Digital Egypt Pioneers Initiative (DEPI)

Final Project

Malware Analysis and Prevention Strategy

What is malware ?

•Definition of malware:

Malicious software designed to harm computer systems.

•Types of malware:

Viruses, worms, trojans, spyware, adware, ransomware, rootkits, and bots

.

•Impact of malware:

Data loss, financial loss, identity theft, system disruption, and productivity loss.

What is malware ?

•Definition of malware:

Malicious software designed to harm computer systems.

•Types of malware:

Viruses, worms, trojans, spyware, adware, ransomware, rootkits, and bots

.

•Impact of malware:

Data loss, financial loss, identity theft, system disruption, and productivity loss.

Your paragraph text

Viruses

•Definition:

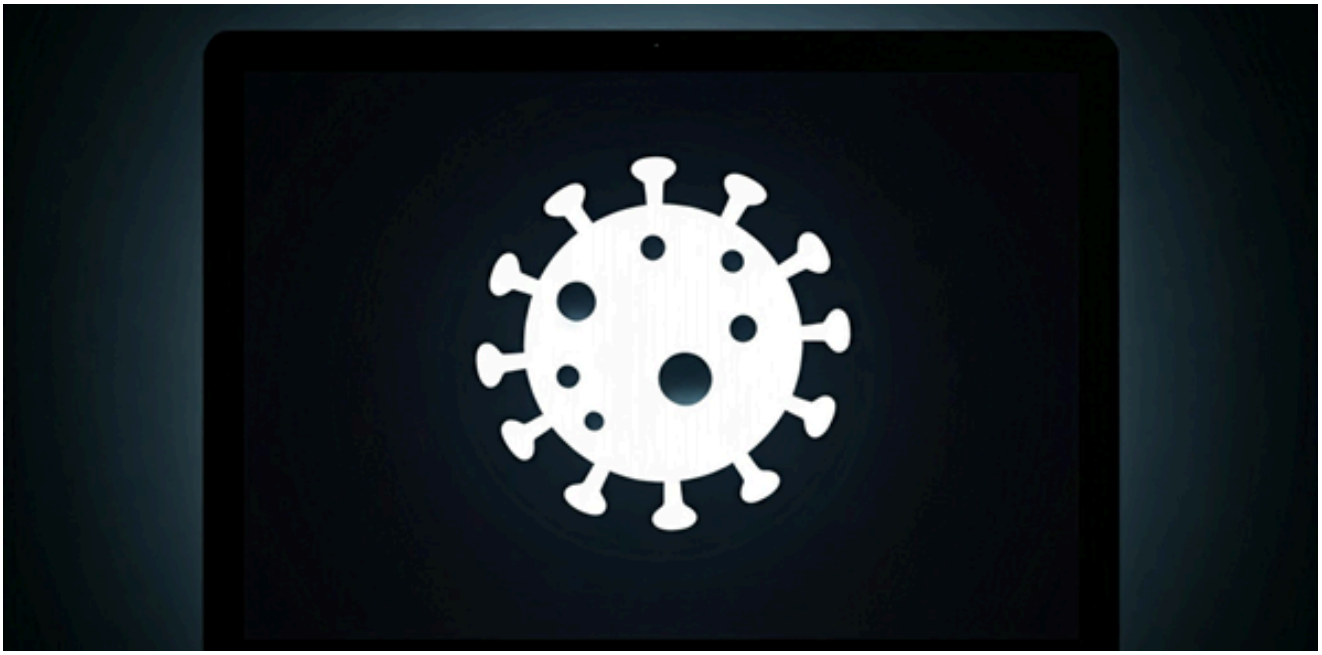
• Self-replicating programs that attach to other files.

•Types:

• Boot sector viruses, file infectors, macro viruses.

•Impact:

• Corrupt files, damage system files, and •slow down performance.



Worms

•Definition:

• Self-replicating programs that spread
• through networks.

•Impact:

Consume network bandwidth, overload
• systems, and disrupt services.

Trojans

•Definition:

• Malicious programs disguised as legitimate software.

•Types:

• Remote access trojans, backdoor trojans,
• keyloggers.

•Impact:

• Allow unauthorized access, steal data, and
•compromise systems

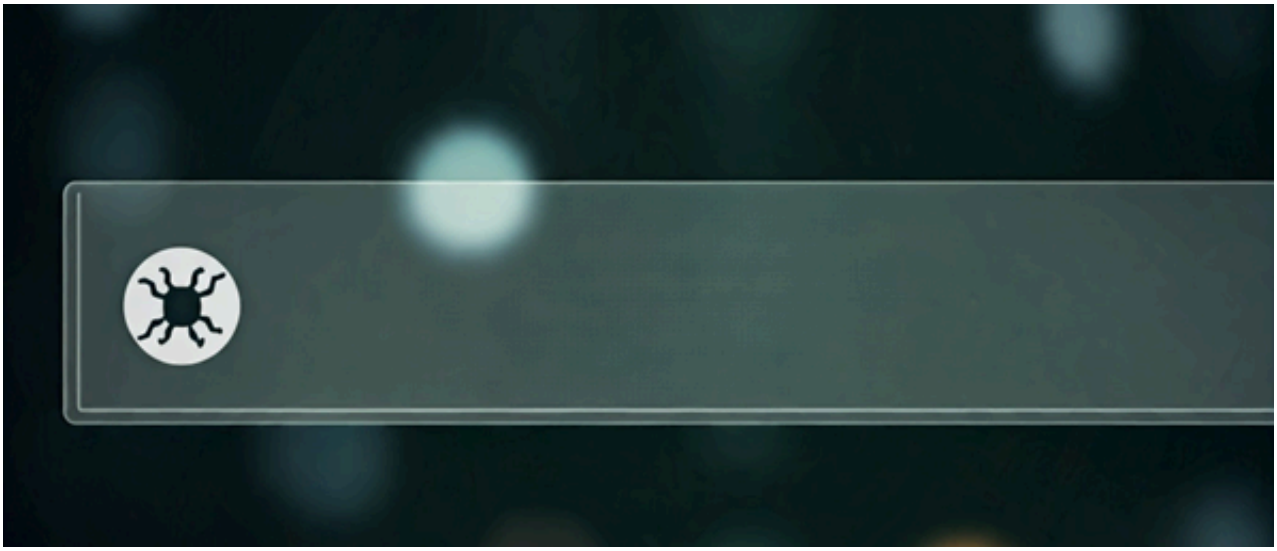
Spyware

•**Definition:** Software that secretly monitors user activity

•**Types:** Keyloggers, screen capture software, cookie hijackers.

•**Impact:**

• Steal personal information, track online behavior,
and sell data to third parties.



Adware

•**Definition:**
Software that displays unwanted advertisements.

•**Impact:**
Slow down performance, consume resources, and
redirect users to malicious websites.

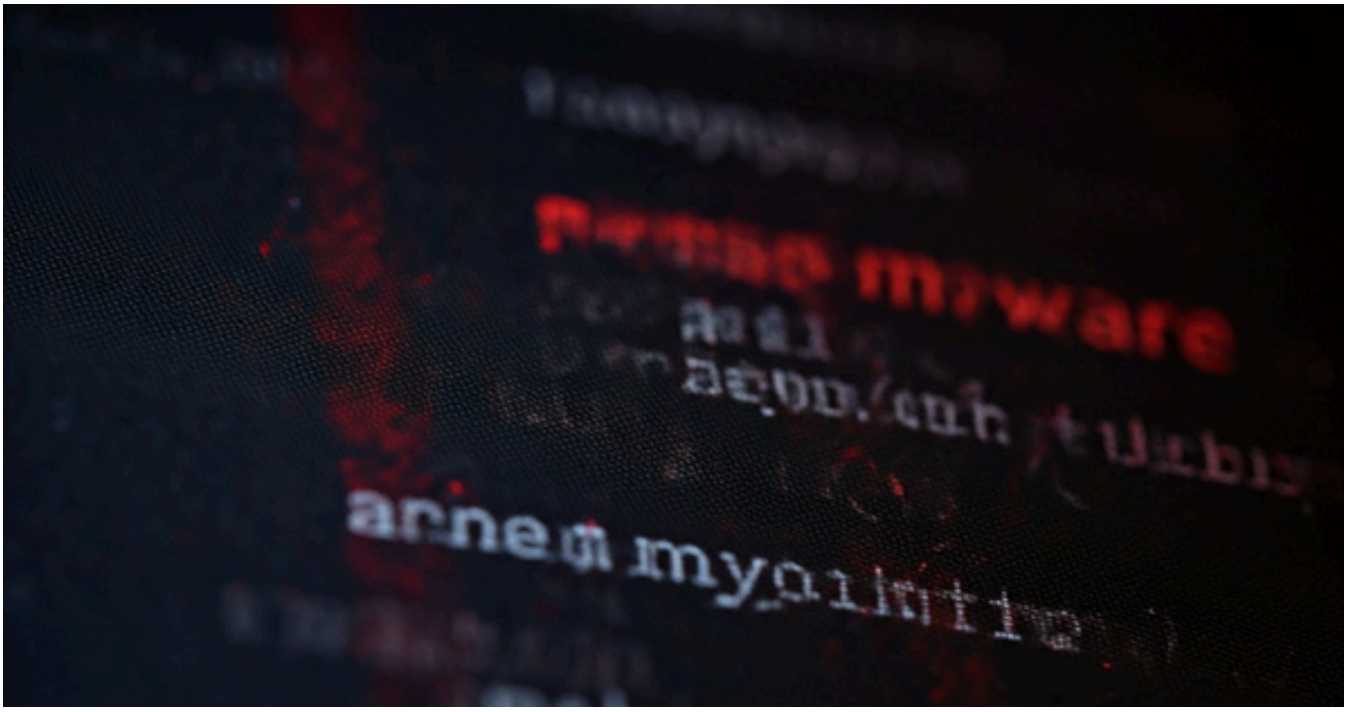
Ransomwar

•Definition

Malware that encrypts files and demands a ransom for decryption.

•Impact

Data loss, financial loss, and disruption of business operations.



Rootkits

•Definition

Software that hides malware and gives attackers administrative privileges.

•Impact

Take control of systems, steal data, and launch attacks.

Bots

•Definition

Malware that performs automated tasks.

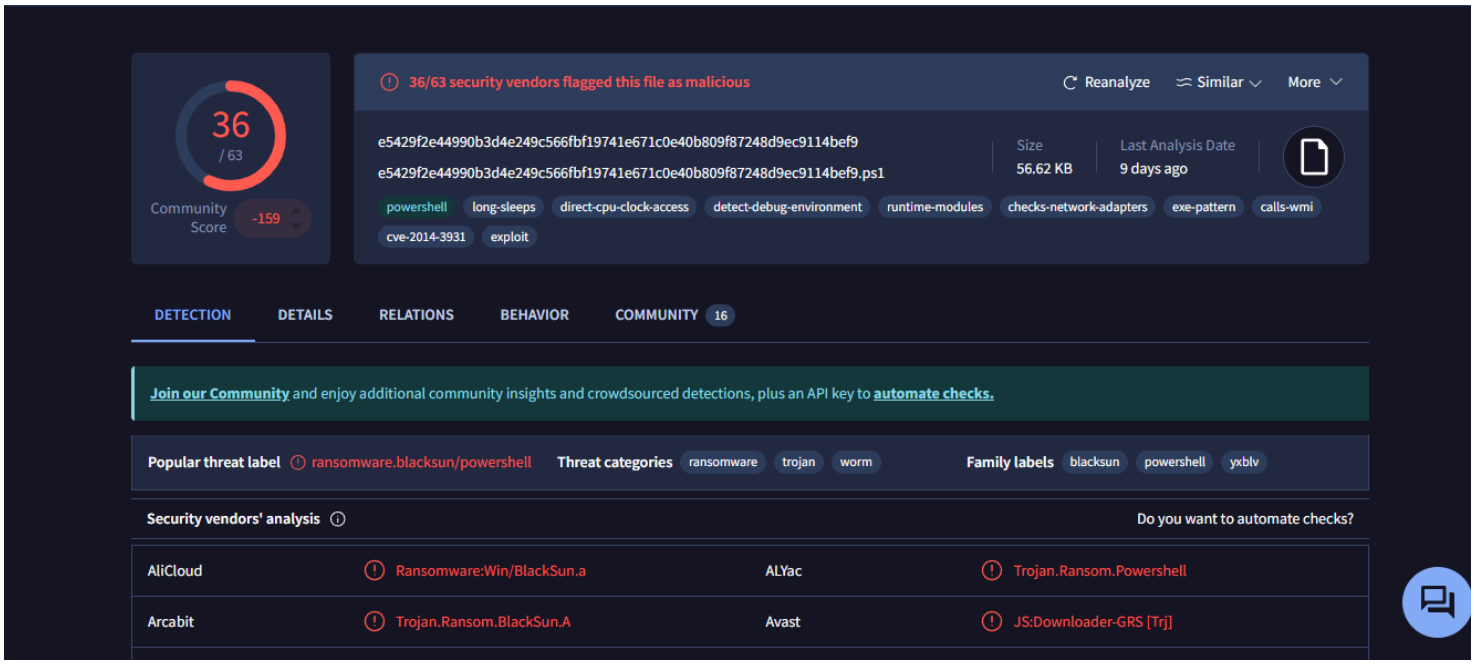
•Types

Spam bots, click fraud bots, DDoS bots.

•Impact

Spam emails, click fraud, and distributed denial-of-service attacks

Malware Analysis



File Names

- e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9.ps1
- 523.mal
- BlackSun.ps1

History

First Submission

2021-09-20 11:16:51 UTC

Last Submission

2024-05-29 15:37:49 UTC

Last Analysis

2024-10-14 11:58:12 UTC

Relations

Contacted URLs (1)

Scanned	Detections	Status	URL
2022-10-09	0 / 89	200	http://ftpserver.net/htdocs/$LogFileName

Contacted Domains (3)

Domain	Detections	Created	Registrar
domaincntrol.com	0 / 94	2017-03-03	GoDaddy.com, LLC
ftpserver.net	0 / 94	1999-03-12	Network Solutions, LLC
mtflats.com	0 / 94	2022-07-17	-

Contacted IP addresses (7)

IP	Detections	Autonomous System	Country
104.26.10.61	0 / 94	13335	-
104.26.11.61	0 / 94	13335	-
172.67.68.176	0 / 94	13335	-
199.59.243.220	1 / 94	16509	US
204.79.197.203	1 / 94	8068	US
23.199.71.185	0 / 94	20940	US
74.220.199.6	3 / 94	46606	US

Hashes

Basic properties

MD5	3ebab71cb71ca5c475202f401de008c8
SHA-1	e0afcf804394abd43ad4723a0feb147f10e589cd
SHA-256	e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9
Vhash	2f04266c495dff557609a6b9b89dbefa
SSDEEP	768:iKEF7iQbM3xo0WhA3tU8zRiopPyZ0rFwF5x1IqgLSCodKW:iKqiCM3xo7hANzRvqyri3xCqgeCowW
TLSH	T1A1432A25B7165C8D4E82039B9CB3FCC0982E88F9057B19E4B4EF95D872D8C9D46783E9
File type	Powershell source powershell ps ps1
Magic	ASCII text, with very long lines (398u), with CRLF line terminators
TrID	file seems to be plain text/ASCII (0%)
Magika	POWERSHELL
File size	56.62 KB (57979 bytes)

Activity of Malware

File system actions

Files opened

- C:\Program Files (x86)\Common Files\Oracle\Java\javapath
- C:\Program Files (x86)\Common Files\Oracle\Java\javapath\
- C:\Program Files\Windows Defender\MpClient.dll
- C:\Program Files\Windows Defender\MpOAV.dll
- C:\Program Files\Windows Defender\MsMpLics.dll
- C:\Program Files\dotnet\
- C:\ProgramData
- C:\Users\<USER>\.dotnet\tools
- C:\Users\<USER>\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log
- C:\Users\<USER>\AppData\Local\Microsoft\WindowsApps

Files written

- C:\Users\Administrator\AppData\Local\Temp\3hrfxqhb.gyz.ps1
- C:\Users\Administrator\AppData\Local\Temp\enbrknaj.uuy.ps1
- C:\Users\<USER>\AppData\Local\Temp\BlackSun_DRIVE_LOCAL_C
- C:\Users\<USER>\AppData\Local\Temp\2ipheyu0.ola.ps1
- C:\Users\<USER>\AppData\Local\Temp\bjgsbtfo.1vv.ps1
- C:\Users\<USER>\AppData\Local\Temp\mr2m3ak2.5ss.ps1
- C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\UPnP Device Host\upnphost\udhisapi.dll
- C:\Users\user\AppData\Local\Microsoft\Windows\Caches
- C:\Users\user\AppData\Local\Temp\BlackSun.log
- C:\Users\user\AppData\Local\Temp\BlackSun_DRIVE_LOCAL_C

Files deleted

- C:\Users\<USER>\AppData\Local\Temp\BlackSun.log
- C:\Users\Administrator\AppData\Local\Temp\3hrfxqhb.gyz.ps1
- C:\Users\Administrator\AppData\Local\Temp\enbrknaj.uuy.ps1
- C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fns342a4.ake.psm1
- C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p43e5pcl.4kr.ps1

Files with modified attributes

- C:\Users\Elijah\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\X7WFZDAKV93LS5FQZJVX.temp

Files dropped

590aee7bdd69b59b.customDestinations-ms

BlackSun.log

__PSScriptPolicyTest_4zpne3ld.amz.psm1

07f702a302d0d5789612235ea7e73533558a91fdec268d6300920dfbb612bf5c

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fns342a4.ake.psm1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p43e5pcl.4kr.ps1

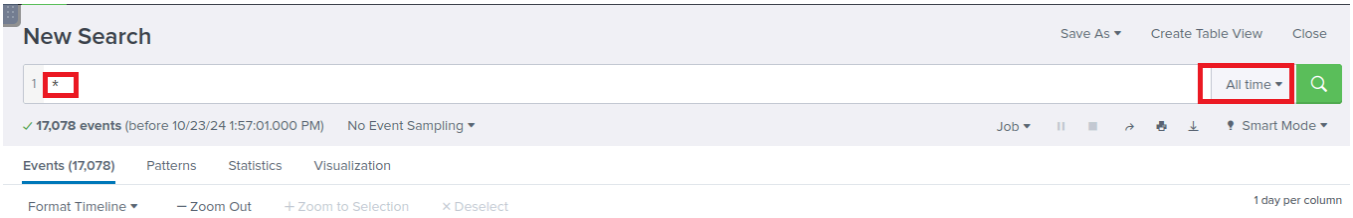
Registry actions

Registry keys opened

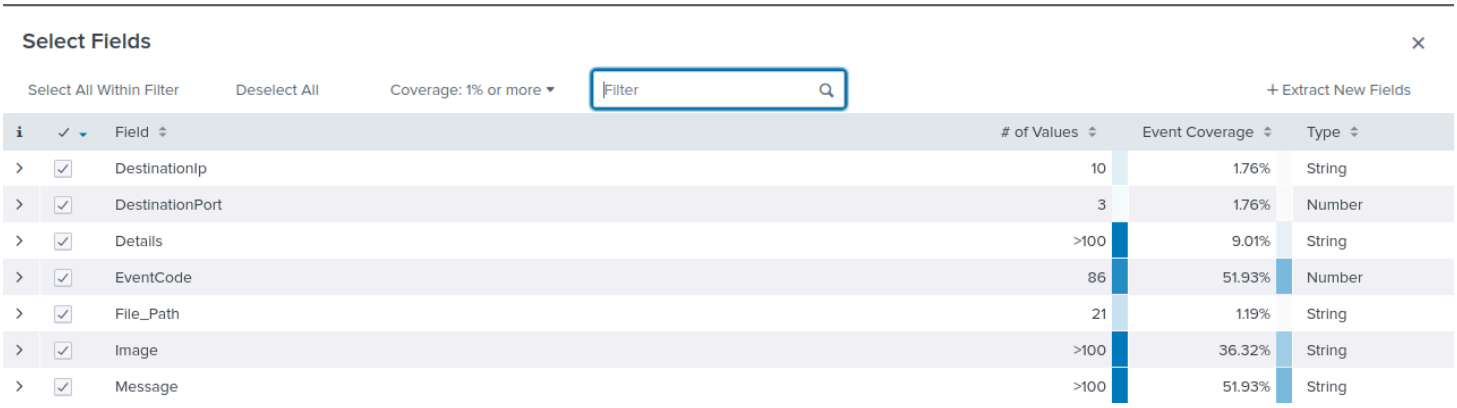
- HKEY_CURRENT_USER\
- HKEY_CURRENT_USER\Control Panel\International\Geo
- HKEY_CURRENT_USER\Control Panel\International\Geo\Nation
- HKEY_CURRENT_USER\Control Panel\International\User Profile
- HKEY_CURRENT_USER\Control Panel\International\User Profile\Languages
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\KnownFolders
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Recent
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel

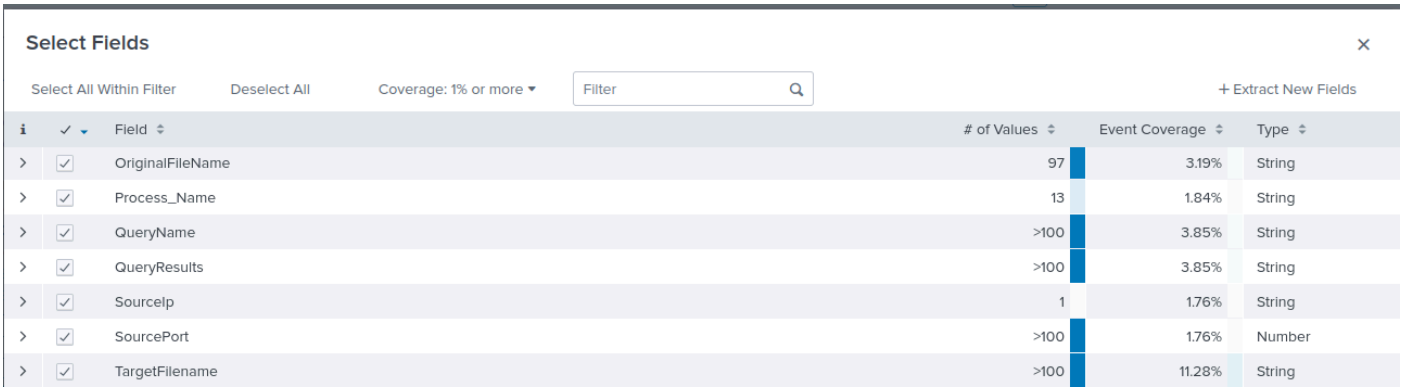
Investigating A Ransomware Attack in Splunk

We display all previous events on Splunk

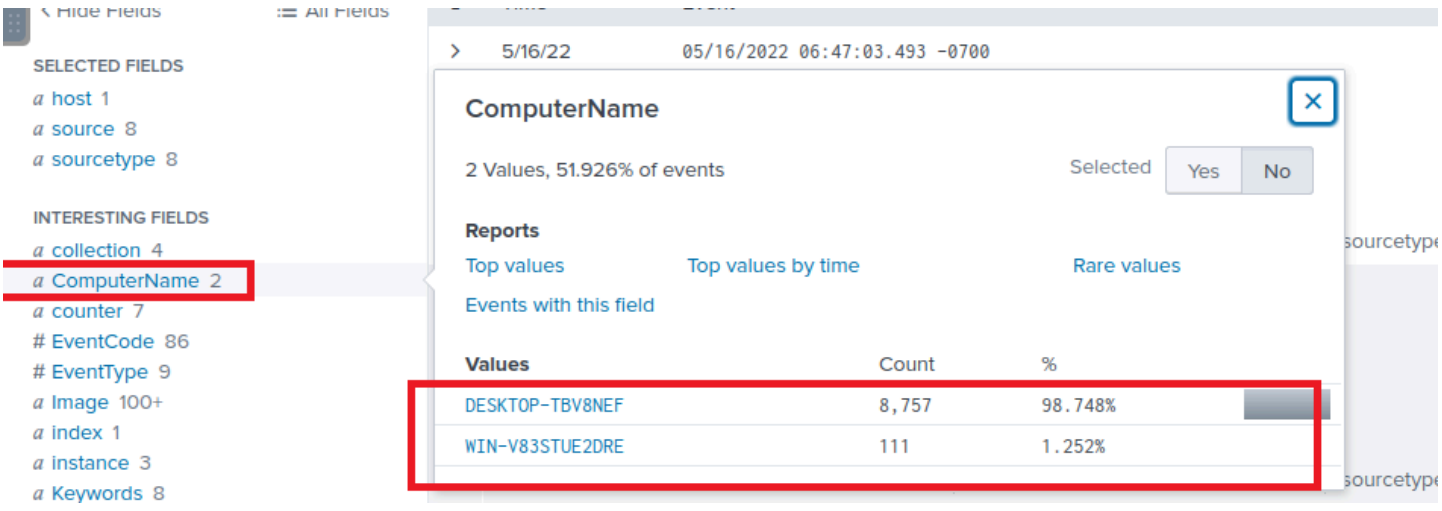


we will select the important fileld

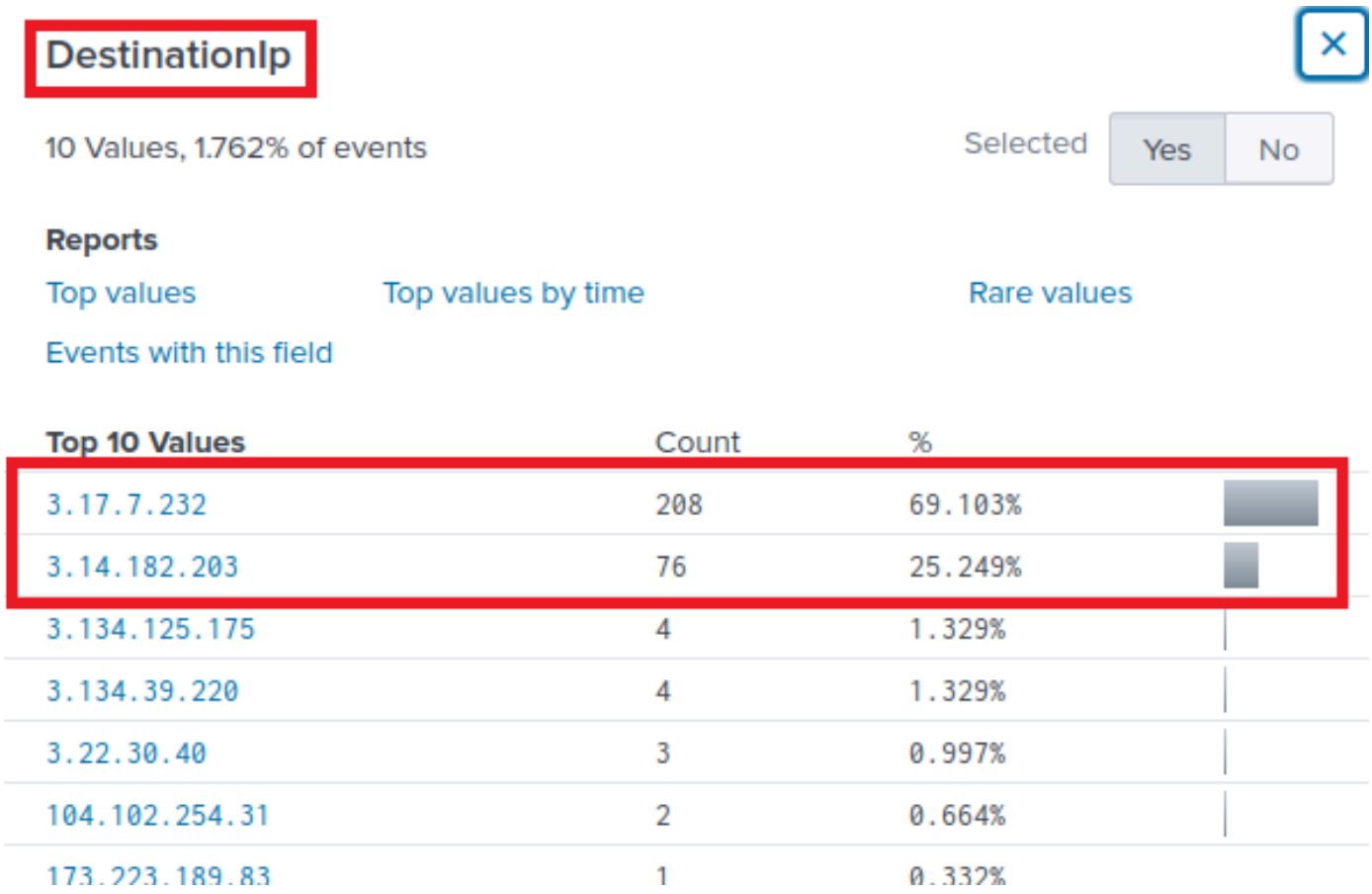




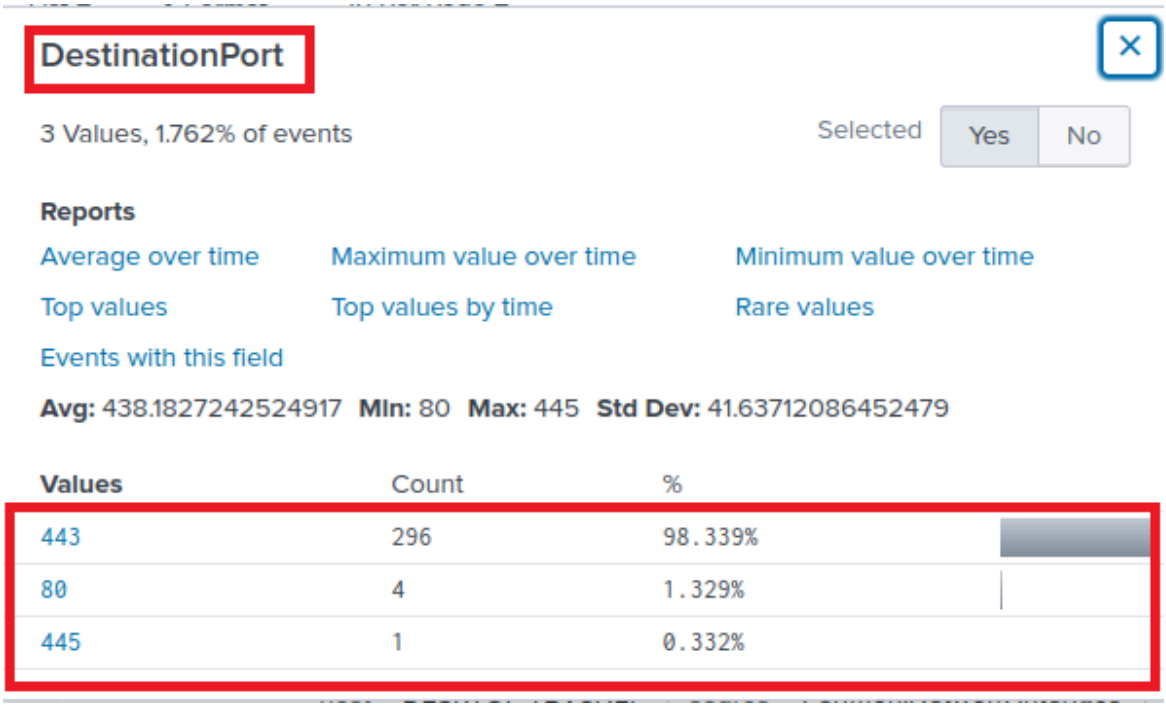
Here we have two computers connected to the Splunk



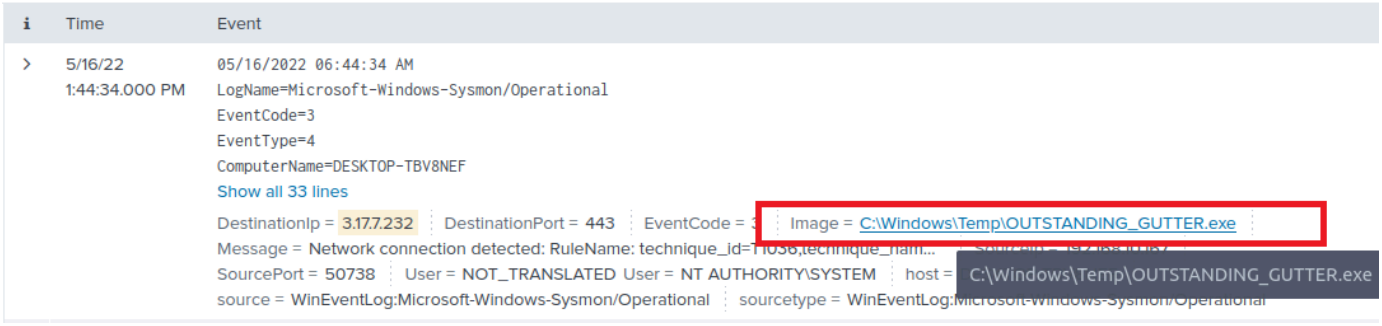
Destination ip



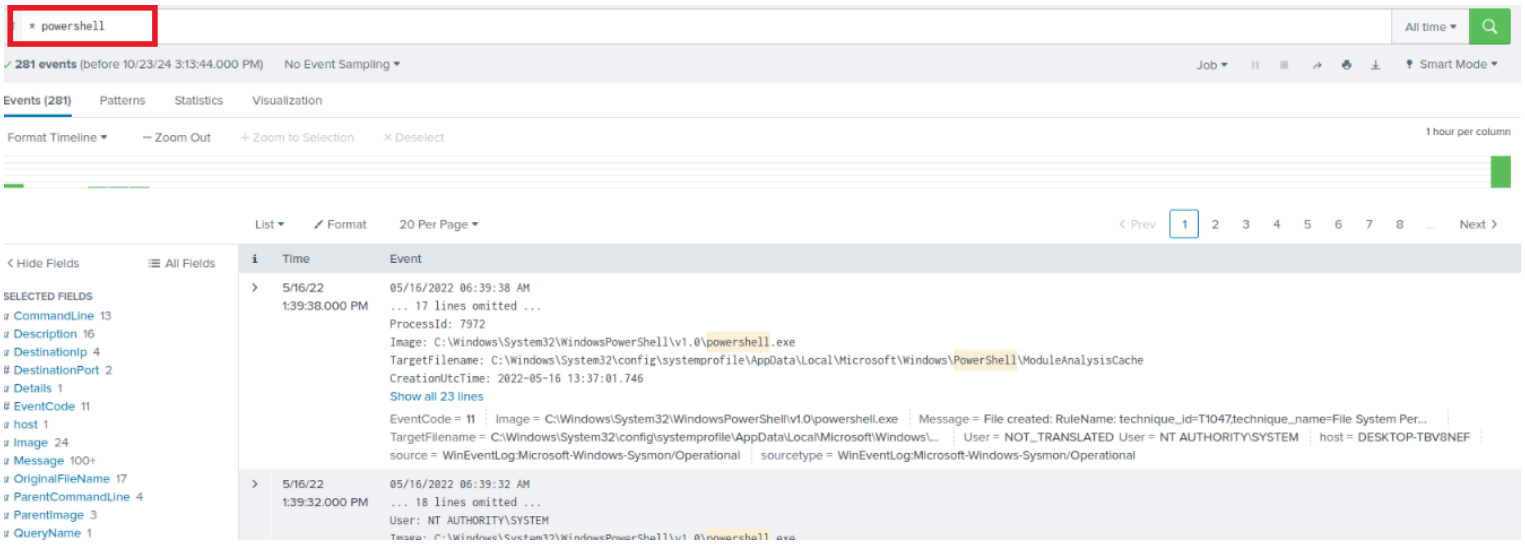
Destination Port



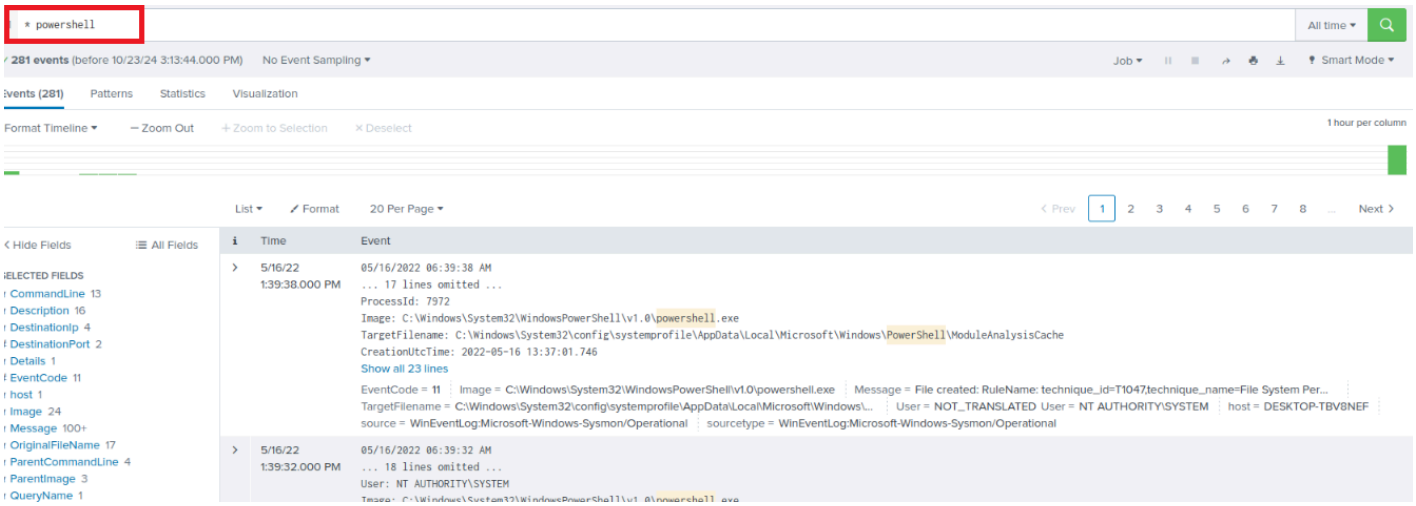
Events in Destination ip (3.17.7.232)

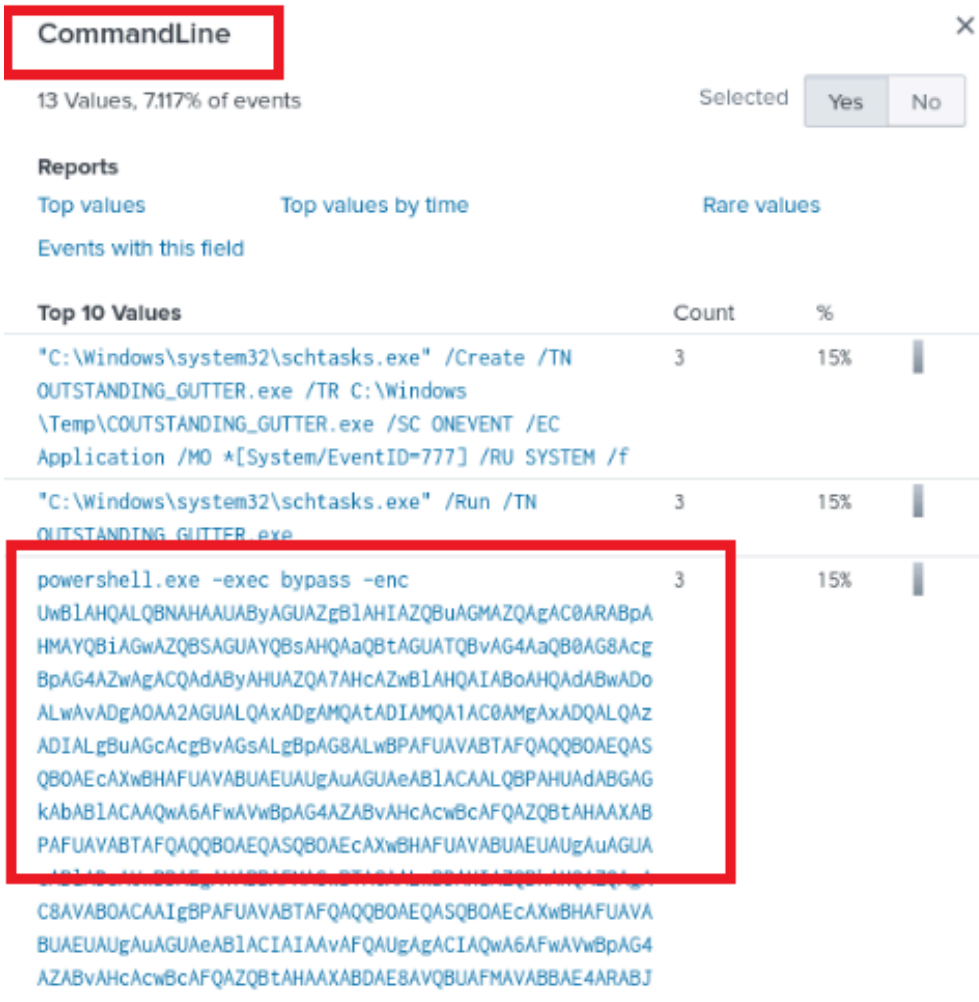


More Detials

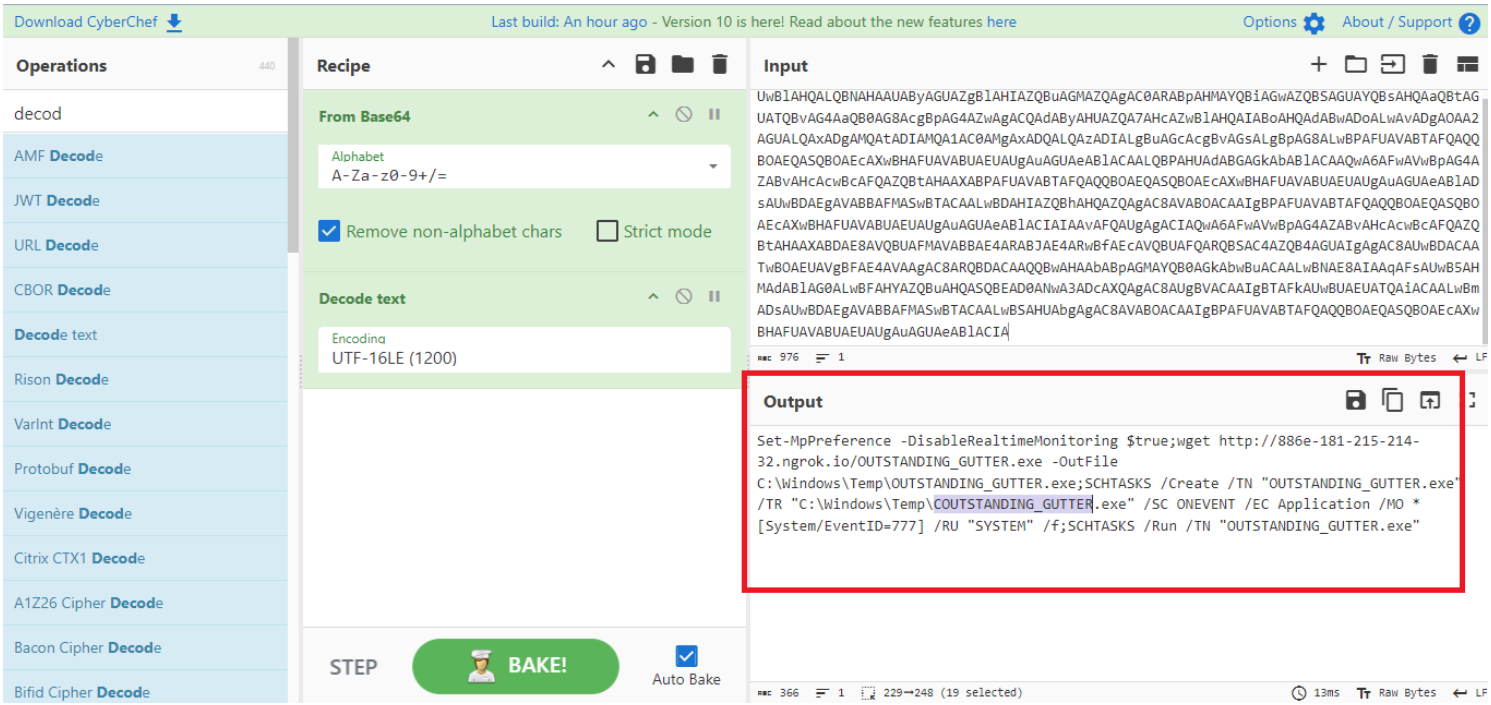


We will look into the Powershell

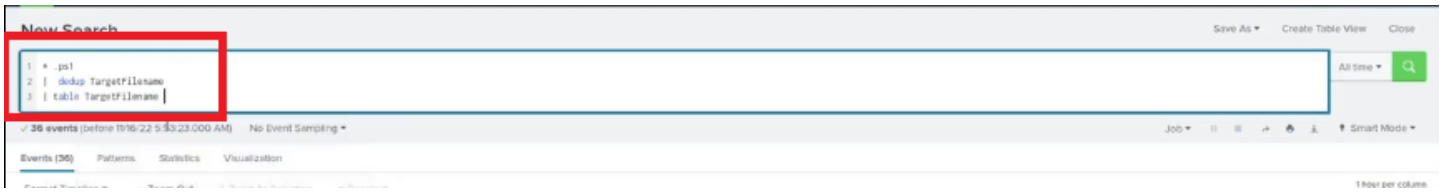




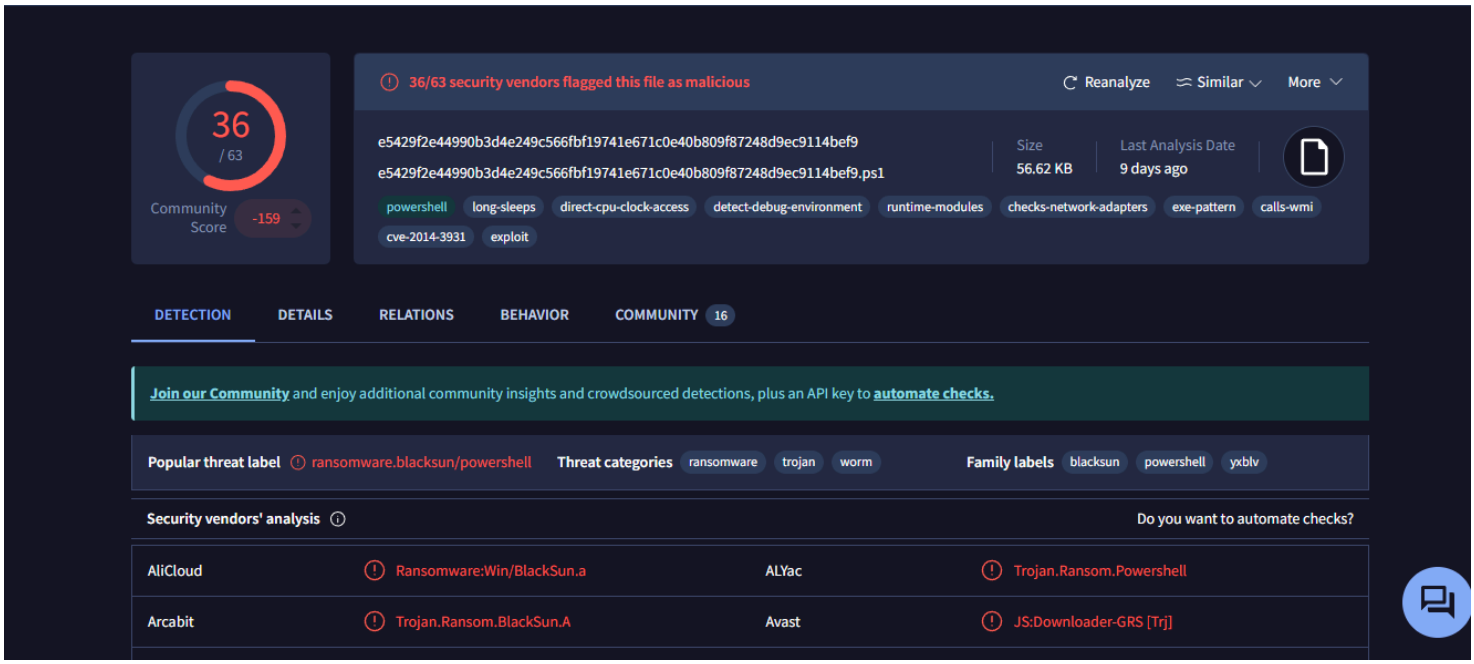
Using Cyberchef, we were able to determine the following: the command issued to disable real-time monitoring, the address the binary was downloaded from is http://886e-181-215-214-32.ngrok.io and the downloaded file creates and runs certain commands.



Get Hash


New Search
Save As
Create Table View
Close
1 *.ps1
2 | dedup TargetFilename
3 | table TargetFilename
All time
36 events (before 11/16/22 5:53:23.000 AM)
No Event Sampling
Job
Smart Mode
Events (36)
Patterns
Statistics
Visualization


2 | dedup TargetFilename
3 | table TargetFilename
10 events (before 11/16/22 5:53:46.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (10)
Visualization
20 Per Page
Format
Preview
TargetFilename
C:\Windows\Temp\script.ps1
C:\Windows\Temp__PSScriptPolicyTest_rmlwvvw4.wdu.ps1
C:\Windows\Temp__PSScriptPolicyTest_3mhxqum0.fcl.ps1
C:\Windows\Temp__PSScriptPolicyTest_nxbdg4vz.owo.ps1
C:\Windows\Temp__PSScriptPolicyTest_znwpkv32.osj.ps1
C:\Users\keegan\AppData\Local\Temp__PSScriptPolicyTest_ocwzia2g.yzb.ps1
C:\Users\keegan\AppData\Local\Temp__PSScriptPolicyTest_gv2h0id4.yub.ps1
C:\Users\keegan\AppData\Local\Temp__PSScriptPolicyTest_1drcoyjc.fn3.ps1
C:\Windows\Temp\SDIAG_61f75ff5-fd72-4c29-9f55-7b44d9f45851\TS_WERQueue.ps1
C:\Windows\Temp\SDIAG_61f75ff5-fd72-4c29-9f55-7b44d9f45851\TS_InaccurateSystemTime.ps1
C:\Windows\Temp\SDIAG_61f75ff5-fd72-4c29-9f55-7b44d9f45851\TS_DiagnosticHistory.ps1
C:\Windows\Temp\SDIAG_61f75ff5-fd72-4c29-9f55-7b44d9f45851\RS_UserWERQueue.ps1
C:\Windows\Temp\SDIAG_61f75ff5-fd72-4c29-9f55-7b44d9f45851\RS_UserDiagnosticHistory.ps1
C:\Windows\Temp\SDIAG_61f75ff5-fd72-4c29-9f55-7b44d9f45851\RS_SyncSystemTime.ps1
C:\Windows\Temp\SDIAG_61f75ff5-fd72-4c29-9f55-7b44d9f45851\RS_MachineWERQueue.ps1


36
/ 63
Community Score
-159
36/63 security vendors flagged this file as malicious
Reanalyze
Similar
More
e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9
e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9.ps1
Size
56.62 KB
Last Analysis Date
9 days ago
powershell
long-sleeps
direct-cpu-clock-access
detect-debug-environment
runtime-modules
checks-network-adapters
exe-pattern
calls-wmi
cve-2014-3931
exploit
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 16
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label ransomware.blacksun/powershell
Threat categories ransomware trojan worm
Family labels blacksun powershell yxblv
Security vendors' analysis
Do you want to automate checks?
AliCloud Ransomware:Win/BlackSun.a
ALYac Trojan.Ransom.Powershell
Arcabit Trojan.Ransom.BlackSun.A
Avast JS:Downloader-GRS [Trj]

USER AWARENESS TRAINING

1- Think before click

01
Look for Red Flags Suspicious email addresses, urgent language, unexpected attachments.

THINK BEFORE YOU CLICK!

02 Verify Links: Hover over links before clicking to check for fake URLs.

03 Report it. If unsure, report phishing attempts to your IT team immediately

REPORT PHISHINGSS TO IT TEAM

3.2-USER AWARENESS TRAINING

4-Keep Your Devices Secure

01 Update Software Regularly: Always install the security patches. latest

02 Use Antivirus Software: Regular scans keep malware

03 Lock Your Device: Always lock your screen when stepping away.

3.2-USER AWARENESS TRAINING

2-Build a Strong Password

1-Use at least 12 characters with a mix of letters, numbers, and symbols.

2- Avoid common words and personal info.

3- Enable MFA (Multi-Factor Authentication) for extra security

3.2-USER AWARENESS TRAINING

3-Handle Data with Care!

01 Encrypt Sensitive Data both in transit and at rest.

02 Share Securely. Use secure methods (VPN, encrypted email) for sharing sensitive info.

03 Access Control Only authorized personnel should have access to sensitive data.

MALWARE PREVENTION STRATEGY

A multi-layered strategy protects against malware across various attack vectors.

01

Update Software:

Regularly patch operating systems and applications to fix vulnerabilities.

02

Antivirus & Antimalware:

Use security tools to detect and block. malicious programs.

03

Firevvalls & IDS:

Monitor network traffic to prevent unauthorized access.

04

Employee Training:

Educate staff on spotting phishing and unsafe practices.

05

Network Segmentation:

Isolate critical systems to limit malware spread.

06

Limit User Access:

Apply the least privilege principle to reduce entry points.

07

Regular Backups:

Ensure frequent backups for quick recovery.

08

Email &

Filtering: Block malicious emails and restrict access to harmful websites.

09

Threat Intelligence:

Stay informed about emerging malware threats.

Thank You!

Rahma Alaa Zakaria
Nada Shehta Saber
Nagwa Mohamed Abd ELKream
Naira Khaled