

powersploit.ps1 

malicious

This report is generated from a file or URL submitted to this webservice on December 16th 2022 06:40:35 Threat Score: 100/100 (UTC) AV Detection: 41%

Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1

Labeled as: [Application.HackTool.PowerS...](#)

#backdoor

#empire

#evasive

Report generated by [Falcon Sandbox](#) © Hybrid Analysis

 Overview

 Sample not shared

 Downloads ▼

 External Reports ▼

 Re-analyze

 Post

 Link

 E-Mail

 Looking for file context ... 

 Looking for similar samples ... 

 Report False-Positive

 Request Report Deletion

Incident Response

Risk Assessment

Evasive Found a reference to a WMI query string known to be used for VM detection

MITRE ATT&CK™ Techniques Detection

This report has 23 indicators that were mapped to 15 attack techniques and 8 tactics.

 [View all details](#)

Additional Context

OSINT

External References <https://www.us-cert.gov/ncas/alerts/TA18-074A>
<https://www.us-cert.gov/ncas/alerts/TA17-293A>
<https://twitter.com/cyb3rops/status/921799386962599936>



E_CSV.csv

External User Tags #dragonfly #elfin #energy #indicator #iran #sha1 #sha256 #ssdeep #ta18-074a #type #us-cert #vertekmti #vsoc

Indicators

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

Malicious Indicators 3

External Systems

- Sample was identified as malicious by a large number of Antivirus engines ▼
- Sample was identified as malicious by a trusted Antivirus engine ▼

Pattern Matching

- YARA signature match ▼

Suspicious Indicators 3

Anti-Detection/Stealthyness

- Contains ability to use cryptographic services (API string) ▼

Environment Awareness

- Found a reference to a WMI query string known to be used for VM detection ▼

External Systems




Informative

30

Anti-Reverse Engineering

Creates guarded memory regions (anti-debugging trick to avoid memory dumping) 

Cryptographic Related

Contains ability to decode base64 data (API string) 

Environment Awareness

Calls an API typically used to get product type 

Calls an API typically used to get system version information 

Contains ability to read software policies 

Reads the active computer name 

Reads the cryptographic machine GUID 

Reads the windows installation date 

General

Calls an API typically used to create a directory 

Creates mutants 

Loads the .NET runtime environment 

Overview of unique CLSIDs touched in registry 

Reads configuration files 

Installation/Persistence



Touches files in the Windows directory	▼
Network Related	
Found potential URL in binary/memory	▼
Possibly tries to communicate over SSL connection (HTTPS)	▼
Spyware/Information Retrieval	
Calls an API typically used for taking snapshot of the specified processes	▼
Calls an API typically used to retrieve information about the current system	▼
Calls an API's typically used for searching a directory for a files	▼
Touches files in program files directory	▼
Tries to access non-existent files	▼
System Destruction	
Opens file with deletion access rights	▼
System Security	
Calls an API typically used to enable or disable privileges in the specified access token	▼
Hooks API calls	▼
Queries the display settings of system associated file extensions	▼
Unusual Characteristics	
Drops files inside appdata directory	▼
Found PowerSploit functions used (API string)	▼



Reads information about supported languages



File Details

All Details: ☐ Off

 powersploit.ps1

Filename	powersploit.ps1
Size	11KiB (11360 bytes)
Type	powershell ps
Description	ASCII text
Architecture	WINDOWS
SHA256	f2943f5e45befa52fb12748ca7171d30096e1d4fc3c365561497c618341299d5 

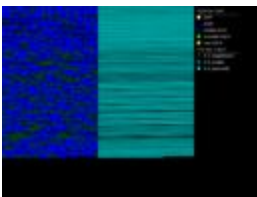
Resources

Icon



Visualization

Input File (PortEx)



Screenshots

 Loading content, please wait...

Hybrid Analysis



Analysed 1 process in total.

powershell.exe "-file" "C:\powersploit.ps1" (PID: 3664)

Logged Script Calls	Logged Stdout	Extracted Streams	Memory Dumps
Reduced Monitoring	Network Activity	Network Error	Multiscan Match

Network Analysis

DNS Requests

No relevant DNS requests were made.

Contacted Hosts

No relevant hosts were contacted.

HTTP Traffic

No relevant HTTP requests were made.

Extracted Strings

Search

All Details: ☐ Off

Download All Memory Strings (4.3KiB)

- All Strings (481)
- Interesting (312)
- powershell.exe (1)
- f2943f5e45befa52fb12748...
- powershell.exe:3664 (320)
- screen_0.png (2)
- screen_1.png (4)

```
"-file" "C:\powersploit.ps1"

#discover potential files containing passwords ; not complaining in case of denied access to a directory

#ensure that machine is domain joined and script is running as a domain account

#Some XML issues between versions
```



```
$AesObject = New-Object System.Security.Cryptography.AesCryptoServiceProvider
$AesObject.Key = $AesKey
$Base64Decoded = [Convert]::FromBase64String($Cpassword)
$Changed += , $Xml | Select-Xml "/DataSources/DataSource/@changed" | Select-Object -Expand Node | ForEach-Object {$_.Value}
$Changed += , $Xml | Select-Xml "/Drives/Drive/@changed" | Select-Object -Expand Node | ForEach-Object {$_.Value}
$Changed += , $Xml | Select-Xml "/Groups/User/@changed" | Select-Object -Expand Node | ForEach-Object {$_.Value}
```

Extracted Files

Informative 1

0K5JSL8CZC9W7ZOFYMK.temp

User Did Not Share

Looking for file context ...

Size	7.8KiB (8016 bytes)
Type	data
Runtime Process	powershell.exe (PID: 3664)
MD5	c11f2e76f895be8d35a468fe84d7fe9f
SHA1	7fc5b6a02e36b2215fd87b90a7201f9eb58fd7a1
SHA256	c2feff9708b7b6fa86d88bd5b4f8e5618fe88143e74ffa2b96a5a0ab20727216

Notifications

Runtime

Environment 1



Community

! There are no community comments.

! You must be logged in to submit a comment.

