The Summary: Malicious PowerShell Execution and Credential Dumping

Crowdstike Incident (or detection) Link:

VMI1146645 at 2023-09-12T07:27:42Z

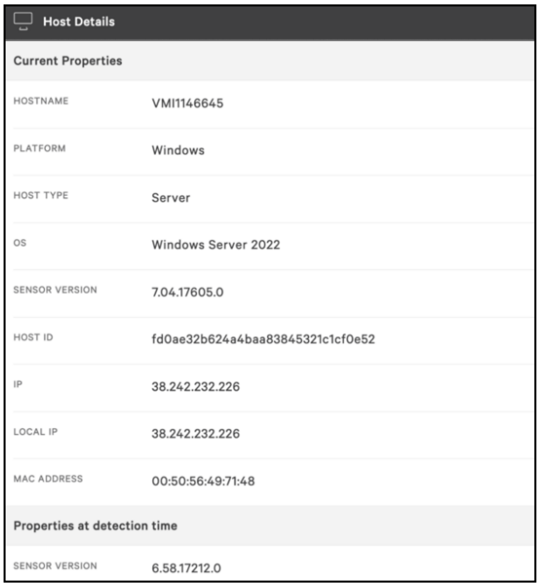
https://falcon.us-2.crowdstrike.com/crowdscore/incidents/details/inc:fd0ae32b624a4baa83845321c1cf0e52:b4c93bd1a35a40e5af84da75cb9cfe8a

Process Tree:

https://falcon.us-2.crowdstrike.com/activity/detections/detail/fd0ae32b624a4baa83845321c1cf0e52/85905108560?pid=275170693264&processView=tree

Description

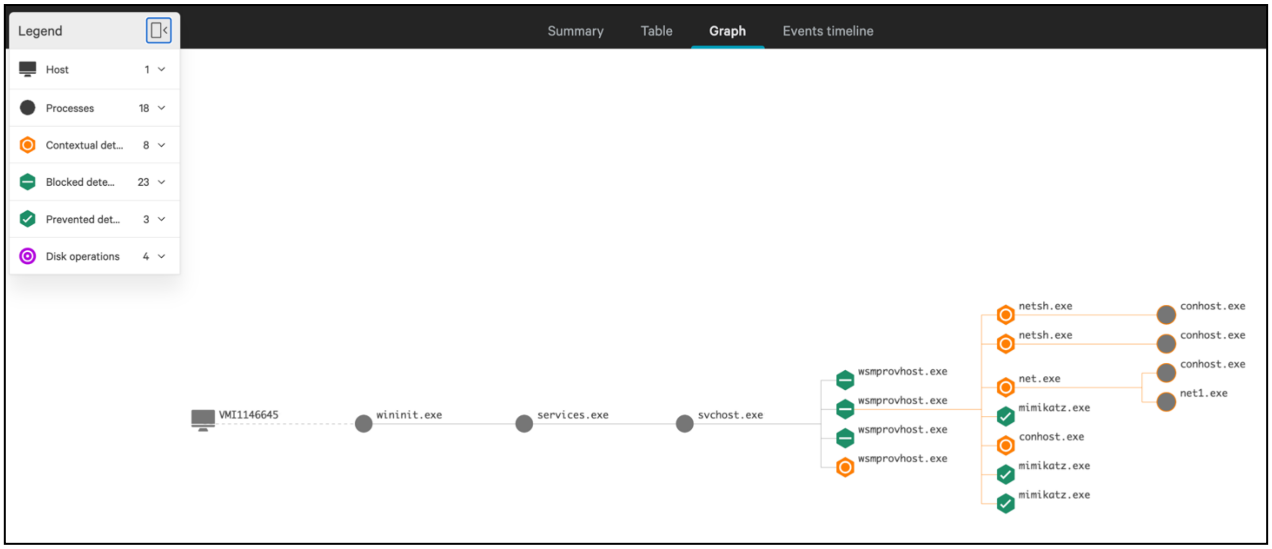
- **Incident name:** VMI1146645 at 2023-09-12T07:27:42Z
- **Victim IP:** 38.242.232.226 (VMI1146645 / OS Windows Server 2022)
- **Objectives in this incident:** Explore, Follow Through, Gain Access, Keep Access, Falcon Detection Method.
- **Techniques:** Windows Remote Management, Command and Scripting Interpreter, PowerShell, OS Credential Dumping, Masquerading, Sensor-based ML.
- **Involved hosts and end users:** VMI1146645, Administrator.



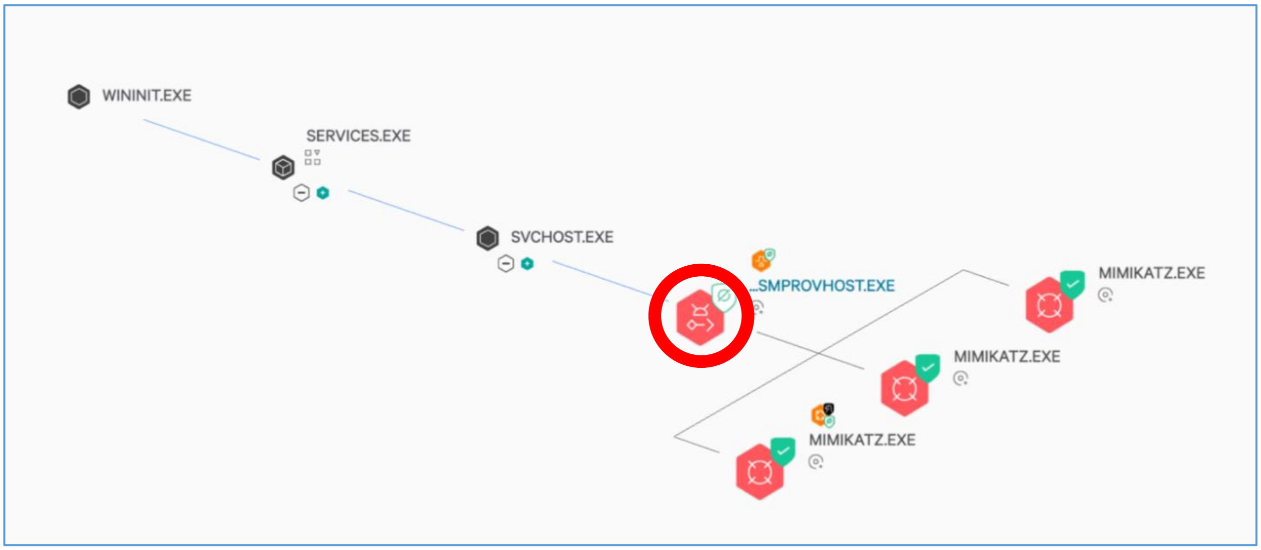
Host Details

Current Properties	
HOSTNAME	VMI1146645
PLATFORM	Windows
HOST TYPE	Server
OS	Windows Server 2022
SENSOR VERSION	7.04.17605.0
HOST ID	fd0ae32b624a4baa83845321c1cf0e52
IP	38.242.232.226
LOCAL IP	38.242.232.226
MAC ADDRESS	00:50:56:49:71:48
Properties at detection time	
SENSOR VERSION	6.58.17212.0

Investigation Findings:

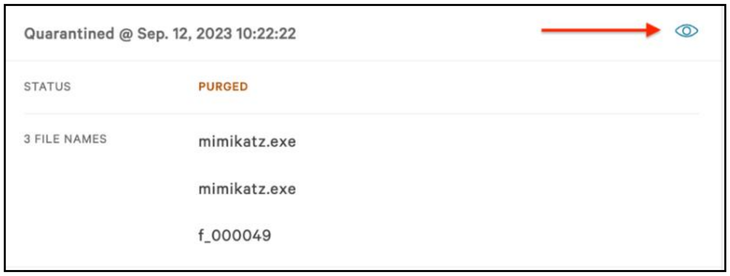


Legend	
Host	1
Processes	18
Contextual det...	8
Blocked dete...	23
Prevented det...	3
Disk operations	4



Analysis: The command "C:\Windows\system32\wsmprovhost.exe -Embedding" which starts execution of the malicious "\??\C:\Users\Administrator\Desktop\winPEAS.ps1" and then execution of "\Device\HarddiskVolume2\Users\Administrator\Desktop\mimikatz.exe" by the user **Administrator** indicates a highly suspicious action. The script, known as Invoke-Mimikatz, is commonly used for credential dumping, which poses a significant security risk.

https://falcon.us-2.crowdstrike.com/activity/detections/detail/fd0ae32b624a4baa83845321c1cf0e52/85905108560?pid=275170693264&processView=tree



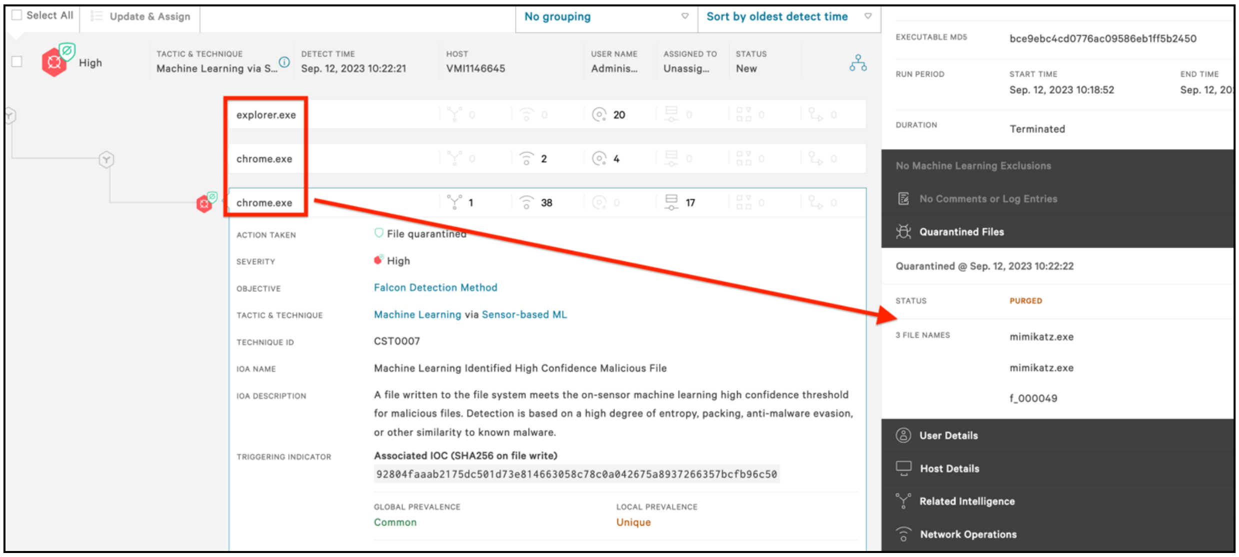
Quarantined @ Sep. 12, 2023 10:22:22

STATUS PURGED

3 FILE NAMES mimikatz.exe
mimikatz.exe
f_000049

https://falcon.us-2.crowdstrike.com/activity/quarantined-files?filter=sha256%3A%20%2792804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50%27%2Bhostname.raw%3A%27VMI1146645%27%2Busername%3A%27Administrator%27

.Observed Files:



	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High	Machine Learning via S...	Sep. 12, 2023 10:22:21	VMI1146645	Adminis...	Unassig...	New

explorer.exe	0	0	20	0	0	0
chrome.exe	0	2	4	0	0	0
chrome.exe	1	38	0	17	0	0

ACTION TAKEN File quarantined

SEVERITY High

OBJECTIVE Falcon Detection Method

TACTIC & TECHNIQUE Machine Learning via Sensor-based ML

TECHNIQUE ID CST0007

IOA NAME Machine Learning Identified High Confidence Malicious File

IOA DESCRIPTION A file written to the file system meets the on-sensor machine learning high confidence threshold for malicious files. Detection is based on a high degree of entropy, packing, anti-malware evasion, or other similarity to known malware.

TRIGGERING INDICATOR Associated IOC (SHA256 on file write)
92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50

GLOBAL PREVALENCE Common

LOCAL PREVALENCE Unique

EXECUTABLE MD5 bce9ebc4cd0776ac09586eb1ff5b2450

RUN PERIOD START TIME Sep. 12, 2023 10:18:52 END TIME Sep. 12, 20

DURATION Terminated

No Machine Learning Exclusions

No Comments or Log Entries

Quarantined Files

Quarantined @ Sep. 12, 2023 10:22:22

STATUS PURGED

3 FILE NAMES mimikatz.exe
mimikatz.exe
f_000049

First Event (Sep. 12, 2023 10:22:21): A cache was created under \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000049 just after ***mimikatz.exe*** was downloaded using chrome browser.

Filename (Executable): ***mimikatz.exe***

Hash - SHA-256:
92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50

FILE PATHS

- \Device\HarddiskVolume2\Users\Administrator\Desktop\mimikatz.exe,
- \Device\HarddiskVolume2\Users\Administrator\Documents\mimikatz.exe,

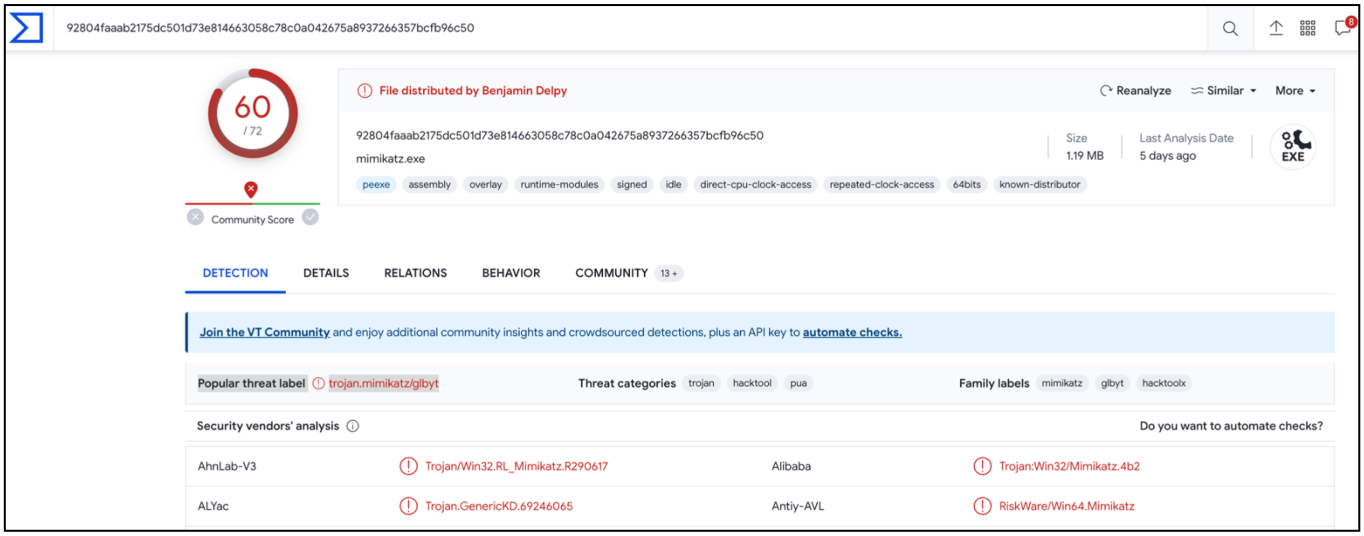
- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000049

Virus Total Result:
https://www.virustotal.com/gui/file/92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50

Brief Community Comments: -
Security Vendors' Analysis from Virus Total: **File distributed by Benjamin Delpy**

Multiple vendors labeled it as malware.
Popular threat label: trojan.mimikatz/glbyt

Other reports:
https://analyze.intezer.com/files/92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50?vt



92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50

60 / 72

File distributed by Benjamin Delpy

92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50
mimikatz.exe

peexe assembly overlay runtime-modules signed idle direct-cpu-clock-access repeated-clock-access 64bits known-distributor

Size 1.19 MB
Last Analysis Date 5 days ago

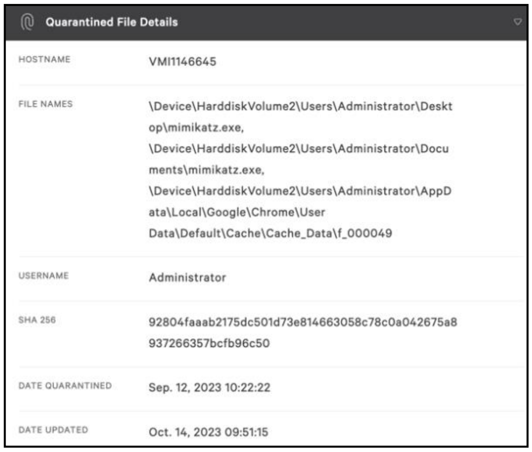
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.mimikatz/glbyt Threat categories trojan hacktool pua Family labels mimikatz glbyt hacktoolx

Security vendors' analysis Do you want to automate checks?

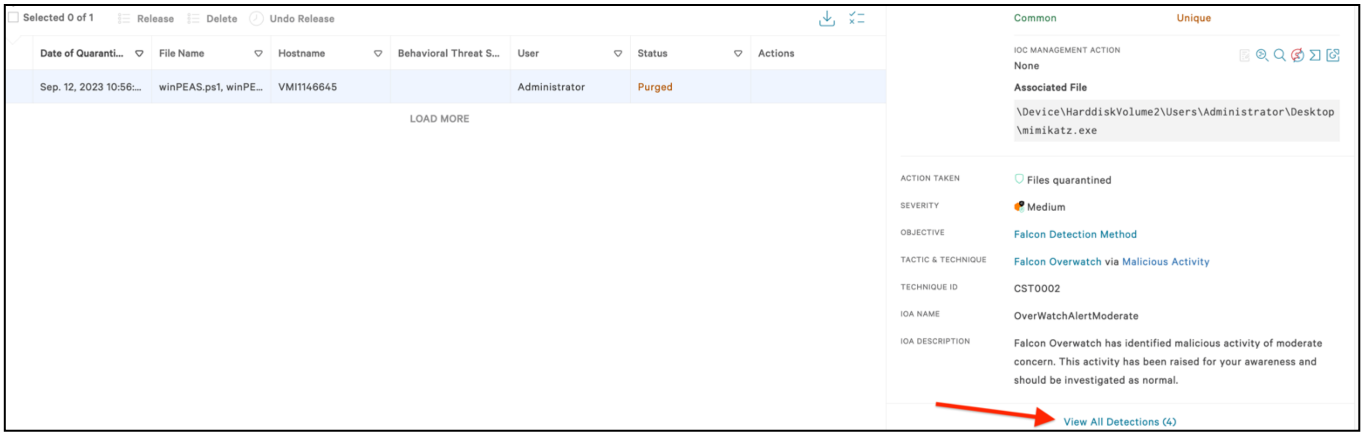
AhnLab-V3	Trojan/Win32.RL_Mimikatz.R290617	Alibaba	Trojan:Win32/Mimikatz.4b2
ALYac	Trojan.GenericKD.69246065	Antiy-AVL	RiskWare/Win64.Mimikatz

ACTIONS TAKEN: All files were quarantined and purged.



Quarantined File Details

HOSTNAME	VMI1146645
FILE NAMES	\Device\HarddiskVolume2\Users\Administrator\Desktop\mimikatz.exe, \Device\HarddiskVolume2\Users\Administrator\Documents\mimikatz.exe, \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000049
USERNAME	Administrator
SHA 256	92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50
DATE QUARANTINED	Sep. 12, 2023 10:22:22
DATE UPDATED	Oct. 14, 2023 09:51:15



Date of Quaranti...	File Name	Hostname	Behavioral Threat S...	User	Status	Actions
Sep. 12, 2023 10:56:...	winPEAS.ps1, winPE...	VMI1146645		Administrator	Purged	

IOC MANAGEMENT ACTION
None

Associated File

```
\Device\HarddiskVolume2\Users\Administrator\Desktop
\mimikatz.exe
```

ACTION TAKEN	Files quarantined
SEVERITY	Medium
OBJECTIVE	Falcon Detection Method
TACTIC & TECHNIQUE	Falcon Overwatch via Malicious Activity
TECHNIQUE ID	CST0002
IOA NAME	OverWatchAlertModerate
IOA DESCRIPTION	Falcon Overwatch has identified malicious activity of moderate concern. This activity has been raised for your awareness and should be investigated as normal.

Go to this link to view all detections related to the mimikatz.exe and cache: https://falcon.us-2.crowdstrike.com/activity/detections/?filter=quarantined_file_hash%3A%2792804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50%27&groupBy=none

COMMAND LINE for downloading mimikatz.exe:

-
  ```
  "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=de --service-sandbox-type=none --mojo-platform-channel-handle=2084 --field-trial-handle=1920,i,9084043800257210304,2273113495787540303,262144 /prefetch:8
  ```

Disk Operations:

explorer.exe:

\Device\HarddiskVolume2\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\de10ae21bb262728c616a707f90aa05088c9d8f2b810fc0f2fb1bddcf9aba938.zip.lnk

\Device\HarddiskVolume2\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\cffa16329e13d62acf61bc633131673dd876a04ed8dd76d178fa98a87e2ee2bb.zip.lnk

\Device\HarddiskVolume2\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk

\Device\HarddiskVolume2\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\88b7aa1440c142faa404021ffe25eb4cf1bf7d4b2b7979c7ffdc98014961aadf.xlsx.lnk

chrome.exe:

\Device\HarddiskVolume2\Windows\SystemTemp\chrome_PuffinComponentUnpacker_BeginUnzipping9504_557610398\page_embed_script.js

\Device\HarddiskVolume2\Windows\SystemTemp\chrome_PuffinComponentUnpacker_BeginUnzipping9504_1612496392\Google.Widevine.CDM.dll

\Device\HarddiskVolume2\Windows\SystemTemp\chrome_PuffinComponentUnpacker_BeginUnzipping9504_1612496392\Google.Widevine.CDM.dll

.Observed Network connections and IP Analysis (for downloading mimikatz.exe)

https://falcon.us-2.crowdstrike.com/activity/detections/?filter=quarantined_file_hash%3A%2792804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50%27&groupBy=none

Chrome connection with the IP: 239.255.255.250 (Phishing Attachment IOC). This IP address might be related with downloading mimikatz.exe to the server. Should be blocked immediately.

IP: 239.255.255.250 (Phishing Attachment IOC - Multicast)

User Agent: -

Browser Name: -

Browser Version: -

OS: -

Analyst Investigation Results:

Virus Total Result: [here|https://www.virustotal.com/gui/ip-address/239.255.255.250]

Brief Community Comments: "ET MALWARE Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)"
"I added the IP 239.255.255.250 to the user defined IOCs and got a couple thousand alerts from the workstations. Apparently it is a UPnP multicast address"

Security Vendors' Analysis from Virus Total: 3 security vendors flagged this IP address as malicious

Talos Intelligence:
REPUTATION DETAILS:
IP Reputation: **Neutral**
Web Reputation: **Unknown**
BLOCK LISTS:
BL.SPAMCOP.NET: **-**
CBL.ABUSEAT.ORG: **-**
PBL.SPAMHAUS.ORG: **-**
SBL.SPAMHAUS.ORG: **-**

Shodan Result: [here|https://www.shodan.io/search?query=239.255.255.250]
Open Ports: 1900, 1723, 520, 20087, 3001

Other reports:

https://blogs.vmware.com/security/2023/11/jupyter-rising-an-update-on-jupyter-infostealer.html#:~:text=netconn_ipv4%3A146.70.101.83%20OR-,239.255.255.250,-OR%20224.0.0.251%20OR

https://blogs.vmware.com/security/2023/11/jupyter-rising-an-update-on-jupyter-infostealer.html

++++++++++++++++++++++++++++++

Second Event (Sep. 12, 2023 10:53:42): wsmprovhost.exe was executed.

File Name: wsmprovhost.exe

Hash - SHA-256:
36f5a0512ff6a9717720fd11b160c88e43cd7a58370a75599a2f9b209ce542d0

Command Line: C:\Windows\system32\wsmprovhost.exe -Embedding

File Path: \Device\HarddiskVolume2\Windows\System32\wsmprovhost.exe

- **wsmprovhost.exe** is likely legitimate and related to Windows Management Instrumentation (WMI) providers. However, it was exploited to run **winPEAS.ps1** script to initiate **mimikatz** attack in the incident.
- The wsmprovhost.exe process is critical and linked to remote sessions in Windows (Remote Desktop Connection).

- The *wsmprovhost.exe* process indicates that a **Windows Remote PowerShell** session is active and generally appears when entering a remote session. The process is created on the server, and more such are added when you run other processes in the remote session.
    - https://windowsreport.com/wsmprovhost-exe/
    - https://windowsreport.com/remote-desktop-connection-windows-10/
    - Possible Misuse: https://strontic.github.io/xcyclopedia/library/wsmprovhost.exe-7FF8C32DD798BAB05FA7B271C09153CA.html
- *-Embedding* switch is often used with COM (Component Object Model) objects to indicate that the program should be run in a mode where it can be controlled by another program.

Objective: Gain Access

Possible Misuse: https://strontic.github.io/xcyclopedia/library/wsmprovhost.exe-7FF8C32DD798BAB05FA7B271C09153CA.html#possible-misuse:~:text=All%20rights%20reserved.-,Possible%20Misuse,-Permalink

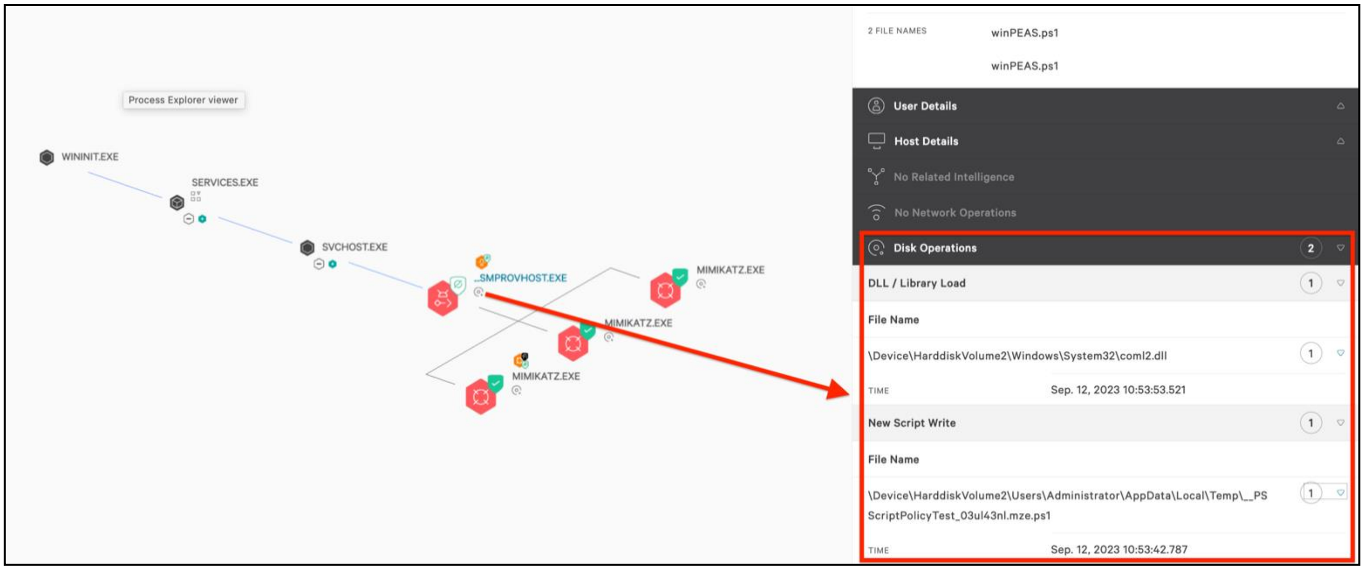
Virus Total Result: https://www.virustotal.com/gui/file/36f5a0512ff6a9717720fd11b160c88e43cd7a58370a75599a2f9b209ce542d0/detection

Brief Community Comments: -
Security Vendors' Analysis from Virus Total: **File distributed by Microsoft**

Popular threat label: -

ACTIONS TAKEN: Operation blocked, Files quarantined

Disk Operations:



2 FILE NAMES winPEAS.ps1

winPEAS.ps1

User Details

Host Details

No Related Intelligence

No Network Operations

Disk Operations 2

DLL / Library Load 1

File Name

\Device\HarddiskVolume2\Windows\System32\coml2.dll 1

TIME Sep. 12, 2023 10:53:53.521

New Script Write 1

File Name

\Device\HarddiskVolume2\Users\Administrator\AppData\Local\Temp\__PSScriptPolicyTest_03ul43nl.mze.ps1 1

TIME Sep. 12, 2023 10:53:42.787

- \Device\HarddiskVolume2\Users\Administrator\Desktop\mimikatz.exe
- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Temp\__PSScriptPolicyTest_4rs0xa4d.j4j.ps1
- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Temp\__PSScriptPolicyTest_03ul43nl.mze.ps1
- \Device\HarddiskVolume2\Windows\System32\coml2.dll
- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Temp\__PSScriptPolicyTest_pu5yy4b0.u0g.ps1
- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Temp\__PSScriptPolicyTest_03ul43nl.mze.ps1
- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Temp\__PSScriptPolicyTest_su1gf442.2md.ps1

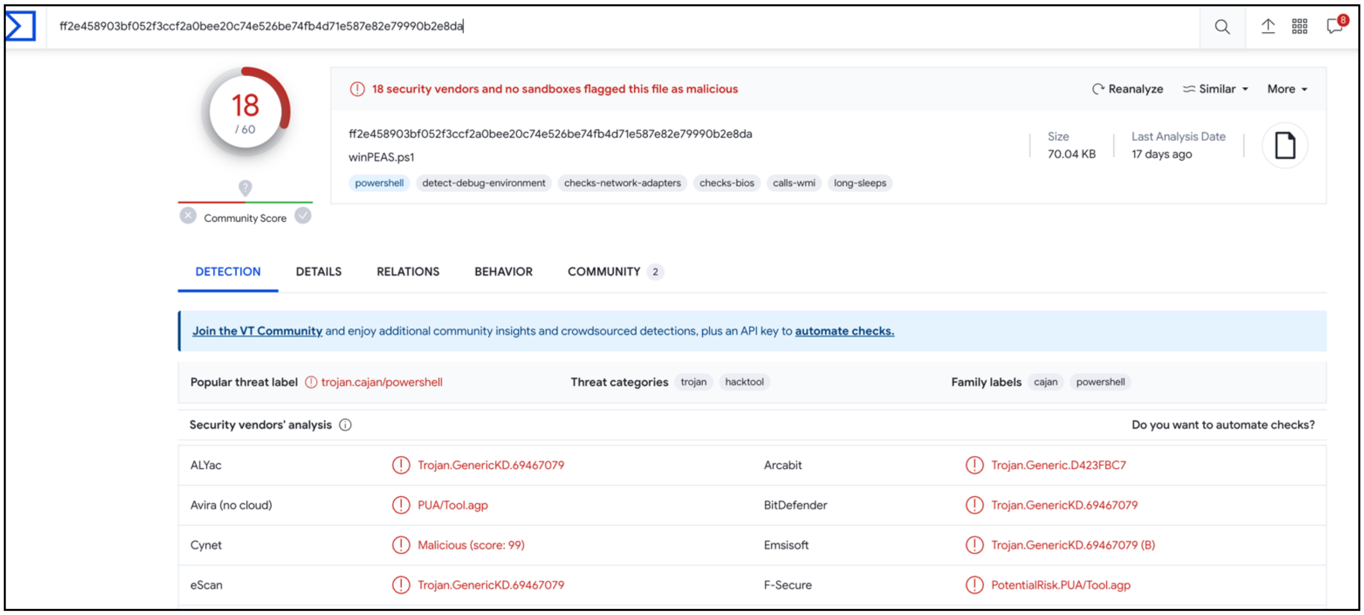
++++++++++++++++++++++++++++++++

Third Event (Sep. 12, 2023 10:53:53):
\??\C:\Users\Administrator\**Desktop****winPEAS.ps1** and \??\C:\Users\Administrator\**Documents****winPEAS.ps1** were executed just after the attacker connected to server VMI1146645 via RDP with **wsmprovhost.exe**.

Filename: winPEAS.ps1
Hash - SHA-256:
ff2e458903bf052f3ccf2a0bee20c74e526be74fb4d71e587e82e79990b2e8da

Virus Total Result:
https://www.virustotal.com/gui/file/ff2e458903bf052f3ccf2a0bee20c74e526be74fb4d71e587e82e79990b2e8da
Brief Community Comments: -
Security Vendors' Analysis from Virus Total: 18 security vendors and no sandboxes flagged this file as malicious

Popular threat label: trojan.cajan/powershell



ff2e458903bf052f3ccf2a0bee20c74e526be74fb4d71e587e82e79990b2e8da

18 / 60

Community Score

18 security vendors and no sandboxes flagged this file as malicious

ff2e458903bf052f3ccf2a0bee20c74e526be74fb4d71e587e82e79990b2e8da

winPEAS.ps1

powershell detect-debug-environment checks-network-adapters checks-bios calls-wmi long-sleeps

Size 70.04 KB

Last Analysis Date 17 days ago

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

Popular threat label trojan.cajan/powershell

Threat categories trojan hacktool

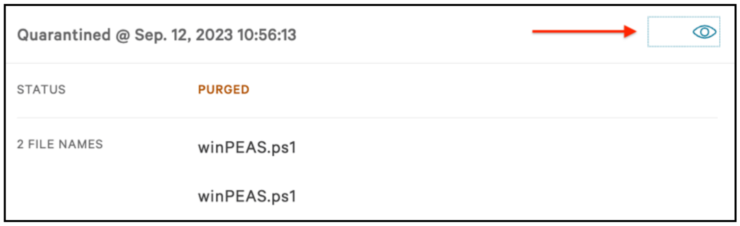
Family labels cajan powershell

Security vendors' analysis

Do you want to automate checks?

ALYac	Trojan.GenericKD.69467079	Arcabit	Trojan.Generic.D423FBC7
Avira (no cloud)	PUA/Tool.agp	BitDefender	Trojan.GenericKD.69467079
Cynet	Malicious (score: 99)	Emsisoft	Trojan.GenericKD.69467079 (B)
eScan	Trojan.GenericKD.69467079	F-Secure	PotentialRisk.PUA/Tool.agp

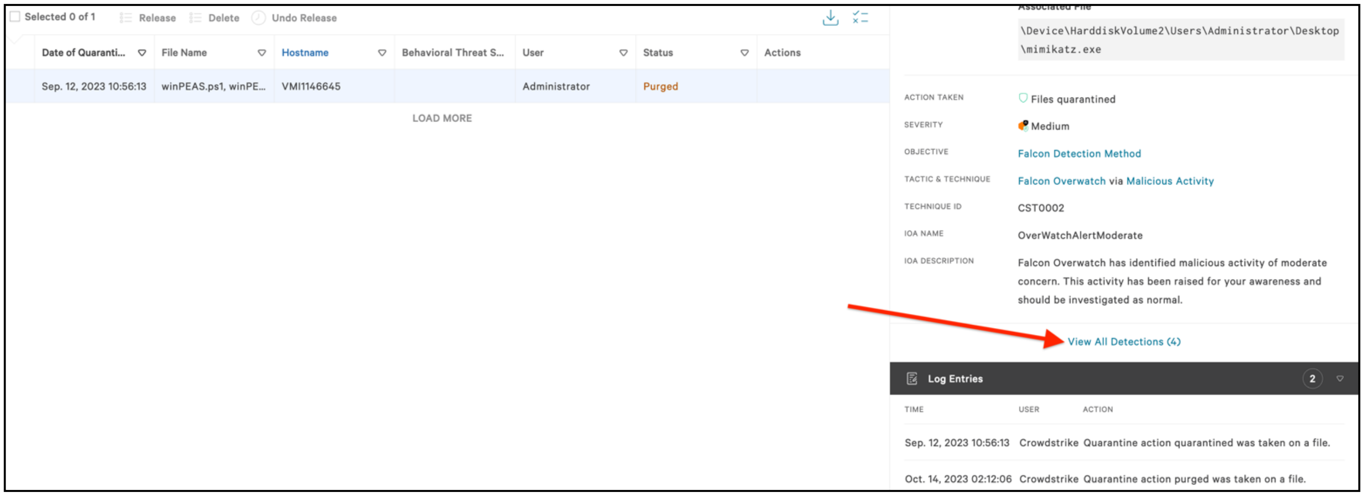
⇒ From the Crowdstrike, go to Quarantined file winPEAS.ps1:



Quarantined @ Sep. 12, 2023 10:56:13

STATUS	PURGED
2 FILE NAMES	winPEAS.ps1 winPEAS.ps1

https://falcon.us-2.crowdstrike.com/activity/quarantined-files?filter=sha256%3A%20%27ff2e458903bf052f3ccf2a0bee20c74e526be74fb4d71e587e82e79990b2e8da%27%2Bhostname.raw%3A%27VMI1146645%27%2Busername%3A%27Administrator%27



Date of Quaranti...	File Name	Hostname	Behavioral Threat S...	User	Status	Actions
Sep. 12, 2023 10:56:13	winPEAS.ps1, winPE...	VMI146645		Administrator	Purged	

Associated File

```
\Device\HarddiskVolume2\Users\Administrator\Desktop
\mimikatz.exe
```

ACTION TAKEN	Files quarantined
SEVERITY	Medium
OBJECTIVE	Falcon Detection Method
TACTIC & TECHNIQUE	Falcon Overwatch via Malicious Activity
TECHNIQUE ID	CST0002
IOA NAME	OverWatchAlertModerate
IOA DESCRIPTION	Falcon Overwatch has identified malicious activity of moderate concern. This activity has been raised for your awareness and should be investigated as normal.

TIME	USER	ACTION
Sep. 12, 2023 10:56:13	Crowdstrike	Quarantine action quarantined was taken on a file.
Oct. 14, 2023 02:12:06	Crowdstrike	Quarantine action purged was taken on a file.

Go to that link https://falcon.us-2.crowdstrike.com/activity/detections/?filter=quarantined_file_hash%3A%27ff2e458903bf052f3ccf2a0bee20c74e526be74fb4d71e587e82e79990b2e8da%27&groupBy=none to view all the detections related with **winPEAS.ps1.**

Description: The PowerShell script **winPEAS.ps1** appears to be launching \Device\HarddiskVolume2\Users\Administrator\Desktop\mimikatz.exe and \Device\HarddiskVolume2\Users\Administrator\Documents\mimikatz.exe, a password dumping utility.

Capabilities of winPEAS.ps1 malicious powershell script file: Windows Privilege Escalation (Privilege Escalation (PrivEsc) in Windows is a process that get the Administrator credential and login.)

Source Code of winPEAS.ps1: https://github.com/carlospolop/PEASS-ng/blob/master/winPEAS/winPEASps1/winPEAS.ps1

ACTIONS TAKEN: Operation blocked, Files (**winPEAS.ps1**) quarantined

Disk Operations:

\Device\HarddiskVolume2\Windows\System32\ntdll.dll

\Device\HarddiskVolume2\Users\Administrator\Desktop\mimikatz.exe

+++++++++++++++++++++++++++

Fourth Event (Sep. 12, 2023 10:59:23): net.exe executable file, which is normally a legitimate file in Windows to deal with accounts, was executed suspiciously and it might be related with *Lateral Movement via Windows Remote Management*

Command Line: `"C:\Windows\system32\net.exe" user /domain`

Filename: net.exe

Hash - SHA-256:
f540747022e0d67722989765b5db268707e4e71538ae0764110eec7b8d9aeef6

+++++++++++++++++++++++++++++++

Fifth Event (Sep. 12, 2023 11:03:34): A suspicious executable file was executed after the incident.

Command Line: `\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1`

Filename: conhost.exe

Hash - SHA-256:
1169576411670c9305b921d2c2c1500ebbae0158fb9cc3e43a5042237a3d00d9
Virus Total Result:
https://www.virustotal.com/gui/file/1169576411670c9305b921d2c2c1500ebbae0158fb9cc3e43a5042237a3d00d9/community
Brief Community Comments: -
Security Vendors' Analysis from Virus Total: **51 security vendors and 1 sandbox flagged this file as malicious**
SRC URL reported to urlhaus.abuse.ch #malicious
Popular threat label: trojan.dloadr/xmrminer

https://any.run/report/1169576411670c9305b921d2c2c1500ebbae0158fb9cc3e43a5042237a3d00d9/4eb598a7-03b8-4c74-8826-afba114c03d7

https://answers.microsoft.com/en-us/windows/forum/all/im-experiencing-random-high-cpu-usage-up-to-30-by/be7fb2f9-a742-4352-baf7-f4771cd717e6

https://answers.microsoft.com/en-us/windows/forum/all/suspicious-conhostexe/a7842ec3-3e17-4ad5-93d4-cf80262ccfb5

++++++++++++++++++++++++++++

.Observed Suspicious DNS Activity:

Domain: bazaar.abuse.ch
Virus Total Result: [here|https://www.virustotal.com/gui/domain/bazaar.abuse.ch]
Brief Community Comments: MalwareBazaar is a site for sharing malware samples with the community. It is safe to visit, but be careful when downloading malware samples.
Security Vendors' Analysis from Virus Total: **1 security vendor flagged this domain as malicious**

.Observed Registry Operations: There is no registry operations.

.Impact Assessment: The potential impact of this activity includes unauthorized access to sensitive credentials, potential compromise of user accounts, and a higher risk of lateral movement.

.Responses: The execution of the command "C:\Windows\system32\wsmprovhost.exe -Embedding" and "\??\C:\Users\Administrator\Desktop\winPEAS.ps1" have been blocked and files were quarantined, however the command "\Device\HarddiskVolume2\Users\Administrator\Desktop\mimikatz.exe" by the user **Administrator** has been executed followed by being blocked and the file was quarantined.

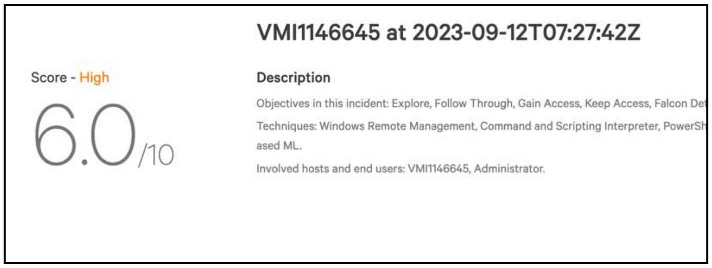
The final command `\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1` was executed. This process "meets the machine learning-based on-sensor AV protection's high confidence threshold for malicious files". And there is no sign of blocking or quarantining action from the Crowdstrike.

+++++++++++++++++++++++++

Recommended Actions:

a. **Contain** affected endpoint VMI1146645
b. **Isolate** affected endpoint from the network to prevent further potential harm and lateral movement infections**.**
c. **Patch** the OS with the latest version.
d. **Restore** the server from clean backups.
e. The server should be **fully scanned**.
f. Apply **performance testing** to verify there is no high usage of CPU and other resources in the machine due to malware artifacts.
g. **Reset/Lock** the account Administrator
h. **Check the exploitable file** \Device\HarddiskVolume2\Windows\System32\wsmprovhost.exe against vulnerabilities. **Removing** wsmprovhost.exe and then configuring the host for allowing only VPN or SSH remote connections could be a proper option.
i. Check out any **spam emails** against phishing attacks.
j. **Educate** users on identifying phishing attempts.
k. **Block** the malicious multicast IP address 239.255.255.250. Also block any multicast traffic to or from the server.

Ticket Priority:



VMI1146645 at 2023-09-12T07:27:42Z

Score - High

6.0/10

Description

Objectives in this incident: Explore, Follow Through, Gain Access, Keep Access, Falcon Det

Techniques: Windows Remote Management, Command and Scripting Interpreter, PowerSh
ased ML.

Involved hosts and end users: VMI1146645, Administrator.

7. Assigned Analyst: Medrkmostafaei (L1 SOC Analyst)