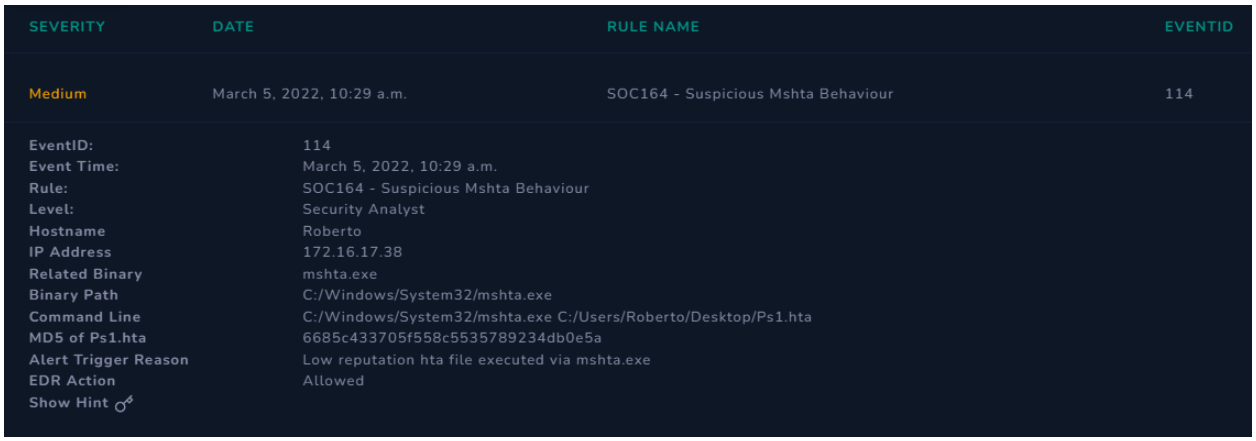
Official Write-Up

Event ID: 114

Rule Name: SOC164 - Suspicious Mshta Behavior

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

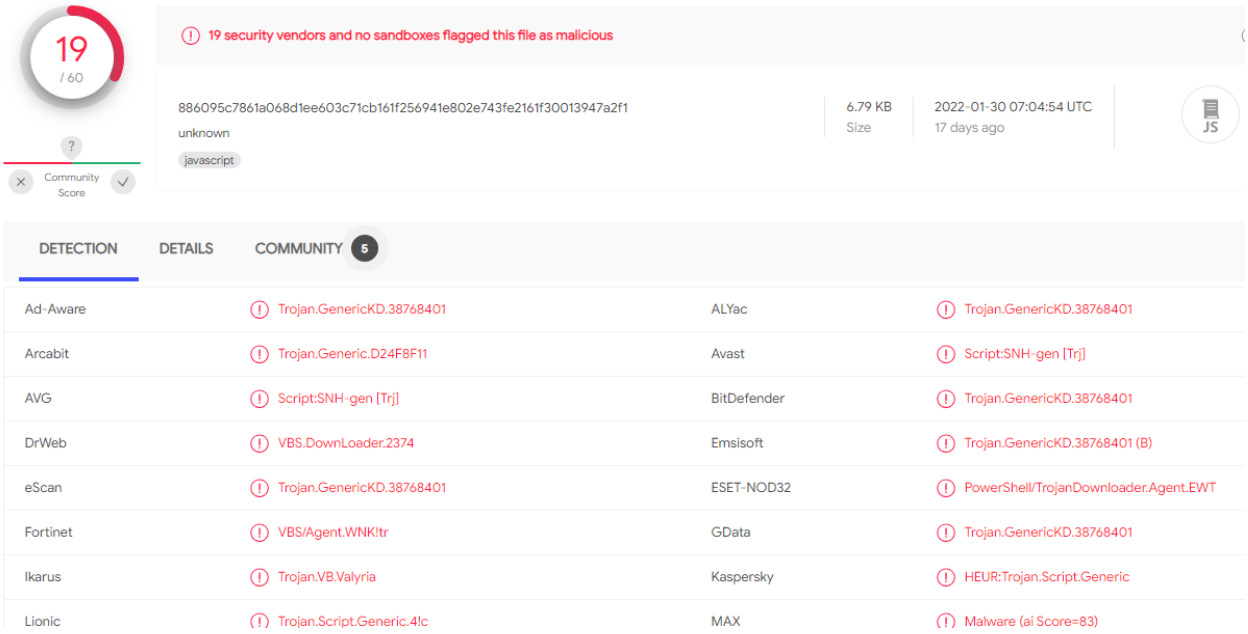
EventID:	114
Event Time:	March 5, 2022, 10:29 a.m.
Rule:	SOC164 - Suspicious Mshta Behaviour
Level:	Security Analyst
Hostname	Roberto
IP Address	172.16.17.38
Related Binary	mshta.exe
Binary Path	C:/Windows/System32/mshta.exe
Command Line	C:/Windows/System32/mshta.exe C:/Users/Roberto/Desktop/Ps1.hta
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

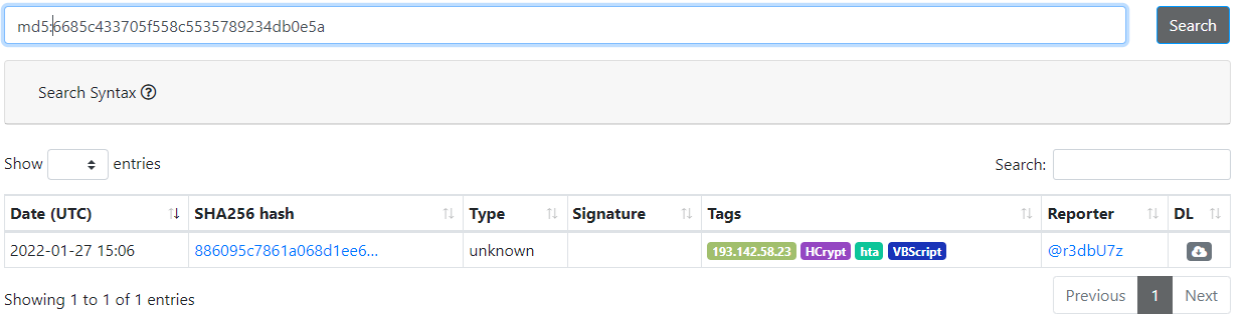
Suspicious File

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.



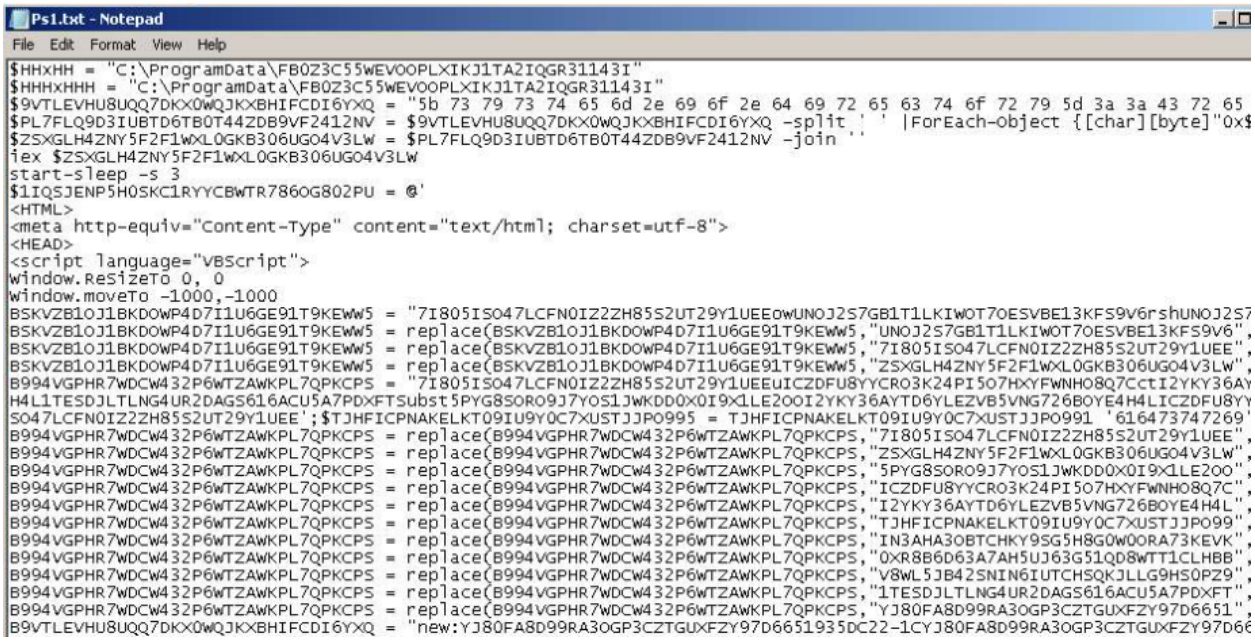
https://www.virustotal.com/gui/file/886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1/detection

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.



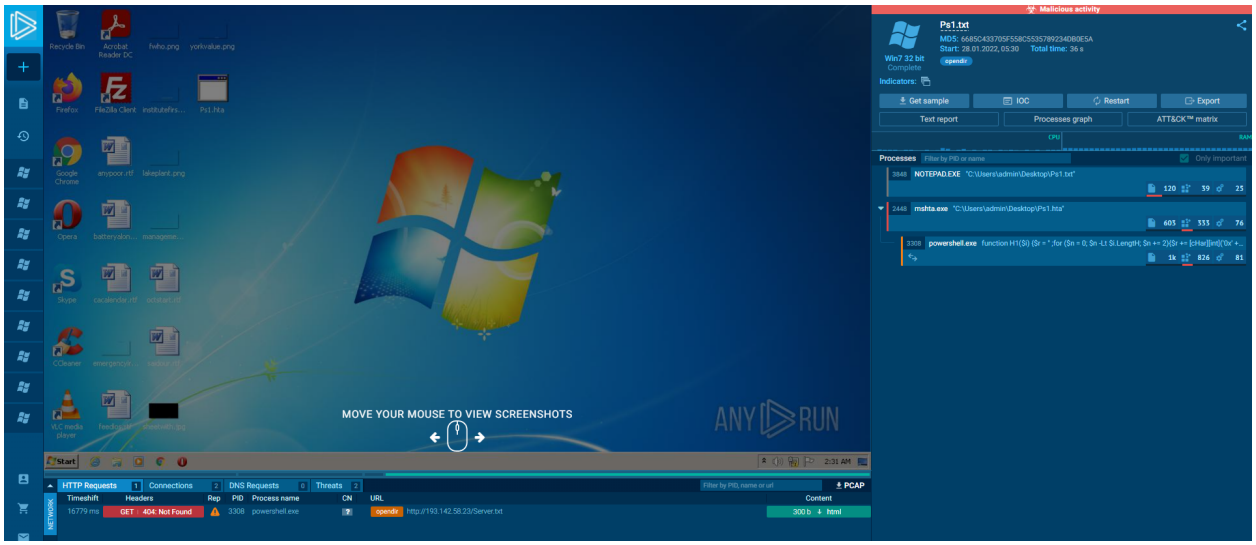
https://bazaar.abuse.ch/sample/886095c7861a068d1ee603c71cb161f256941e802e743fe2161f30013947a2f1/

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



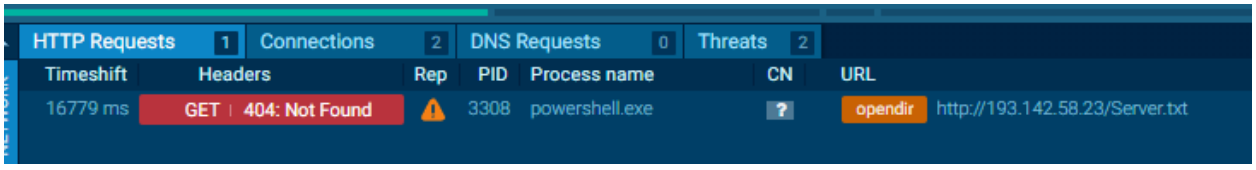
DETECTION

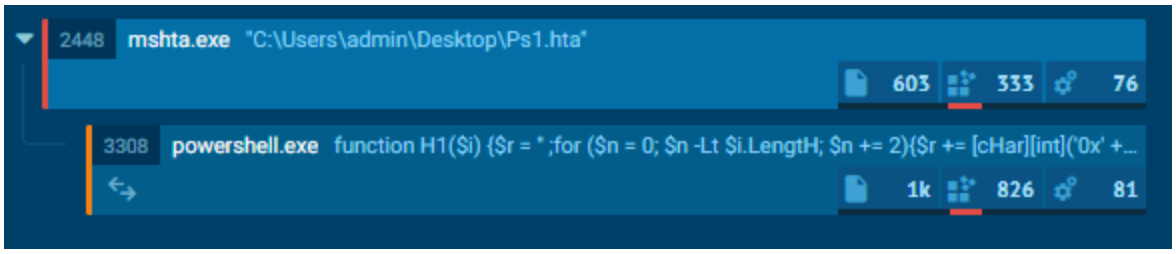
We can perform a dynamic analysis in AnyRun to understand what kind of behavior the obtained “Ps1.hta” file shows.



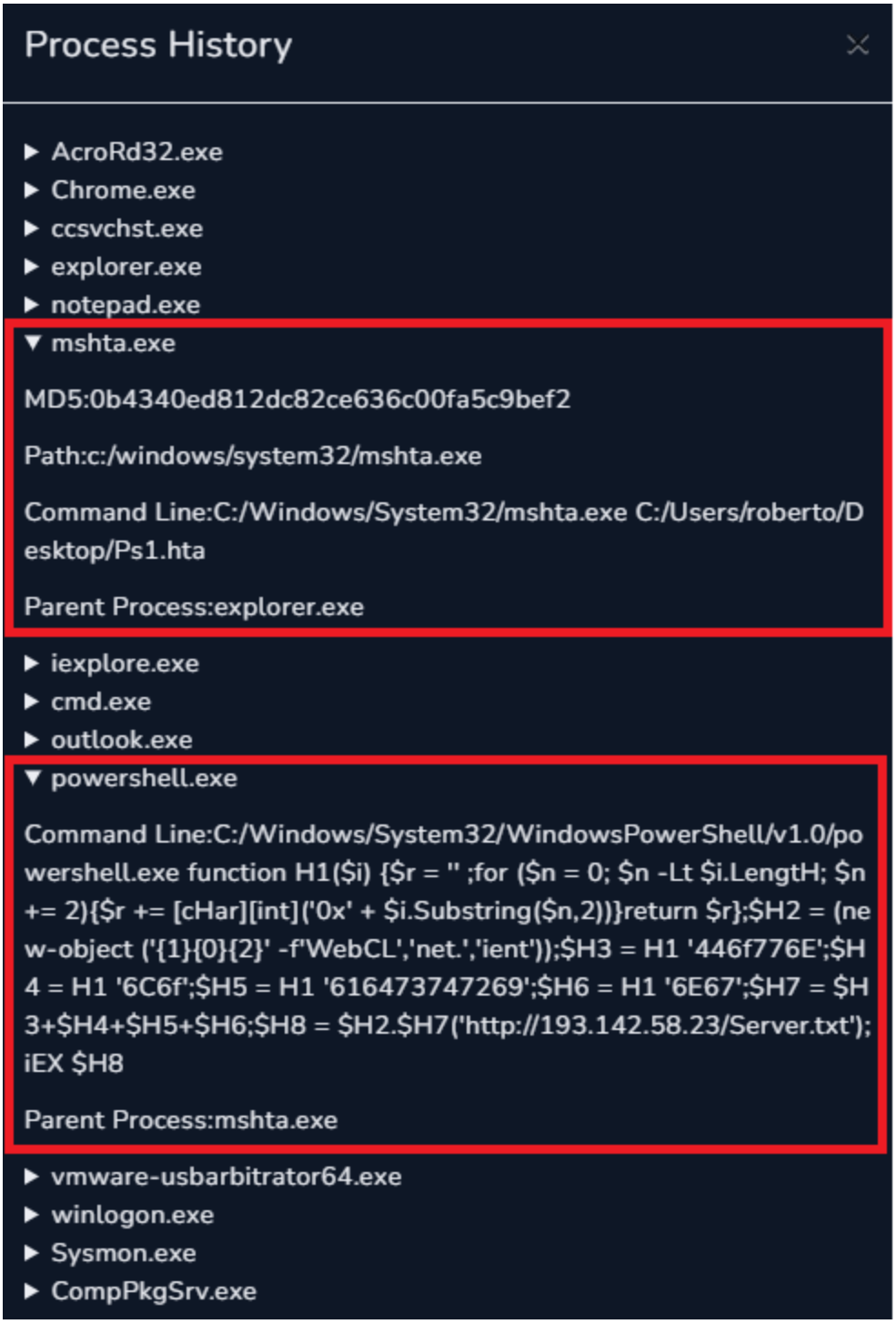
https://app.any.run/tasks/729ba27c-16b6-4075-81f7-4e9058fda29b/

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/

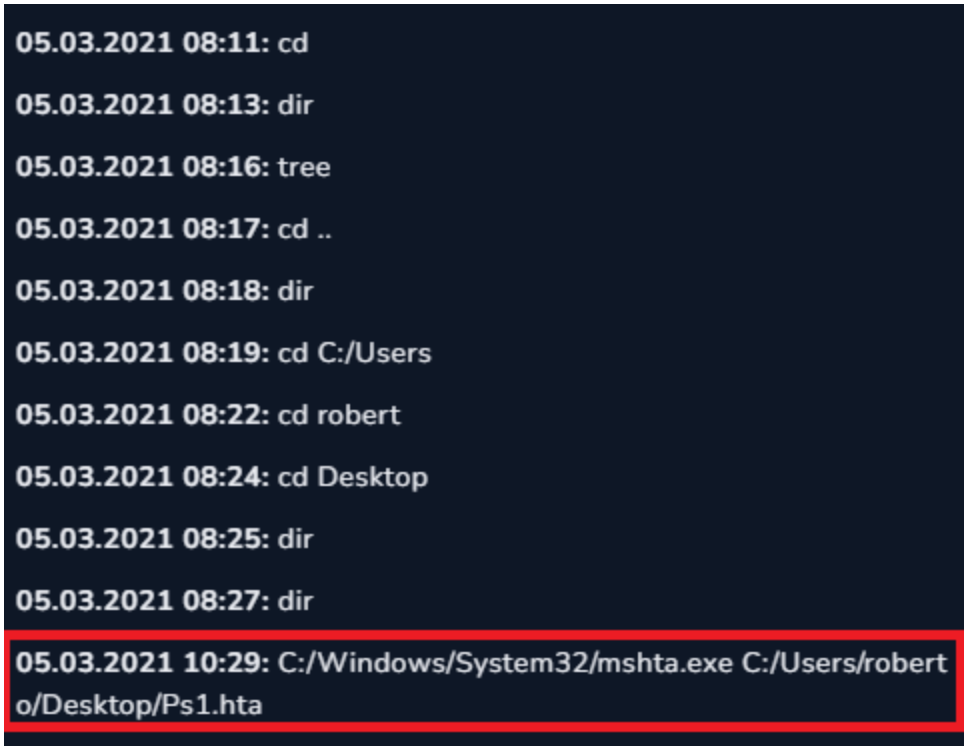
Execute

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.

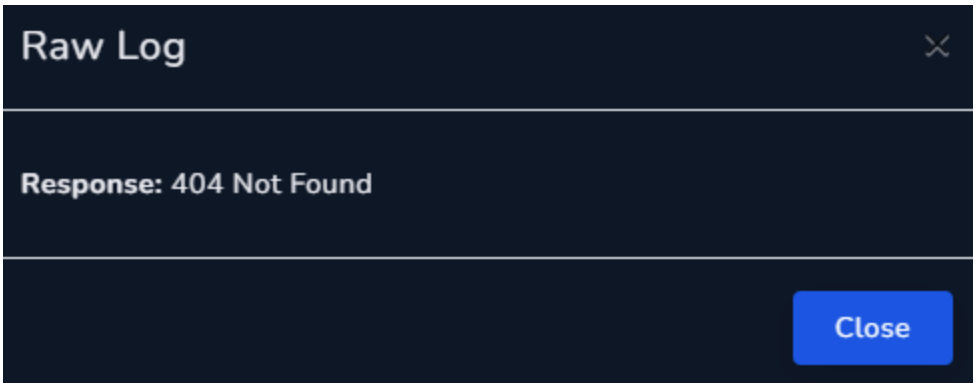


As a result of the dynamic analysis we performed in Anyrun, we saw that an HTTP request was sent to the address 193[.]142[.]58[.]23/Server.txt.

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

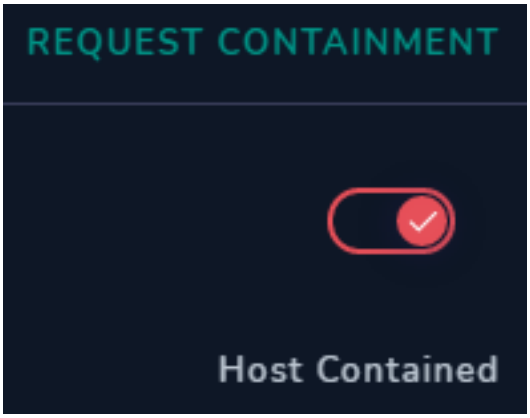


As a result, we see that “mshta.exe” was actually used to perform a malicious activity. The related .hta file is malicious.

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	● 193[.]142[.]58[.]23
URL Address	● 193[.]142[.]58[.]23/Server.txt
MD5	● 6685c433705f558c5535789234db0e5a
Filename	● Ps1.hta