C:\Program Files (x86)\Common Files\Oracle\Java\javapath\

C:\Users\user\Desktop\msimg32.dll

C:\Users\user\Desktop\msimg32.dll.123.Manifest

C:\Users\user\Desktop\msimg32.dll.124.Manifest

C:\Users\user\Desktop\msimg32.dll.2.Manifest

C:\Windows\AppPatch\sysmain.sdb

C:\Windows\Globalization\Sorting\sortdefault.nls

C:\Windows\SYSTEM32\AcLayers.dll

C:\Windows\SYSTEM32\IPHLPAPI.DLL

C:\Windows\SYSTEM32\PROPSYS.dll

Files Written

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies

\Device\ConDrv\\Connect

Registry actions

Registry Keys Opened

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings

HKEY_CURRENT_USER\Software

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB9[illegible]2562

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALWAYS_USE_DNS_FOR_SPN_KB3022771

Registry Keys Set

- HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\SystemCertificates\Root\Certificates\0174E68C97DDF1E0EEEA415EA336A163D2B61AFD\Blob
- HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
- HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
- HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\Windows Error Reporting\Debug\StoreLocation

Process and service actions

Shell Commands

- %SANDBOX_DLL_LOADER_AMD64% %SAMPLEPATH% %WORKDIR% 483
- rundll32.exe %SAMPLEPATH%,DllGetClassObject
- rundll32.exe %SAMPLEPATH%,DllMain
- rundll32.exe %SAMPLEPATH%,StartW

Processes Terminated

- %SANDBOX_DLL_LOADER_AMD64% %SAMPLEPATH% %WORKDIR% 483
- %windir%\System32\svchost.exe -k WerSvcGroup
- %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}
- %windir%\system32\WerFault.exe -u -p 2616 -s 92
- %windir%\system32\WerFault.exe -u -p 2700 -s 640
- rundll32.exe %SAMPLEPATH%,DllGetClassObject
- rundll32.exe %SAMPLEPATH%,DllMain
- rundll32.exe %SAMPLEPATH%,StartW
- wmiadap.exe /F /T /R

Processes Tree

- 2616 - %SANDBOX_DLL_LOADER_AMD64% %SAMPLEPATH% %WORKDIR% 483
  - ↳ 2692 - rundll32.exe %SAMPLEPATH%,DllMain
  - ↳ 2700 - rundll32.exe %SAMPLEPATH%,StartW
  - ↳ 2684 - rundll32.exe %SAMPLEPATH%,DllGetClassObject
- 2208 - %windir%\System32\svchost.exe -k WerSvcGroup
  - ↳ 2732 - %windir%\system32\WerFault.exe -u -p 2616 -s 92
  - ↳ 2868 - %windir%\system32\WerFault.exe -u -p 2700 -s 640
- 816 - wmiadap.exe /F /T /R
- 2808 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}
- 2008 - %windir%\system32\wbem\wmiprvse.exe

Synchronization mechanisms & Signals

Mutexes Created

- \Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex
- \Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex

Highlighted actions

{ "c2server" : "http://192.168.88.128:25345/jquery-3.3.2.slim.min.js", "User-Agent" : "User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko\r\n"}