🔍 Unit 42 SOC Lab – Sysmon Log Analysis & Backdoor Investigation

Analyst: Aarush Nepali
Source: Hack The Box – *Sherlock Lab: Unit 42*
Focus: Detection and analysis of UltraVNC backdoor using Sysmon and Splunk

---

🧠 Objective

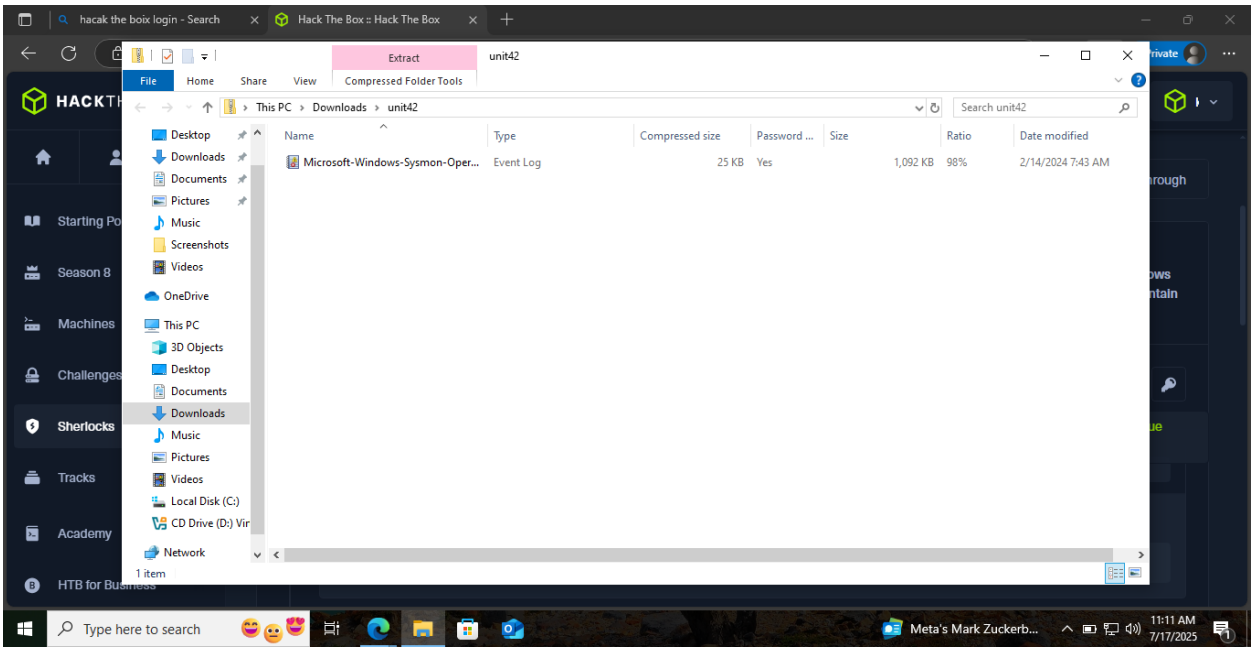
Conduct structured threat hunting using Sysmon logs to:

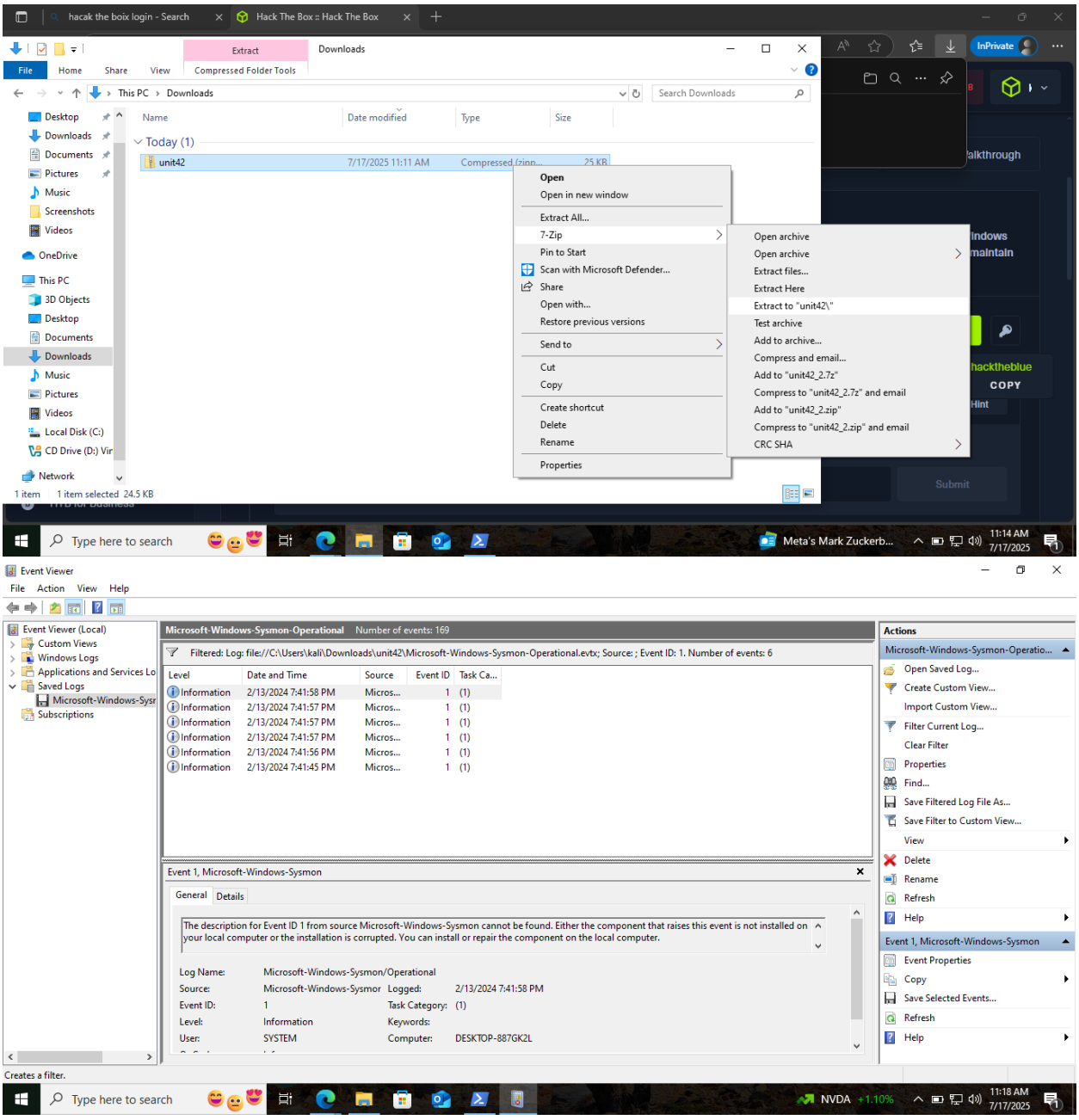
- Detect suspicious processes and file activity
- Trace potential backdoor behavior
- Practice advanced log analysis workflows in a simulated SOC setting

---

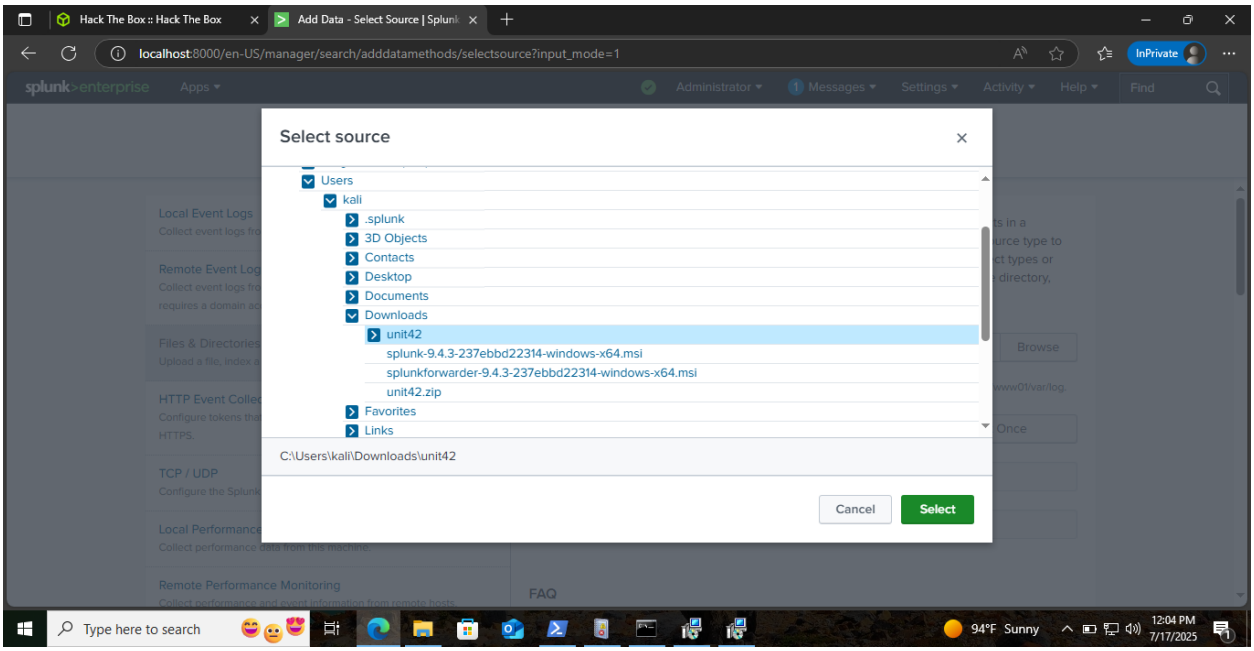
🛠️ Lab Environment

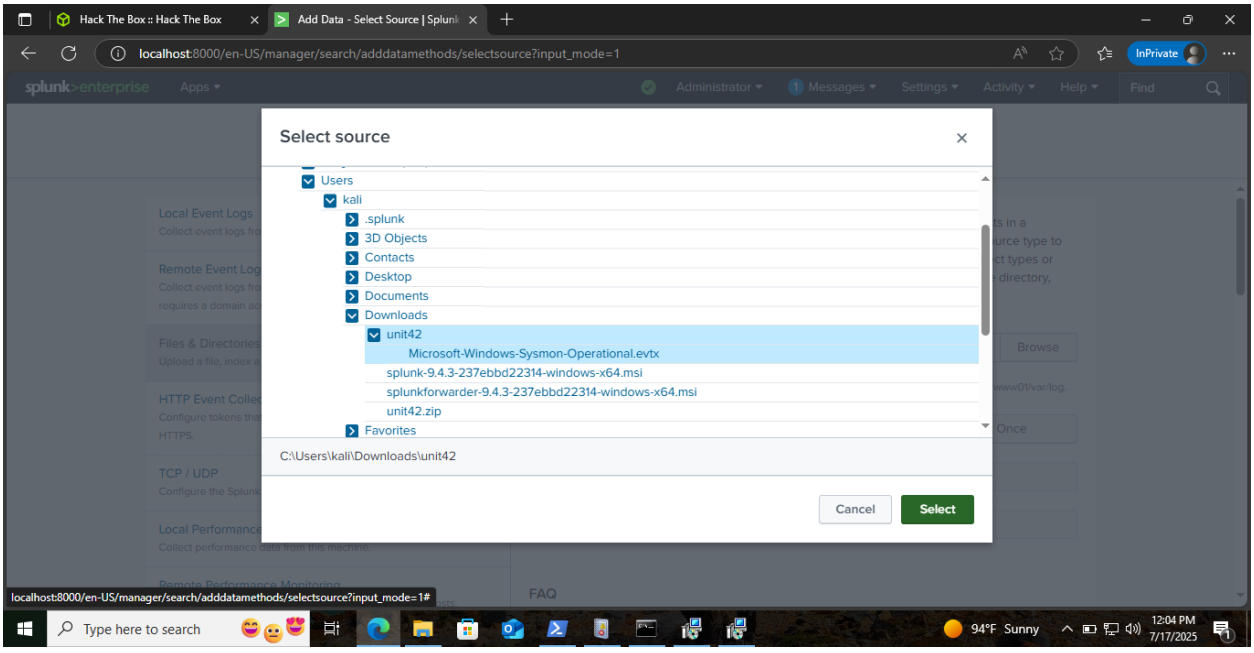
- Platform: Hack The Box → *Sherlocks* > *Unit 42*
- Files: `unit42.zip` extracted with password `hackthebox`
- Log File: `Microsoft-Windows-Sysmon operational.evtx`
- Tools Used:
  - 📦 7-Zip (to extract log archive)
  - 🧠 Event Viewer (for quick inspection)
  - 📊 Splunk (for structured log ingestion and analysis)
  - 🕵️ VirusTotal (for IOC validation)


hacak the boix login - Search
Hack The Box :: Hack The Box
HACKTH
Starting Po
Season 8
Machines
Challenges
Sherlocks
Tracks
Academy
HTB for Business
Extract
unit42
File
Home
Share
View
Compressed Folder Tools
This PC › Downloads › unit42
Search unit42
Desktop
Downloads
Documents
Pictures
Music
Screenshots
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:) Vir
Network
1 item
Name
Type
Compressed size
Password ...
Size
Ratio
Date modified
Microsoft-Windows-Sysmon-Oper...
Event Log
25 KB
Yes
1,092 KB
98%
2/14/2024 7:43 AM
Type here to search
Meta's Mark Zuckerb...
11:11 AM
7/17/2025


hacak the boix login - Search
Hack The Box :: Hack The Box
Downloads
File Home Share View Compressed Folder Tools
This PC › Downloads
Search Downloads
Name Date modified Type Size
Today (1)
unit42 7/17/2025 11:11 AM Compressed (zipp... 25 KB
Open
Open in new window
Extract All...
7-Zip
Pin to Start
Scan with Microsoft Defender...
Share
Open with...
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Open archive
Open archive
Extract files...
Extract Here
Extract to "unit42\"
Test archive
Add to archive...
Compress and email...
Add to "unit42_2.7z"
Compress to "unit42_2.7z" and email
Add to "unit42_2.zip"
Compress to "unit42_2.zip" and email
CRC SHA
1 item 1 item selected 24.5 KB
Type here to search
Meta's Mark Zuckerb...
11:14 AM
7/17/2025

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Lo
Saved Logs
Microsoft-Windows-Sysr
Subscriptions
Microsoft-Windows-Sysmon-Operational Number of events: 169
Filtered: Log: file://C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx; Source: ; Event ID: 1. Number of events: 6
Level Date and Time Source Event ID Task Ca...
Information 2/13/2024 7:41:58 PM Micros... 1 (1)
Information 2/13/2024 7:41:57 PM Micros... 1 (1)
Information 2/13/2024 7:41:57 PM Micros... 1 (1)
Information 2/13/2024 7:41:57 PM Micros... 1 (1)
Information 2/13/2024 7:41:56 PM Micros... 1 (1)
Information 2/13/2024 7:41:45 PM Micros... 1 (1)
Event 1, Microsoft-Windows-Sysmon
General Details
The description for Event ID 1 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmor Logged: 2/13/2024 7:41:58 PM
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-887GK2L
Actions
Microsoft-Windows-Sysmon-Operatio...
Open Saved Log...
Create Custom View...
Import Custom View...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File As...
Save Filter to Custom View...
View
Delete
Rename
Refresh
Help
Event 1, Microsoft-Windows-Sysmon
Event Properties
Copy
Save Selected Events...
Refresh
Help
Creates a filter.
Type here to search
NVDA +1.10%
11:18 AM
7/17/2025





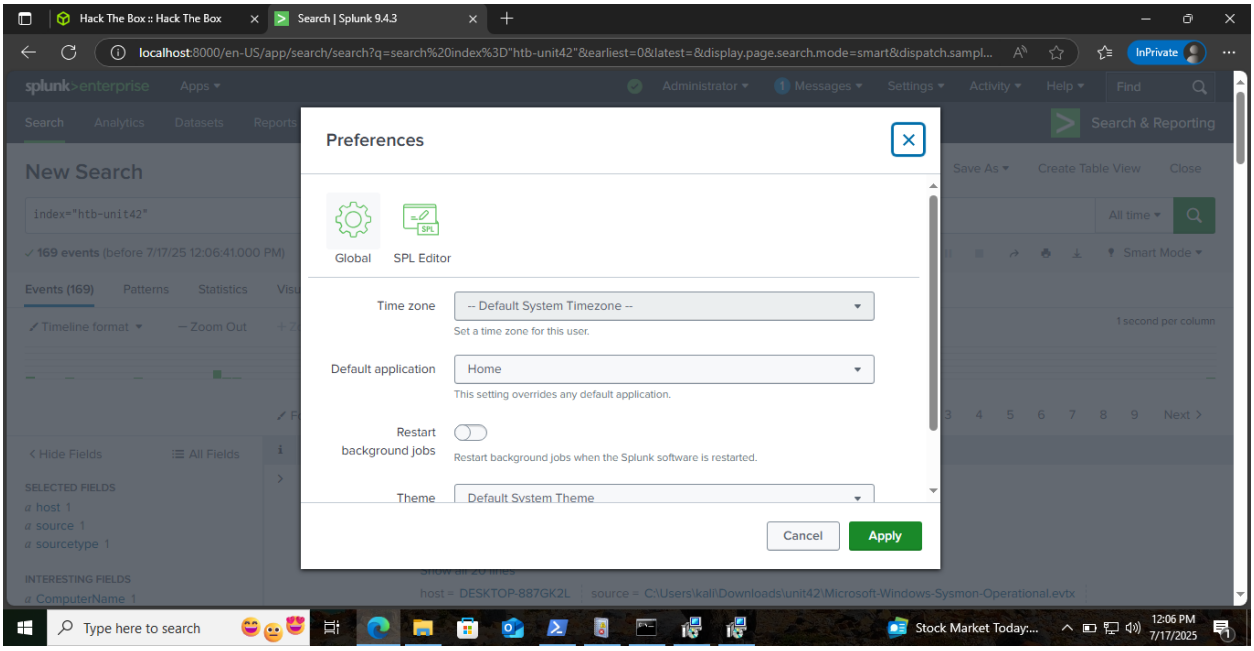
🔄 Data Ingestion & Setup

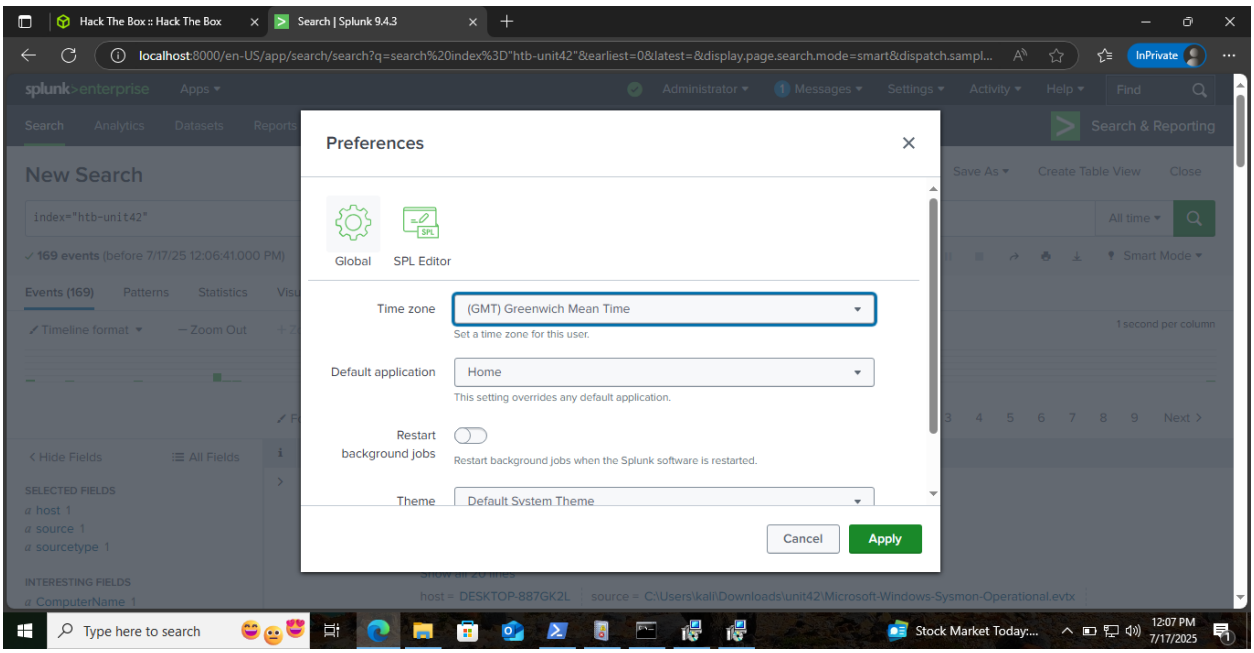
➤ Event Viewer

- Opened `.evtx` in native viewer
- Filtered for Event ID 1 (Process Creation) to spot execution artifacts

➤ Splunk Workflow

1. Ingested extracted log file into new index `htb_unit42`
2. Used `Monitor Directory` method under Splunk's "Add Data" wizard
3. Set time zone to GMT (UTC) to normalize log timelines
4. ✅ Confirmed **169 events** successfully indexed

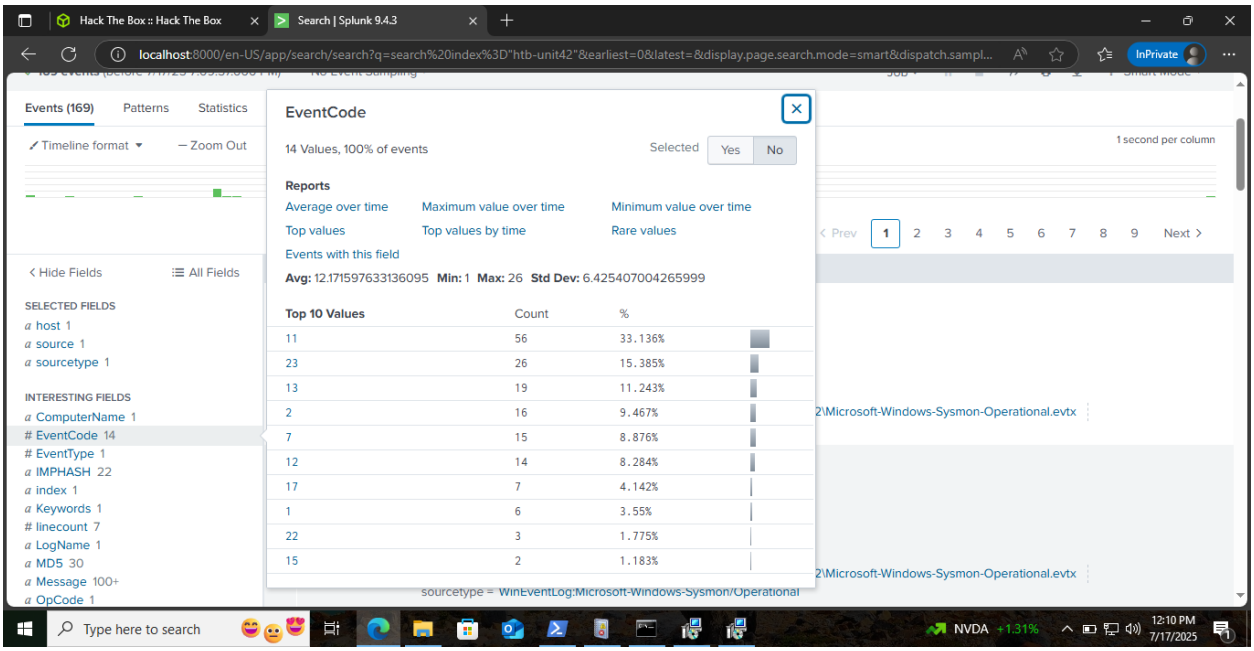


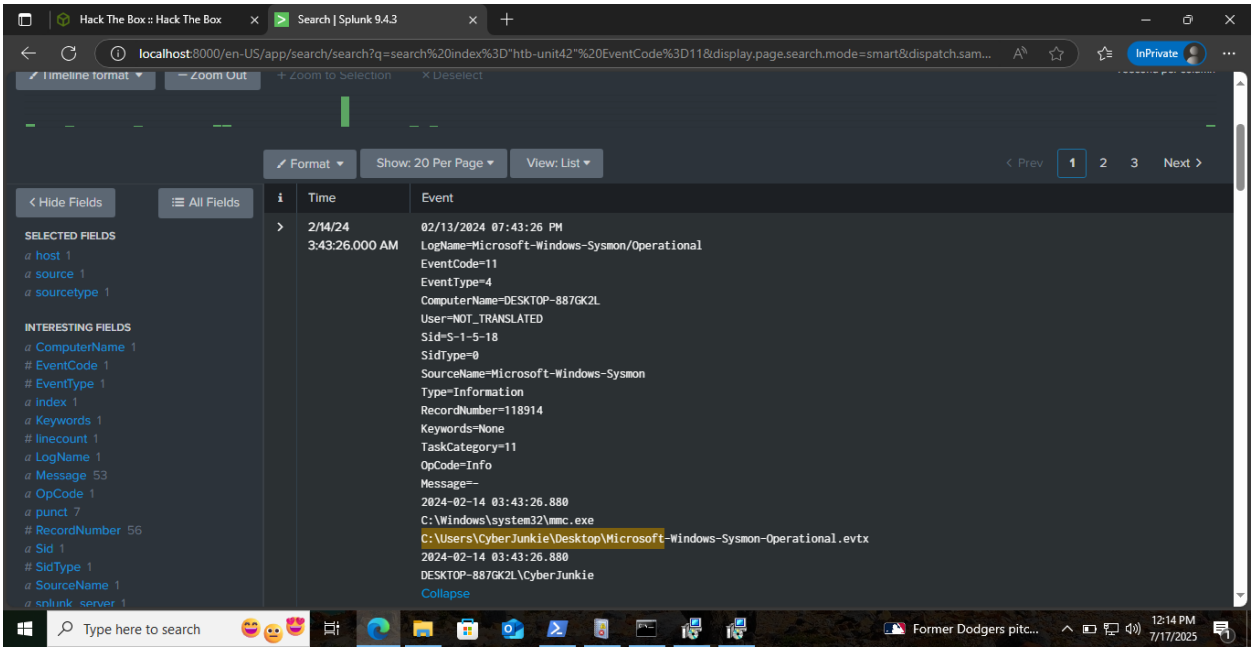


📈 Threat Hunting Results

Q1. File Creation Events (Event ID 11)

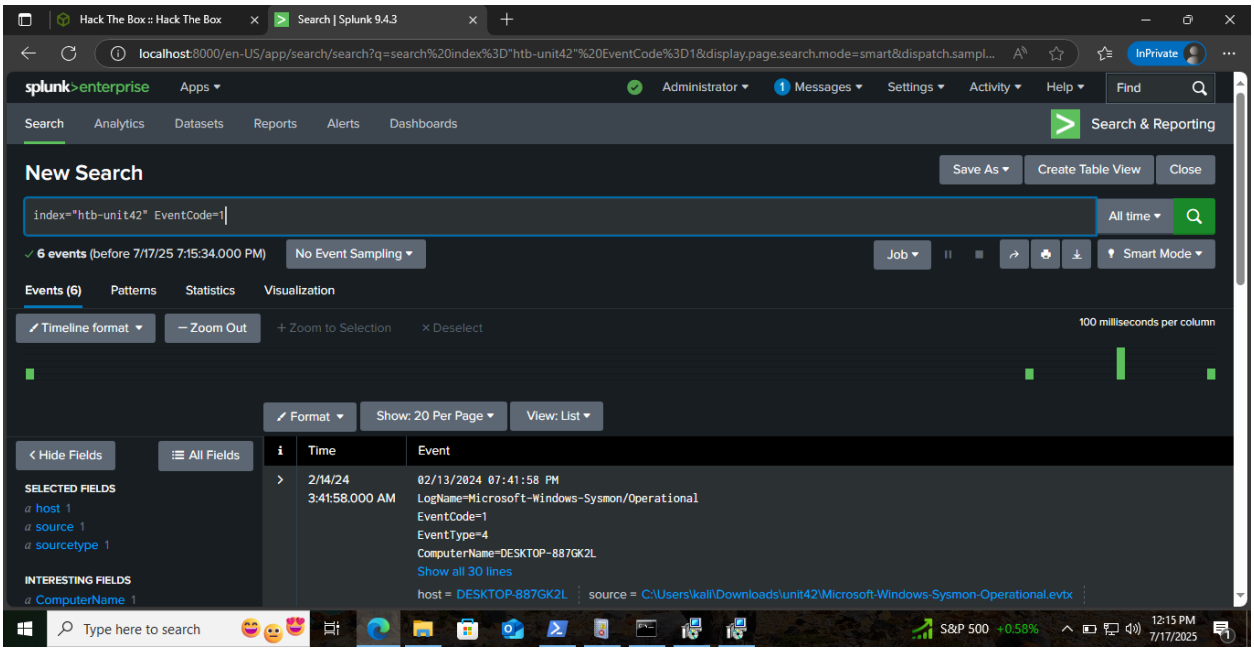
- **Splunk Query:** `index="htb_unit42" EventCode=11`
- **Findings:** 56 file creation/overwrite events

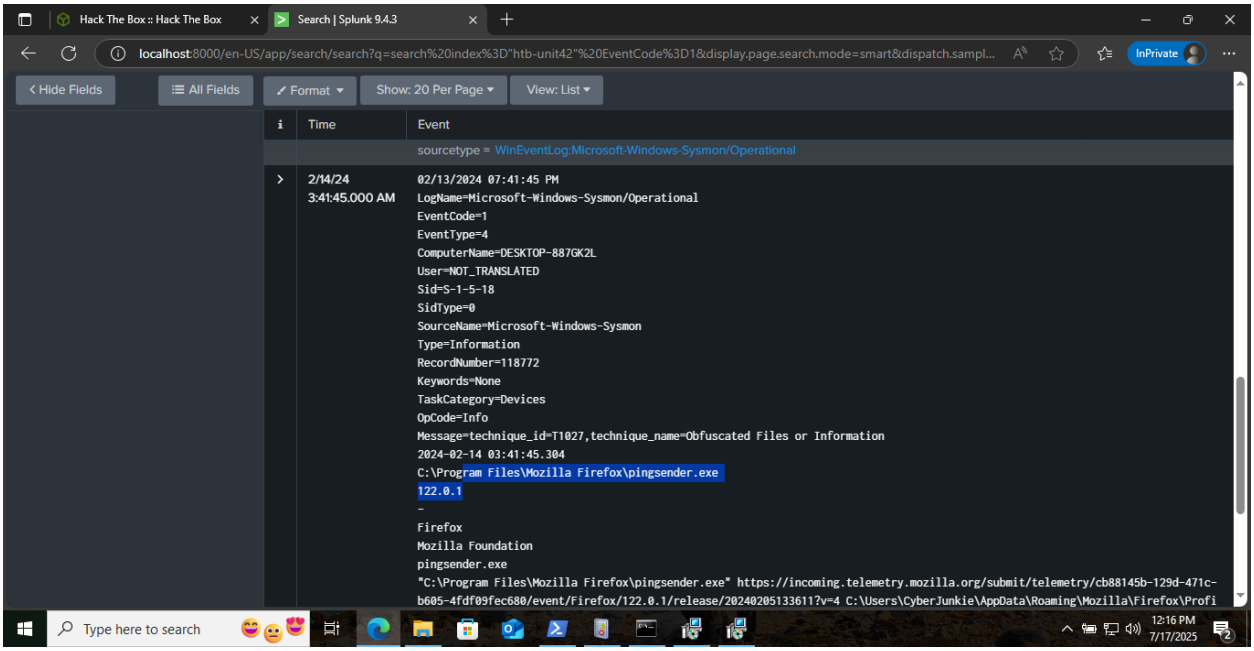


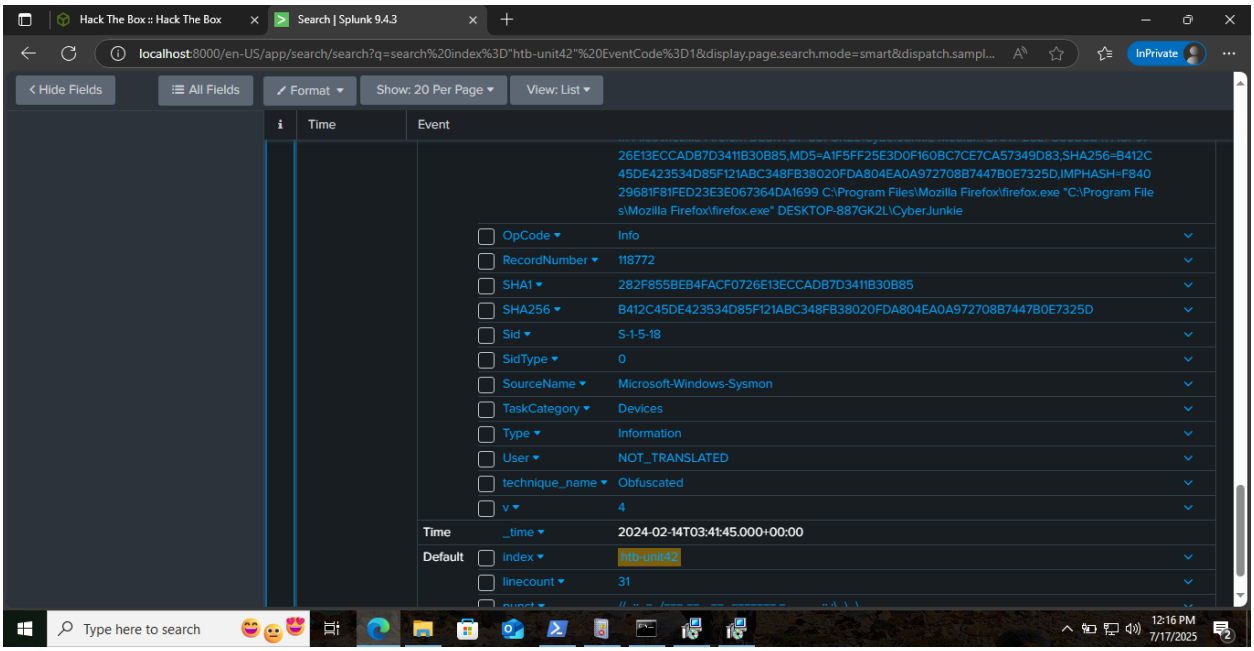


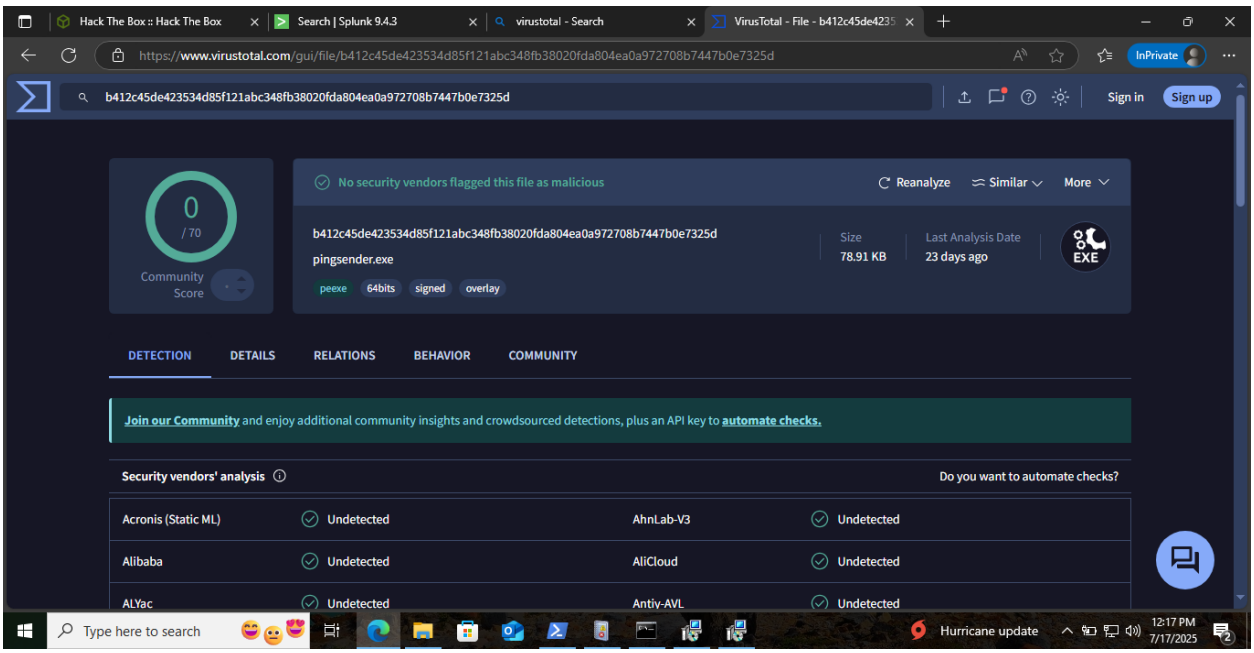
Q2. Malicious Process Execution

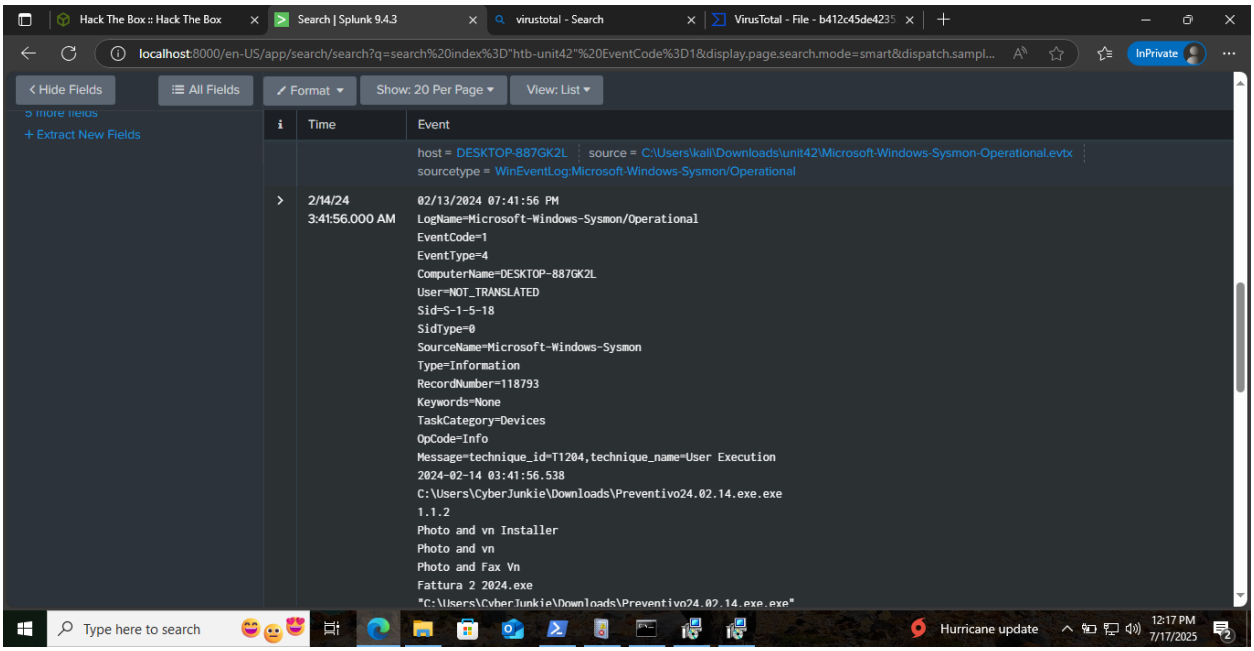
- **Query:** `index="htb-unit42" EventCode=1`
- Identified suspicious EXE:
  - `C:\Users\cyberjunkie\Downloads\preventivo_24.02.14.exe`
  - Flagged by 47 AV engines on VirusTotal (tagged: *UltraVNC, Backdoor*)

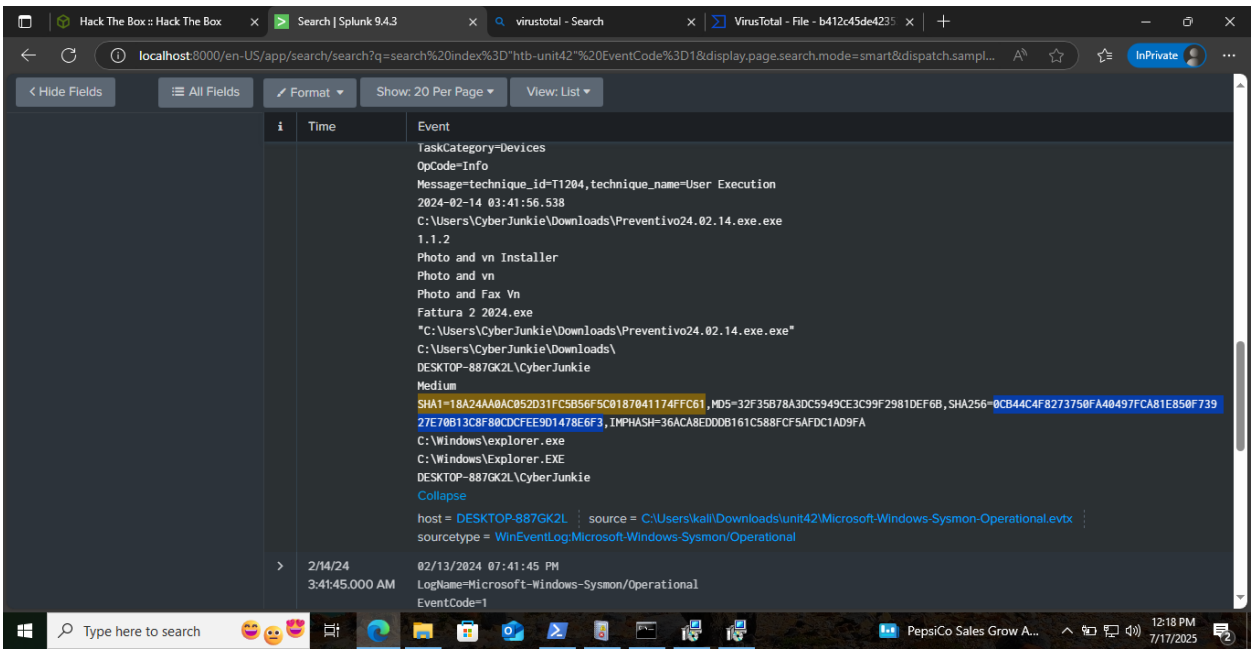

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D1&display.page.search.mode=smart&dispatch.sampl...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="htb-unit42" EventCode=1
All time
6 events (before 7/17/25 7:15:34.000 PM)
No Event Sampling
Job
Smart Mode
Events (6)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
100 milliseconds per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
Time
Event
2/14/24 3:41:58.000 AM
02/13/2024 07:41:58 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-887GK2L
Show all 30 lines
host = DESKTOP-887GK2L
source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
Type here to search
S&P 500 +0.58%
12:15 PM
7/17/2025

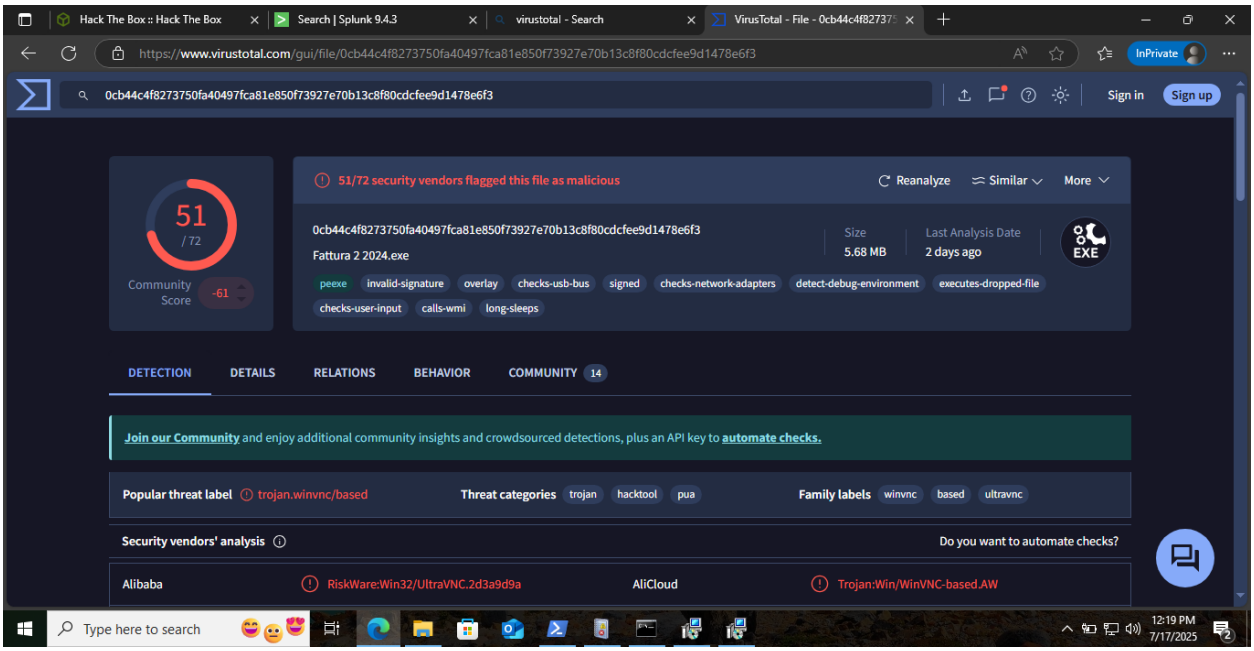

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D1&display.page.search.mode=smart&dispatch.sampl...
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
Time
Event
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24 3:41:45.000 AM
02/13/2024 07:41:45 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-887GK2L
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118772
Keywords=None
TaskCategory=Devices
OpCode=Info
Message=technique_id=T1027,technique_name=Obfuscated Files or Information
2024-02-14 03:41:45.304
C:\Program Files\Mozilla Firefox\pingsender.exe
122.0.1
-
Firefox
Mozilla Foundation
pingsender.exe
"C:\Program Files\Mozilla Firefox\pingsender.exe" https://incoming.telemetry.mozilla.org/submit/telemetry/cb88145b-129d-471c-b605-4fdf09fec680/event/Firefox/122.0.1/release/20240205133611?v=4 C:\Users\CyberJunkie\AppData\Roaming\Mozilla\Firefox\Profi
Type here to search
12:16 PM
7/17/2025

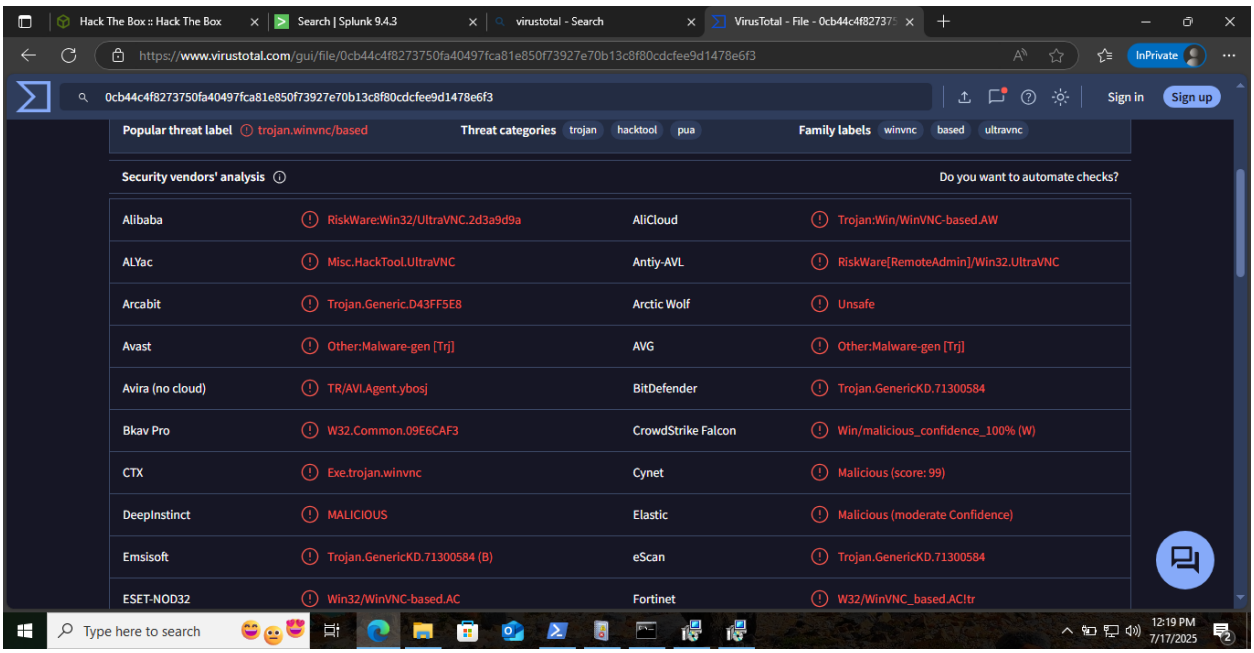

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D1&display.page.search.mode=smart&dispatch.sampl...
InPrivate
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
Time
Event
26E13ECCADB7D3411B30B85,MD5=A1F5FF25E3D0F160BC7CE7CA57349D83,SHA256=B412C45DE423534D85F121ABC348FB38020FDA804EA0A972708B7447B0E7325D,IMPHASH=F84029681F81FED23E3E067364DA1699 C:\Program Files\Mozilla Firefox\firefox.exe "C:\Program Files\Mozilla Firefox\firefox.exe" DESKTOP-887GK2L\CyberJunkie
OpCode Info
RecordNumber 118772
SHA1 282F855BEB4FACF0726E13ECCADB7D3411B30B85
SHA256 B412C45DE423534D85F121ABC348FB38020FDA804EA0A972708B7447B0E7325D
Sid S-1-5-18
SidType 0
SourceName Microsoft-Windows-Sysmon
TaskCategory Devices
Type Information
User NOT_TRANSLATED
technique_name Obfuscated
v 4
Time _time 2024-02-14T03:41:45.000+00:00
Default index htb-unit42
linecount 31
Type here to search
12:16 PM
7/17/2025

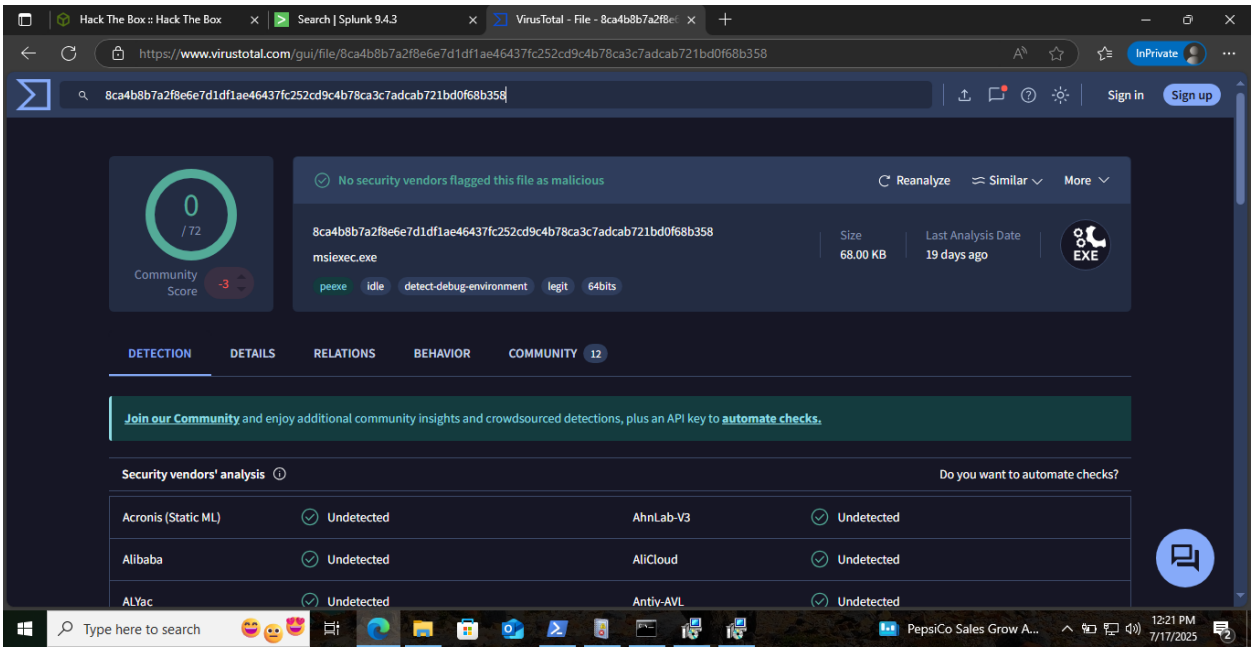

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
virustotal - Search
VirusTotal - File - b412c45de423...
https://www.virustotal.com/gui/file/b412c45de423534d85f121abc348fb38020fda804ea0a972708b7447b0e7325d
InPrivate
b412c45de423534d85f121abc348fb38020fda804ea0a972708b7447b0e7325d
Sign in
Sign up
0
/ 70
Community Score
No security vendors flagged this file as malicious
Reanalyze
Similar
More
b412c45de423534d85f121abc348fb38020fda804ea0a972708b7447b0e7325d
pingsender.exe
peexe
64bits
signed
overlay
Size
78.91 KB
Last Analysis Date
23 days ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML)
Undetected
AhnLab-V3
Undetected
Alibaba
Undetected
AliCloud
Undetected
ALYac
Undetected
Antiy-AVL
Undetected
Type here to search
Hurricane update
12:17 PM
7/17/2025

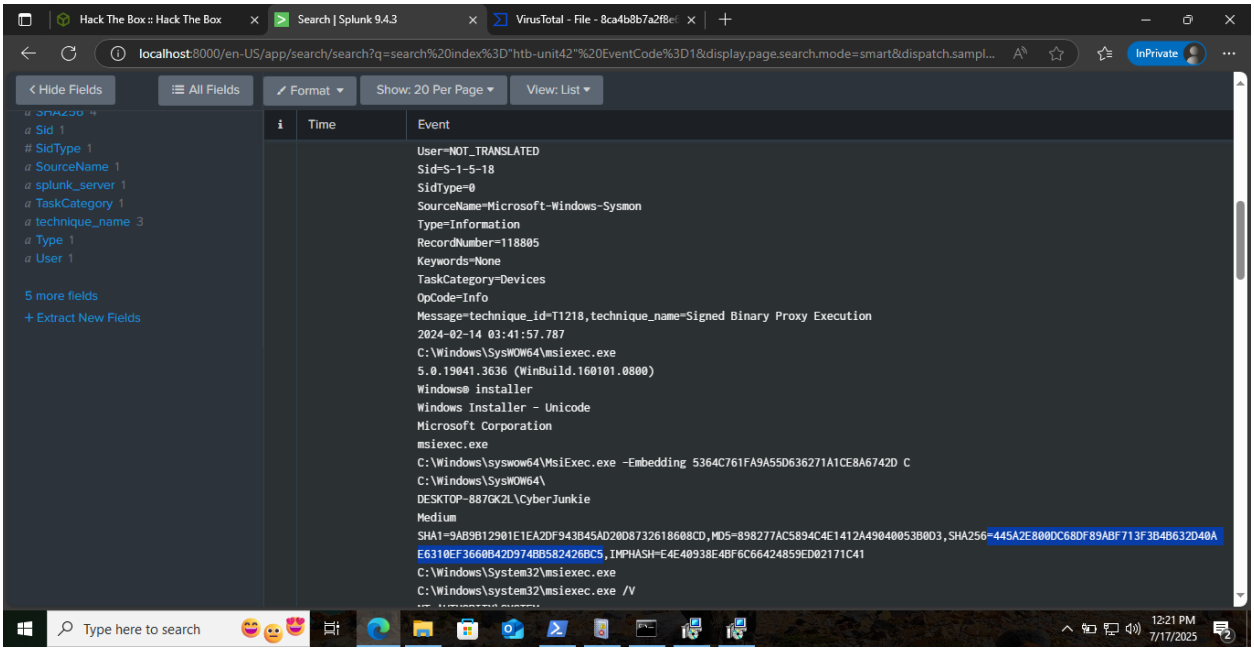

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
virustotal - Search
VirusTotal - File - b412c45de4235
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D1&display.page.search.mode=smart&dispatch.sampl...
InPrivate
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
+ Extract New Fields
Time
Event
host = DESKTOP-887GK2L source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24 3:41:56.000 AM
02/13/2024 07:41:56 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-887GK2L
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118793
Keywords=None
TaskCategory=Devices
OpCode=Info
Message=technique_id=T1204,technique_name=User Execution
2024-02-14 03:41:56.538
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
1.1.2
Photo and vn Installer
Photo and vn
Photo and Fax Vn
Fattura 2 2024.exe
Type here to search
Hurricane update
12:17 PM
7/17/2025

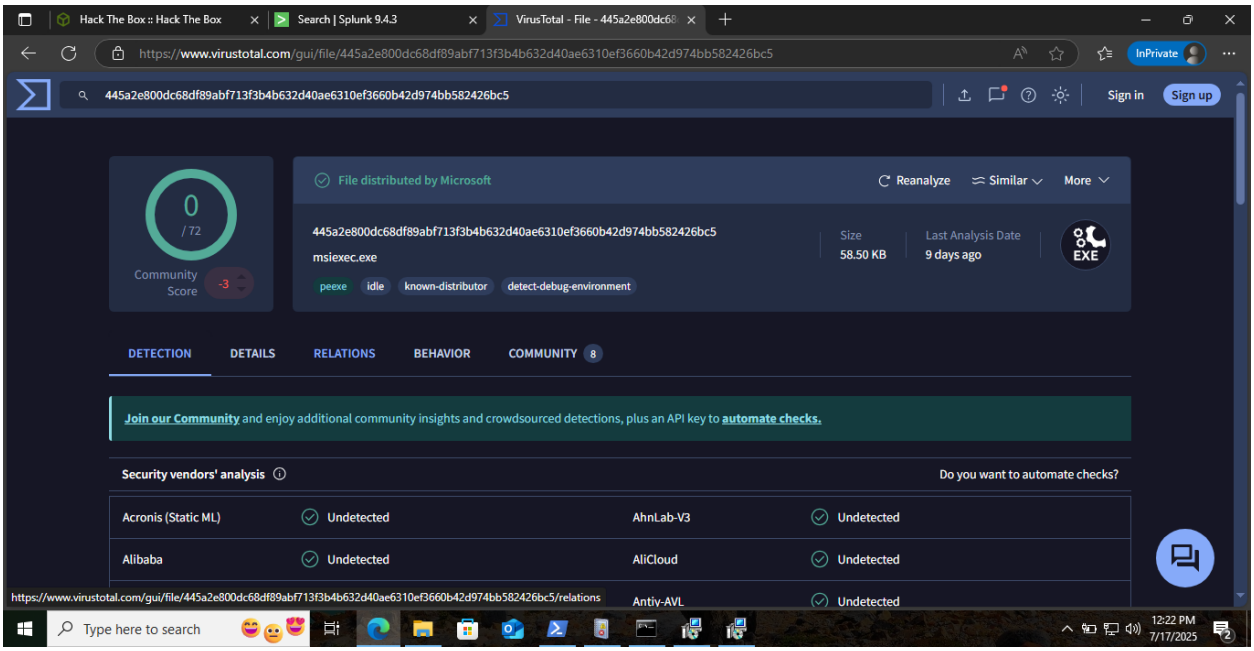

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
virustotal - Search
VirusTotal - File - b412c45de4235
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D1&display.page.search.mode=smart&dispatch.sampl...
InPrivate
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
Time
Event
TaskCategory=Devices
OpCode=Info
Message=technique_id=T1204,technique_name=User Execution
2024-02-14 03:41:56.538
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
1.1.2
Photo and vn Installer
Photo and vn
Photo and Fax Vn
Fattura 2 2024.exe
"C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe"
C:\Users\CyberJunkie\Downloads\
DESKTOP-887GK2L\CyberJunkie
Medium
SHA1=18A24AA0AC052D31FC5B56F5C0187041174FFC61,MD5=32F35B78A3DC5949CE3C99F2981DEF6B,SHA256=0CB44C4F8273750FA40497FCA81E850F73927E70B13C8F80CDCFEE9D1478E6F3,IMPHASH=36ACA8EDDDB161C588FCF5AFDC1AD9FA
C:\Windows\explorer.exe
C:\Windows\Explorer.EXE
DESKTOP-887GK2L\CyberJunkie
Collapse
host = DESKTOP-887GK2L source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24 3:41:45.000 AM
02/13/2024 07:41:45 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
Type here to search
PepsiCo Sales Grow A...
12:18 PM
7/17/2025


Hack The Box :: Hack The Box
Search | Splunk 9.4.3
virustotal - Search
VirusTotal - File - 0cb44c4f82737
https://www.virustotal.com/gui/file/0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3
InPrivate
0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3
Sign in
Sign up
51
/ 72
Community Score
-61
51/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3
Fattura 2 2024.exe
Size
5.68 MB
Last Analysis Date
2 days ago
EXE
peexe
invalid-signature
overlay
checks-usb-bus
signed
checks-network-adapters
detect-debug-environment
executes-dropped-file
checks-user-input
calls-wmi
long-sleeps
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 14
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.winvnc/based
Threat categories trojan hacktool pua
Family labels winvnc based ultravnc
Security vendors' analysis
Do you want to automate checks?
Alibaba
RiskWare:Win32/UltraVNC.2d3a9d9a
AliCloud
Trojan:Win/WinVNC-based.AW
Type here to search
12:19 PM
7/17/2025


Hack The Box :: Hack The Box
Search | Splunk 9.4.3
virustotal - Search
VirusTotal - File - 0cb44c4f82737
https://www.virustotal.com/gui/file/0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3
InPrivate
0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3
Sign in
Sign up
Popular threat label trojan.winvnc/based
Threat categories trojan hacktool pua
Family labels winvnc based ultravnc
Security vendors' analysis
Do you want to automate checks?
Alibaba
RiskWare:Win32/UltraVNC.2d3a9d9a
AliCloud
Trojan:Win/WinVNC-based.AW
ALYac
Misc.HackTool.UltraVNC
Antiy-AVL
RiskWare[RemoteAdmin]/Win32.UltraVNC
Arcabit
Trojan.Generic.D43FF5E8
Arctic Wolf
Unsafe
Avast
Other:Malware-gen [Trj]
AVG
Other:Malware-gen [Trj]
Avira (no cloud)
TR/AVI.Agent.ybosj
BitDefender
Trojan.GenericKD.71300584
Bkav Pro
W32.Common.09E6CAF3
CrowdStrike Falcon
Win/malicious_confidence_100% (W)
CTX
Exe.trojan.winvnc
Cynet
Malicious (score: 99)
DeepInstinct
MALICIOUS
Elastic
Malicious (moderate Confidence)
Emsisoft
Trojan.GenericKD.71300584 (B)
eScan
Trojan.GenericKD.71300584
ESET-NOD32
Win32/WinVNC-based.AC
Fortinet
W32/WinVNC_based.AC!tr
Type here to search
12:19 PM
7/17/2025

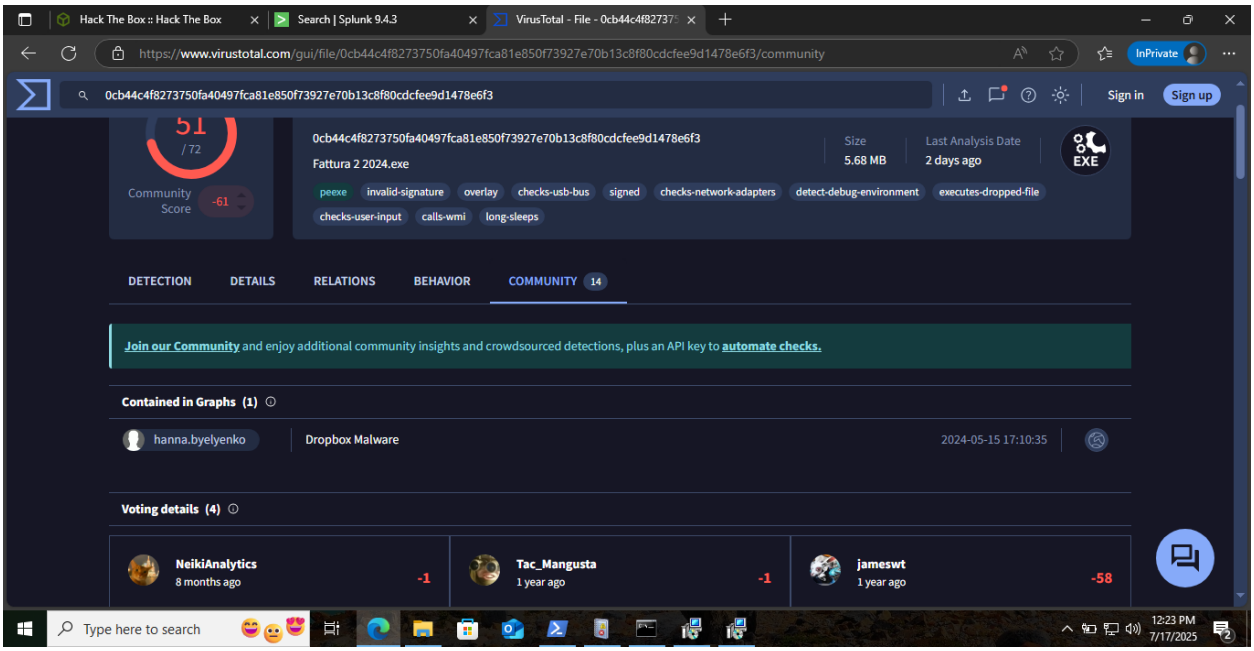

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 8ca4b8b7a2f8e6
https://www.virustotal.com/gui/file/8ca4b8b7a2f8e6e7d1df1ae46437fc252cd9c4b78ca3c7adcab721bd0f68b358
InPrivate
8ca4b8b7a2f8e6e7d1df1ae46437fc252cd9c4b78ca3c7adcab721bd0f68b358
Sign in
Sign up
0
/ 72
Community Score
-3
No security vendors flagged this file as malicious
Reanalyze
Similar
More
8ca4b8b7a2f8e6e7d1df1ae46437fc252cd9c4b78ca3c7adcab721bd0f68b358
msiexec.exe
peexe
idle
detect-debug-environment
legit
64bits
Size
68.00 KB
Last Analysis Date
19 days ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 12
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML)
Undetected
AhnLab-V3
Undetected
Alibaba
Undetected
AliCloud
Undetected
ALYac
Undetected
Antiy-AVL
Undetected
Type here to search
PepsiCo Sales Grow A...
12:21 PM
7/17/2025

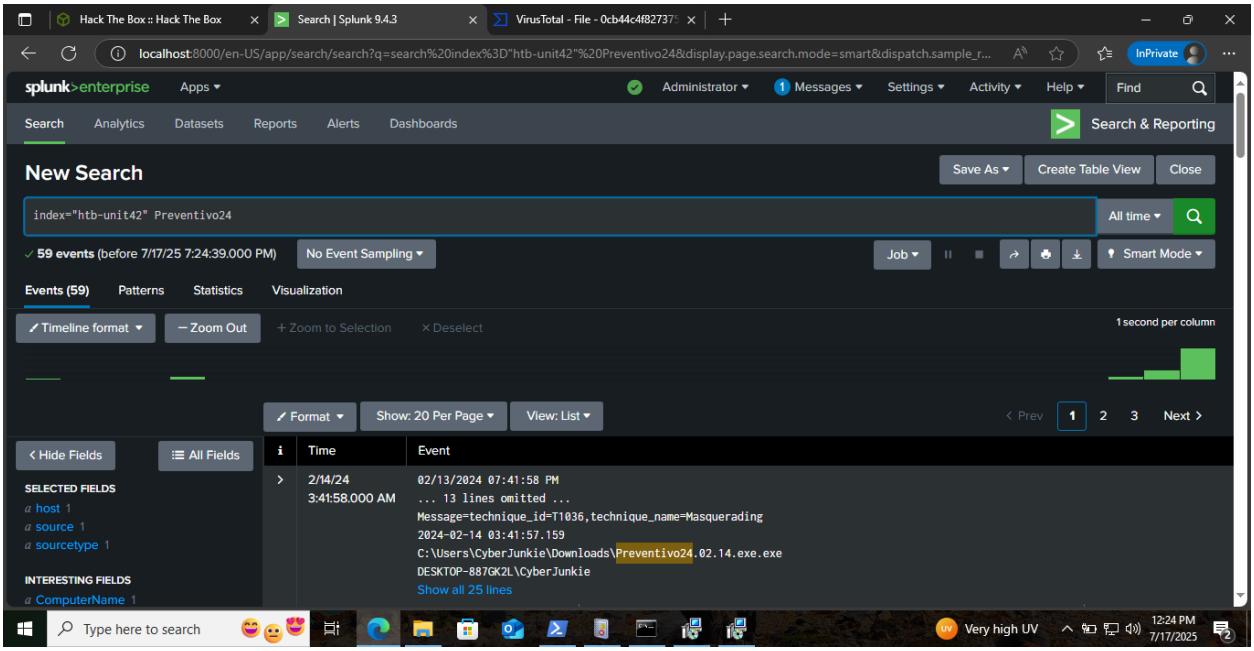

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 8ca4b8b7a2f8e6
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D1&display.page.search.mode=smart&dispatch.sampl...
InPrivate
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
Sid 1
SidType 1
SourceName 1
splunk_server 1
TaskCategory 1
technique_name 3
Type 1
User 1
5 more fields
Extract New Fields
Time
Event
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118805
Keywords=None
TaskCategory=Devices
OpCode=Info
Message=technique_id=T1218,technique_name=Signed Binary Proxy Execution
2024-02-14 03:41:57.787
C:\Windows\SysWOW64\msiexec.exe
5.0.19041.3636 (WinBuild.160101.0800)
Windows® installer
Windows Installer - Unicode
Microsoft Corporation
msiexec.exe
C:\Windows\syswow64\MsiExec.exe -Embedding 5364C761FA9A55D636271A1CE8A6742D C
C:\Windows\SysWOW64\
DESKTOP-887GK2L\CyberJunkie
Medium
SHA1=9AB9B12901E1EA2DF943B45AD20D8732618608CD,MD5=898277AC5894C4E1412A49040053B0D3,SHA256=445A2E800DC68DF89ABF713F3B4B632D40AE6310EF3660B42D974BB582426BC5,IMPHASH=E4E40938E4BF6C66424859ED02171C41
C:\Windows\System32\msiexec.exe
C:\Windows\system32\msiexec.exe /V
Type here to search
12:21 PM
7/17/2025

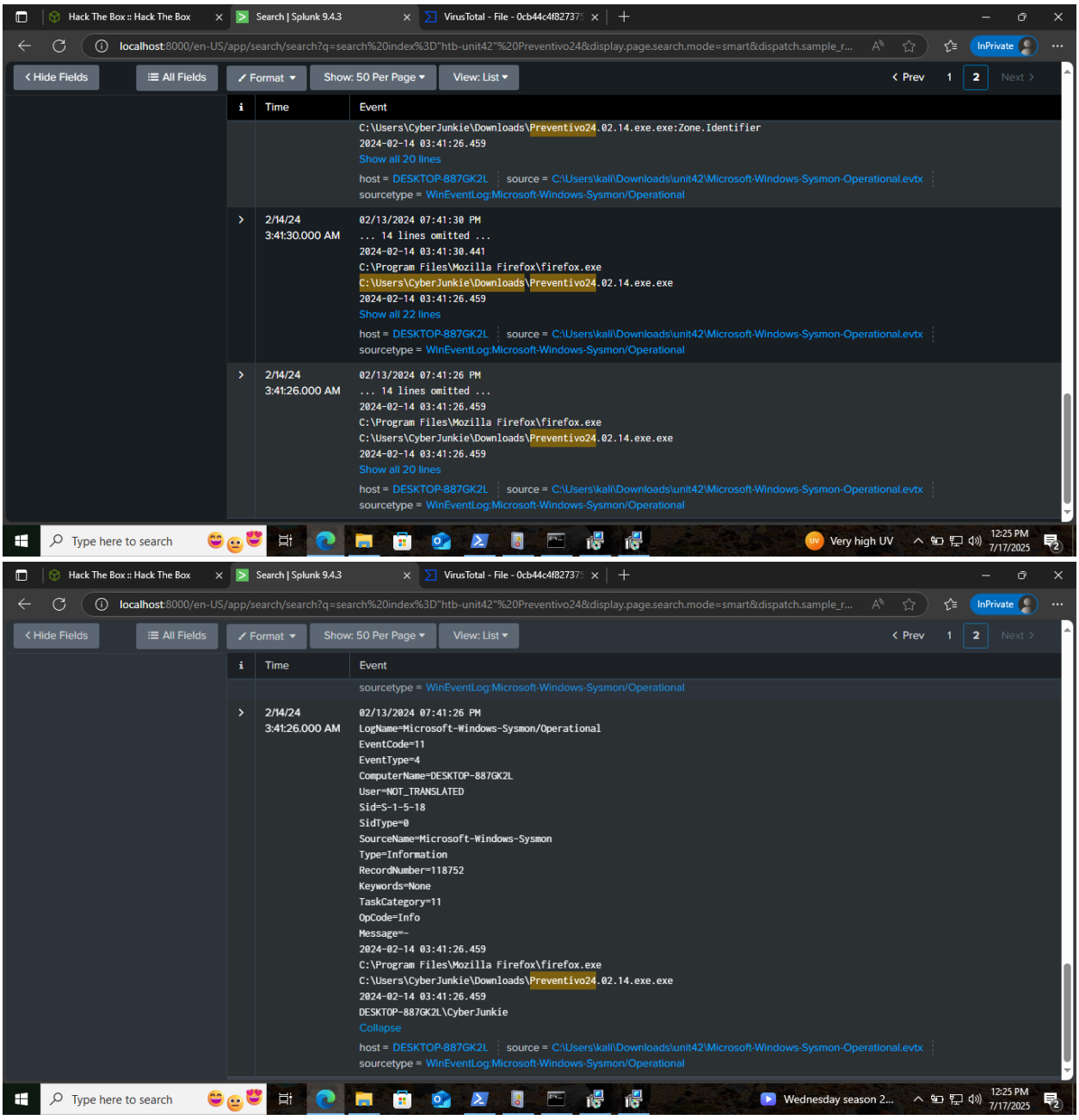


Q3. Cloud Distribution Channel

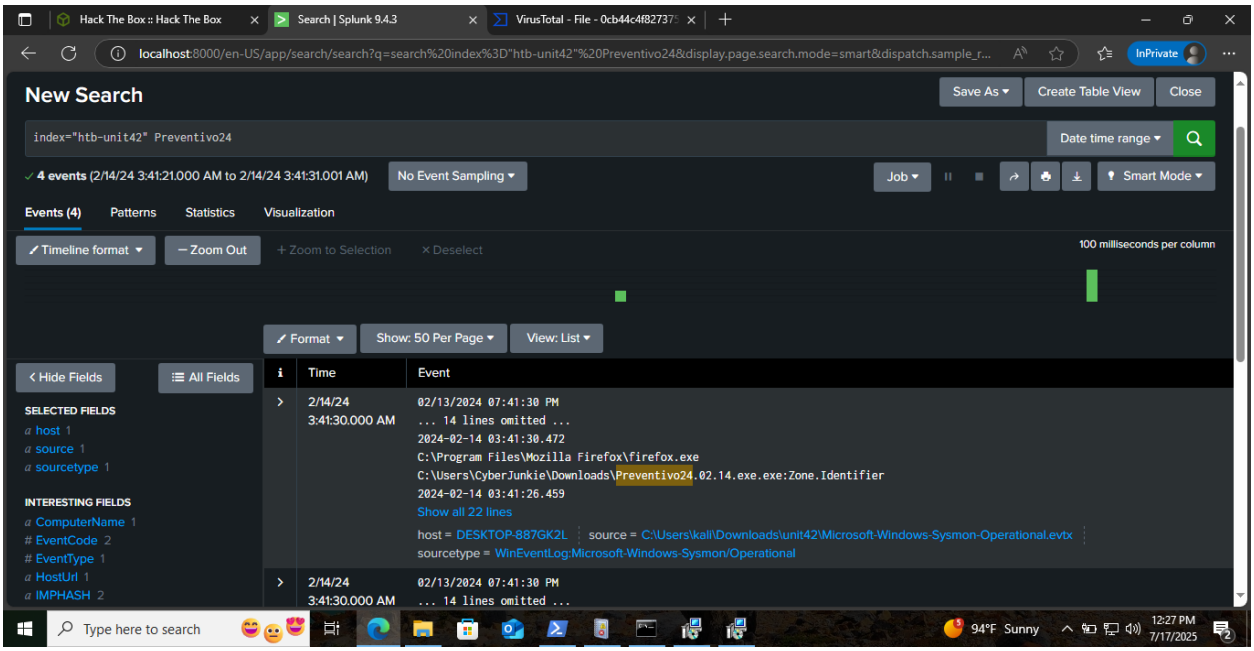
- VirusTotal comments showed usage of Dropbox
- Event ID 15 revealed:
  - URL: `https://www.dropbox.com/s/...`

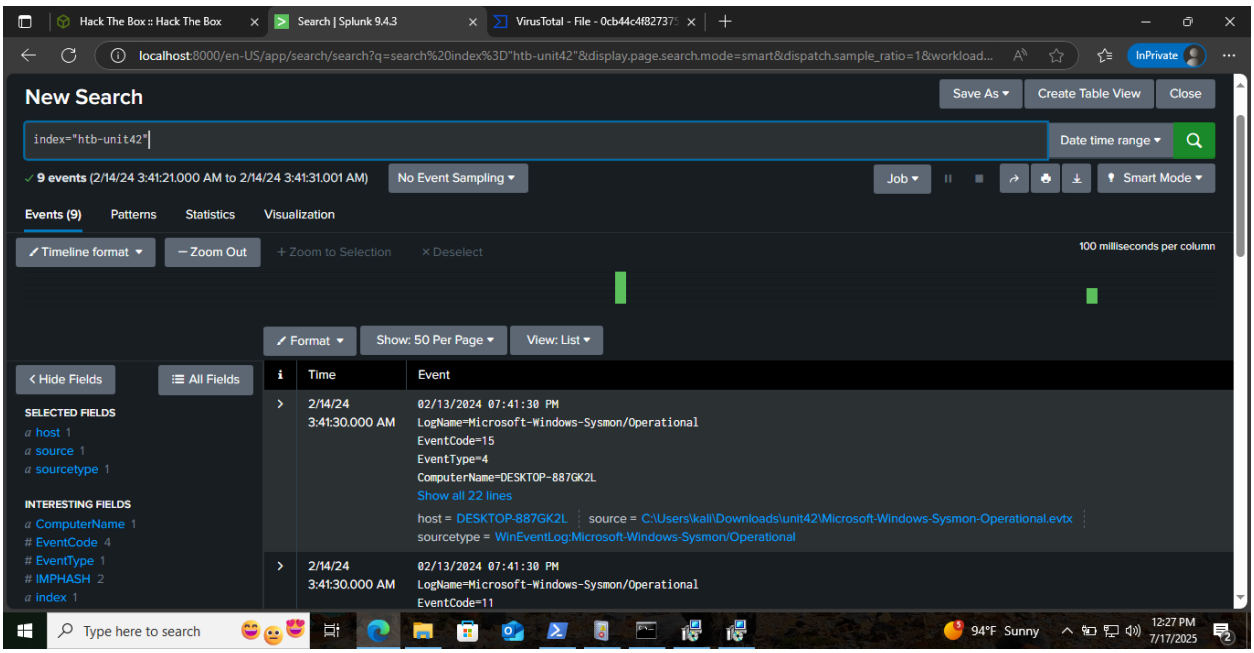

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
https://www.virustotal.com/gui/file/0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3/community
InPrivate
0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3
Sign in
Sign up
51
/ 72
Community Score
-61
0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3
Fattura 2 2024.exe
Size
5.68 MB
Last Analysis Date
2 days ago
EXE
peexe
invalid-signature
overlay
checks-usb-bus
signed
checks-network-adapters
detect-debug-environment
executes-dropped-file
checks-user-input
calls-wmi
long-sleeps
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 14
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Contained in Graphs (1)
hanna.byelyenko
Dropbox Malware
2024-05-15 17:10:35
Voting details (4)
NeikiAnalytics
8 months ago
-1
Tac_Mangusta
1 year ago
-1
jameswt
1 year ago
-58
Type here to search
12:23 PM
7/17/2025

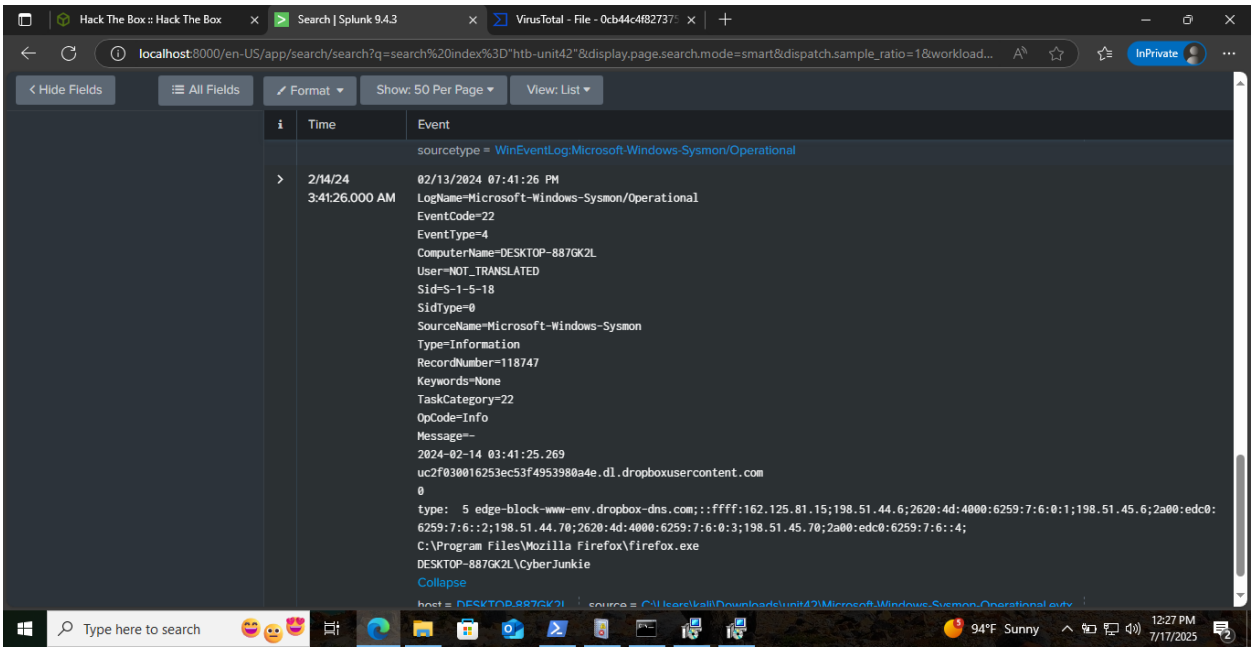

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20Preventivo24&display.page.search.mode=smart&dispatch.sample_r...
InPrivate
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="htb-unit42" Preventivo24
All time
59 events (before 7/17/25 7:24:39.000 PM)
No Event Sampling
Job
Smart Mode
Events (59)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 second per column
Format
Show: 20 Per Page
View: List
Prev
1
2
3
Next
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
Time
Event
2/14/24
3:41:58.000 AM
02/13/2024 07:41:58 PM
... 13 lines omitted ...
Message=technique_id=T1036,technique_name=Masquerading
2024-02-14 03:41:57.159
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
DESKTOP-887GK2L\CyberJunkie
Show all 25 lines
Type here to search
Very high UV
12:24 PM
7/17/2025

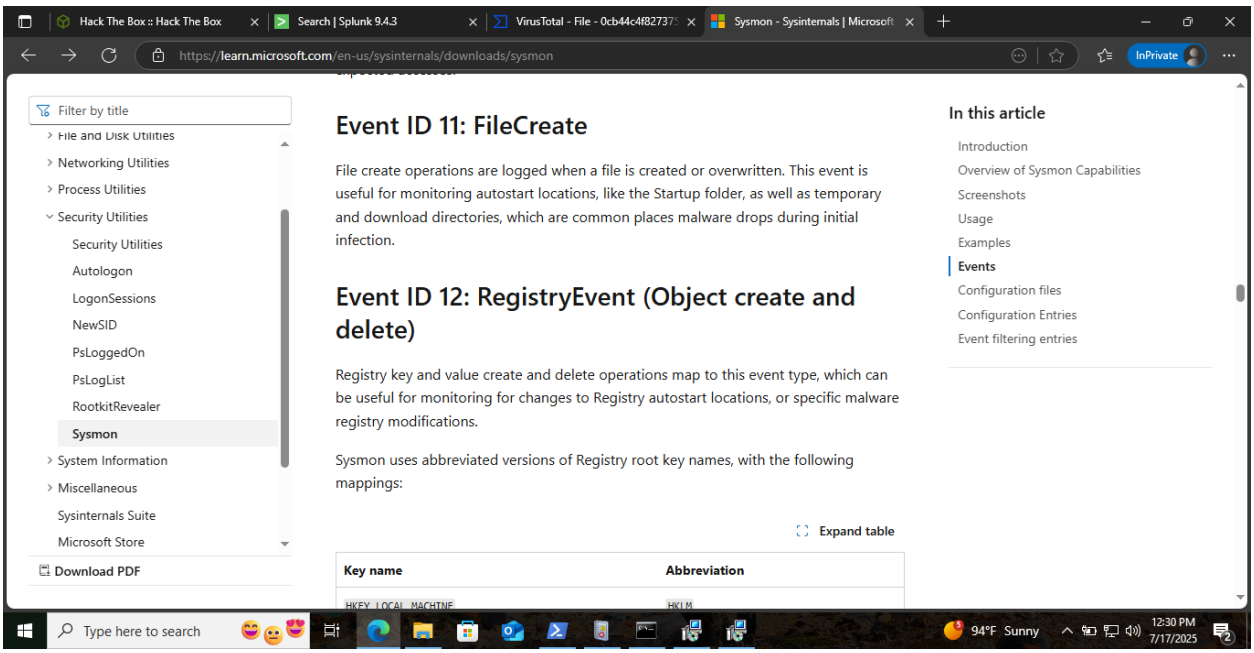

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20Preventivo24&display.page.search.mode=smart&dispatch.sample_r...
InPrivate
Hide Fields
All Fields
Format
Show: 50 Per Page
View: List
Prev 1 2 Next
Time
Event
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe:Zone.Identifier
2024-02-14 03:41:26.459
Show all 20 lines
host = DESKTOP-887GK2L source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24 3:41:30.000 AM
02/13/2024 07:41:30 PM
... 14 lines omitted ...
2024-02-14 03:41:30.441
C:\Program Files\Mozilla Firefox\firefox.exe
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
2024-02-14 03:41:26.459
Show all 22 lines
host = DESKTOP-887GK2L source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24 3:41:26.000 AM
02/13/2024 07:41:26 PM
... 14 lines omitted ...
2024-02-14 03:41:26.459
C:\Program Files\Mozilla Firefox\firefox.exe
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
2024-02-14 03:41:26.459
Show all 20 lines
host = DESKTOP-887GK2L source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
Type here to search
Very high UV
12:25 PM
7/17/2025

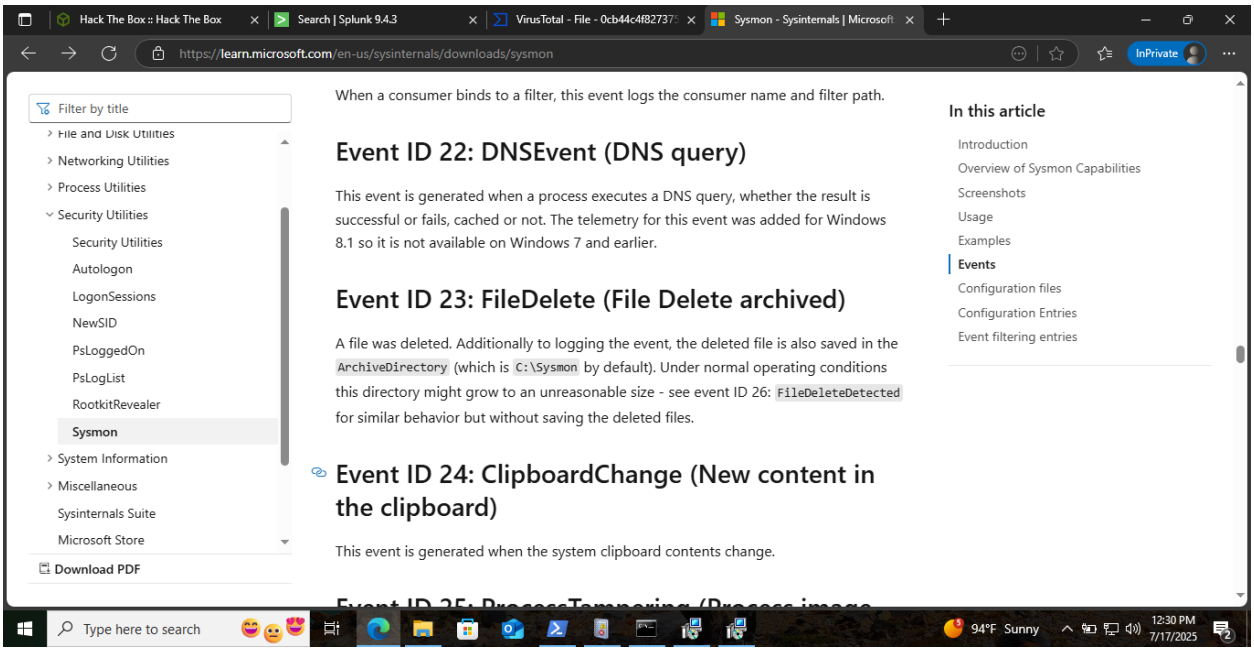
Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20Preventivo24&display.page.search.mode=smart&dispatch.sample_r...
InPrivate
Hide Fields
All Fields
Format
Show: 50 Per Page
View: List
Prev 1 2 Next
Time
Event
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24 3:41:26.000 AM
02/13/2024 07:41:26 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=11
EventType=4
ComputerName=DESKTOP-887GK2L
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118752
Keywords=None
TaskCategory=11
OpCode=Info
Message=-
2024-02-14 03:41:26.459
C:\Program Files\Mozilla Firefox\firefox.exe
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
2024-02-14 03:41:26.459
DESKTOP-887GK2L\CyberJunkie
Collapse
host = DESKTOP-887GK2L source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
Type here to search
Wednesday season 2...
12:25 PM
7/17/2025

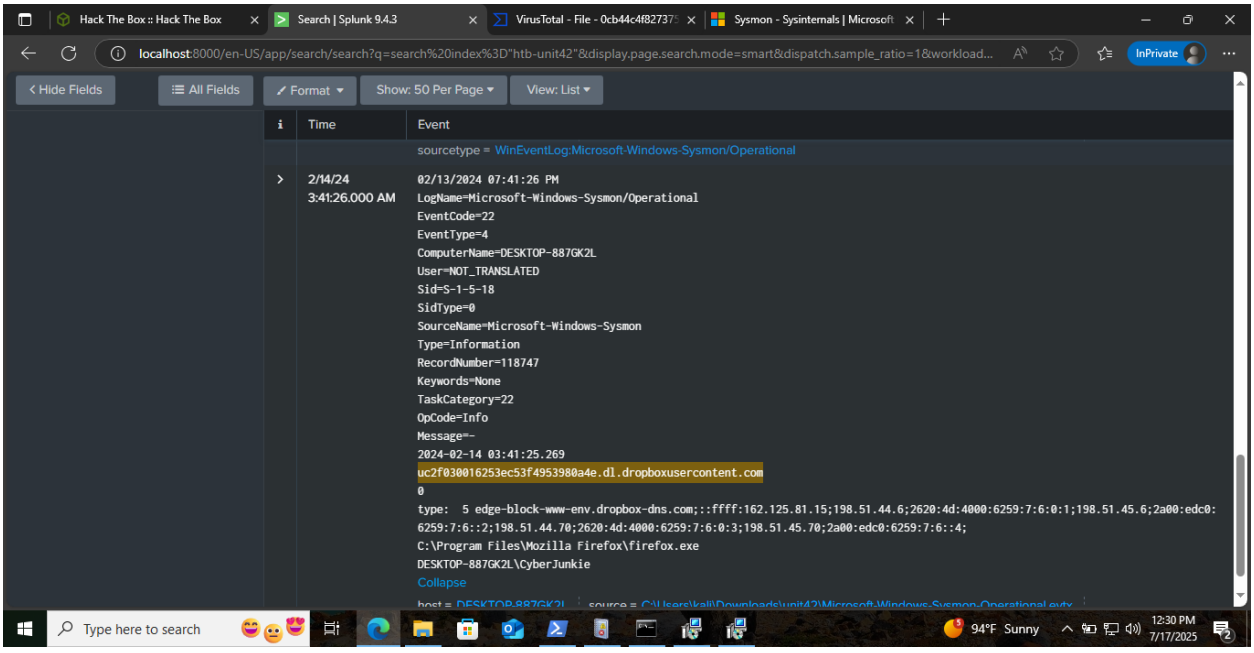

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20Preventivo24&display.page.search.mode=smart&dispatch.sample_r...
InPrivate
New Search
Save As
Create Table View
Close
index="htb-unit42" Preventivo24
Date time range
4 events (2/14/24 3:41:21.000 AM to 2/14/24 3:41:31.001 AM)
No Event Sampling
Job
Smart Mode
Events (4)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
100 milliseconds per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
EventCode 2
EventType 1
HostUrl 1
IMPHASH 2
Time
Event
2/14/24 3:41:30.000 AM
02/13/2024 07:41:30 PM
... 14 lines omitted ...
2024-02-14 03:41:30.472
C:\Program Files\Mozilla Firefox\firefox.exe
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe:Zone.Identifier
2024-02-14 03:41:26.459
Show all 22 lines
host = DESKTOP-887GK2L
source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24 3:41:30.000 AM
02/13/2024 07:41:30 PM
... 14 lines omitted ...
Type here to search
94°F Sunny
12:27 PM
7/17/2025

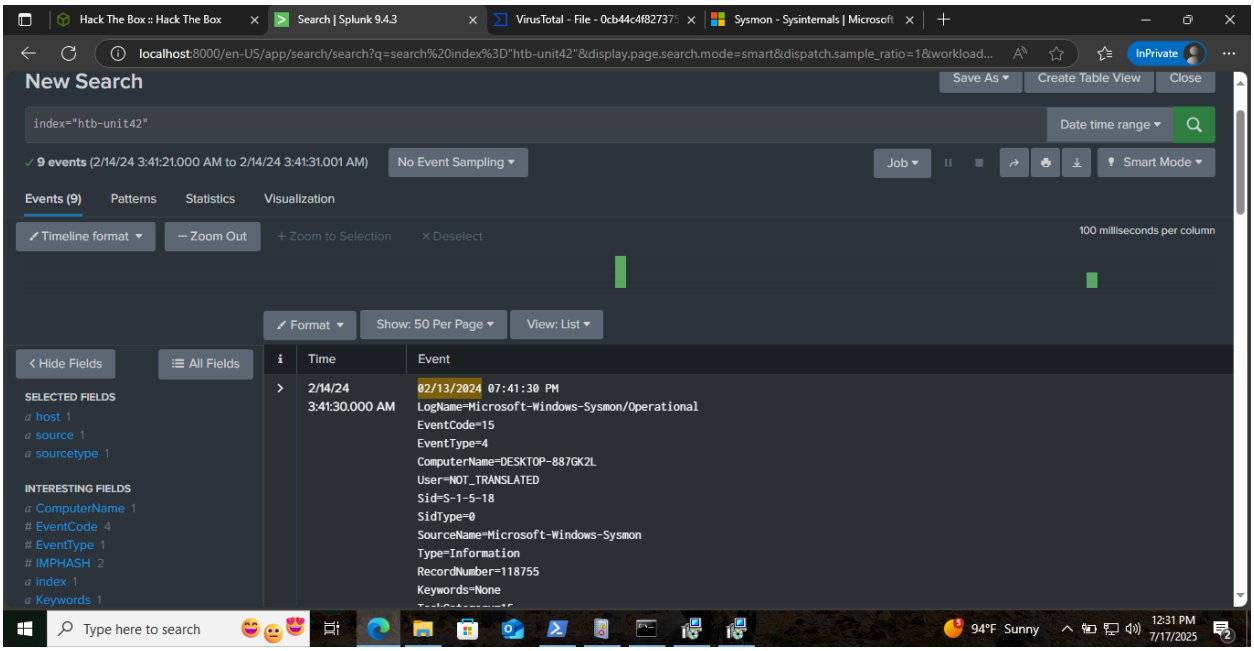

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"&display.page.search.mode=smart&dispatch.sample_ratio=1&workload...
InPrivate
New Search
Save As
Create Table View
Close
index="htb-unit42"
Date time range
9 events (2/14/24 3:41:21.000 AM to 2/14/24 3:41:31.001 AM)
No Event Sampling
Job
Smart Mode
Events (9)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
100 milliseconds per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
EventCode 4
EventType 1
IMPHASH 2
index 1
Time
Event
2/14/24 3:41:30.000 AM
02/13/2024 07:41:30 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=15
EventType=4
ComputerName=DESKTOP-887GK2L
Show all 22 lines
host = DESKTOP-887GK2L
source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24 3:41:30.000 AM
02/13/2024 07:41:30 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=11
Type here to search
94°F Sunny
12:27 PM
7/17/2025

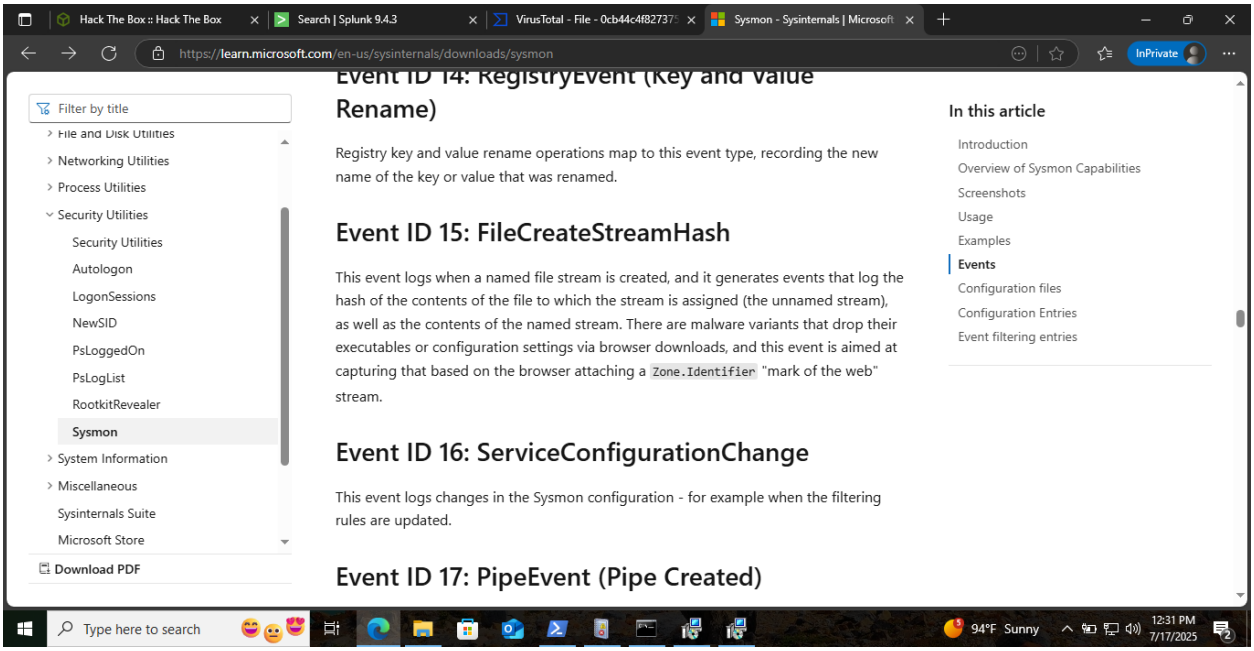

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"&display.page.search.mode=smart&dispatch.sample_ratio=1&workload...
InPrivate
Hide Fields
All Fields
Format
Show: 50 Per Page
View: List
Time
Event
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24 3:41:26.000 AM
02/13/2024 07:41:26 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=22
EventType=4
ComputerName=DESKTOP-887GK2L
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118747
Keywords=None
TaskCategory=22
OpCode=Info
Message=-
2024-02-14 03:41:25.269
uc2f030016253ec53f4953980a4e.dl.dropboxusercontent.com
0
type: 5 edge-block-www-env.dropbox-dns.com;::ffff:162.125.81.15;198.51.44.6;2620:4d:4000:6259:7:6:0:1;198.51.45.6;2a00:edc0:6259:7:6::2;198.51.44.70;2620:4d:4000:6259:7:6:0:3;198.51.45.70;2a00:edc0:6259:7:6::4;
C:\Program Files\Mozilla Firefox\firefox.exe
DESKTOP-887GK2L\CyberJunkie
Collapse
Type here to search
94°F Sunny
12:27 PM
7/17/2025

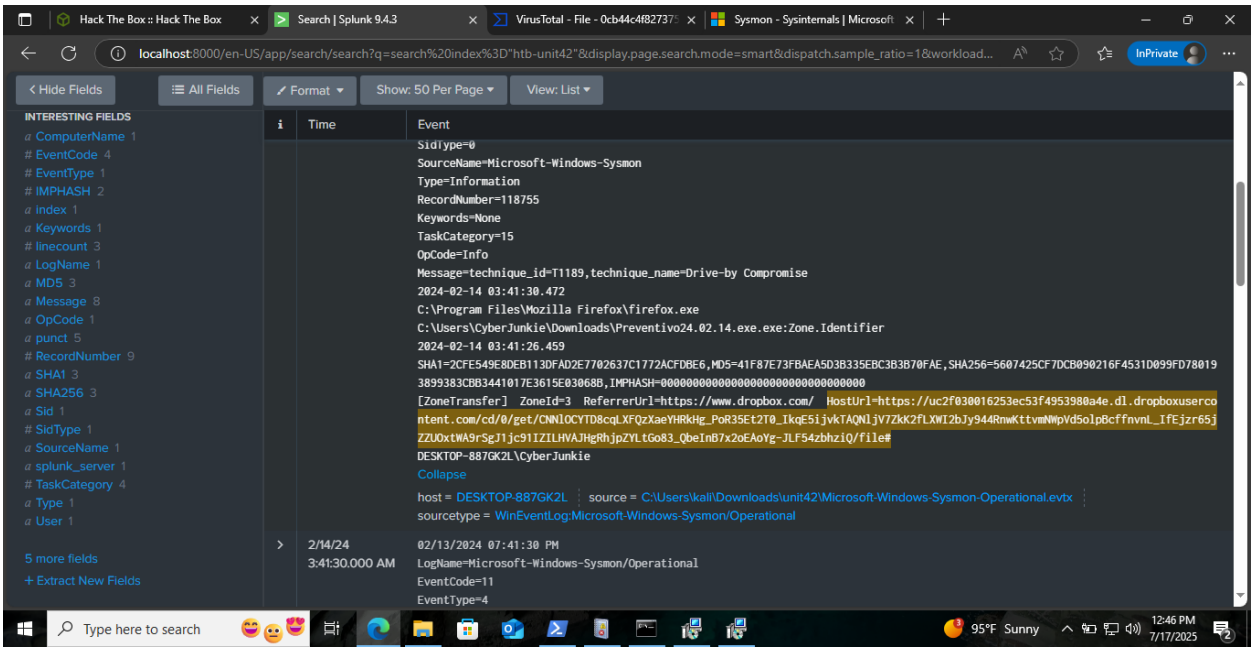

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
InPrivate
Filter by title
File and Disk Utilities
Networking Utilities
Process Utilities
Security Utilities
Security Utilities
Autologon
LogonSessions
NewSID
PsLoggedOn
PsLogList
RootkitRevealer
Sysmon
System Information
Miscellaneous
Sysinternals Suite
Microsoft Store
Download PDF
Event ID 11: FileCreate
File create operations are logged when a file is created or overwritten. This event is useful for monitoring autostart locations, like the Startup folder, as well as temporary and download directories, which are common places malware drops during initial infection.
Event ID 12: RegistryEvent (Object create and delete)
Registry key and value create and delete operations map to this event type, which can be useful for monitoring for changes to Registry autostart locations, or specific malware registry modifications.
Sysmon uses abbreviated versions of Registry root key names, with the following mappings:
Expand table
Key name
Abbreviation
HKEY_LOCAL_MACHINE
HKLM
In this article
Introduction
Overview of Sysmon Capabilities
Screenshots
Usage
Examples
Events
Configuration files
Configuration Entries
Event filtering entries
Type here to search
94°F Sunny
12:30 PM
7/17/2025


Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
InPrivate
Filter by title
File and Disk Utilities
Networking Utilities
Process Utilities
Security Utilities
Security Utilities
Autologon
LogonSessions
NewSID
PsLoggedOn
PsLogList
RootkitRevealer
Sysmon
System Information
Miscellaneous
Sysinternals Suite
Microsoft Store
Download PDF
When a consumer binds to a filter, this event logs the consumer name and filter path.
Event ID 22: DNSEvent (DNS query)
This event is generated when a process executes a DNS query, whether the result is successful or fails, cached or not. The telemetry for this event was added for Windows 8.1 so it is not available on Windows 7 and earlier.
Event ID 23: FileDelete (File Delete archived)
A file was deleted. Additionally to logging the event, the deleted file is also saved in the ArchiveDirectory (which is C:\Sysmon by default). Under normal operating conditions this directory might grow to an unreasonable size - see event ID 26: FileDeleteDetected for similar behavior but without saving the deleted files.
Event ID 24: ClipboardChange (New content in the clipboard)
This event is generated when the system clipboard contents change.
In this article
Introduction
Overview of Sysmon Capabilities
Screenshots
Usage
Examples
Events
Configuration files
Configuration Entries
Event filtering entries
Type here to search
94°F Sunny
12:30 PM
7/17/2025


Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"&display.page.search.mode=smart&dispatch.sample_ratio=1&workload...
InPrivate
Hide Fields
All Fields
Format
Show: 50 Per Page
View: List
Time
Event
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24
3:41:26.000 AM
02/13/2024 07:41:26 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=22
EventType=4
ComputerName=DESKTOP-887GK2L
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118747
Keywords=None
TaskCategory=22
OpCode=Info
Message=-
2024-02-14 03:41:25.269
uc2f030016253ec53f4953980a4e.dl.dropboxusercontent.com
0
type: 5 edge-block-www-env.dropbox-dns.com;::ffff:162.125.81.15;198.51.44.6;2620:4d:4000:6259:7:6:0:1;198.51.45.6;2a00:edc0:6259:7:6::2;198.51.44.70;2620:4d:4000:6259:7:6:0:3;198.51.45.70;2a00:edc0:6259:7:6::4;
C:\Program Files\Mozilla Firefox\firefox.exe
DESKTOP-887GK2L\CyberJunkie
Collapse
Type here to search
94°F Sunny
12:30 PM
7/17/2025

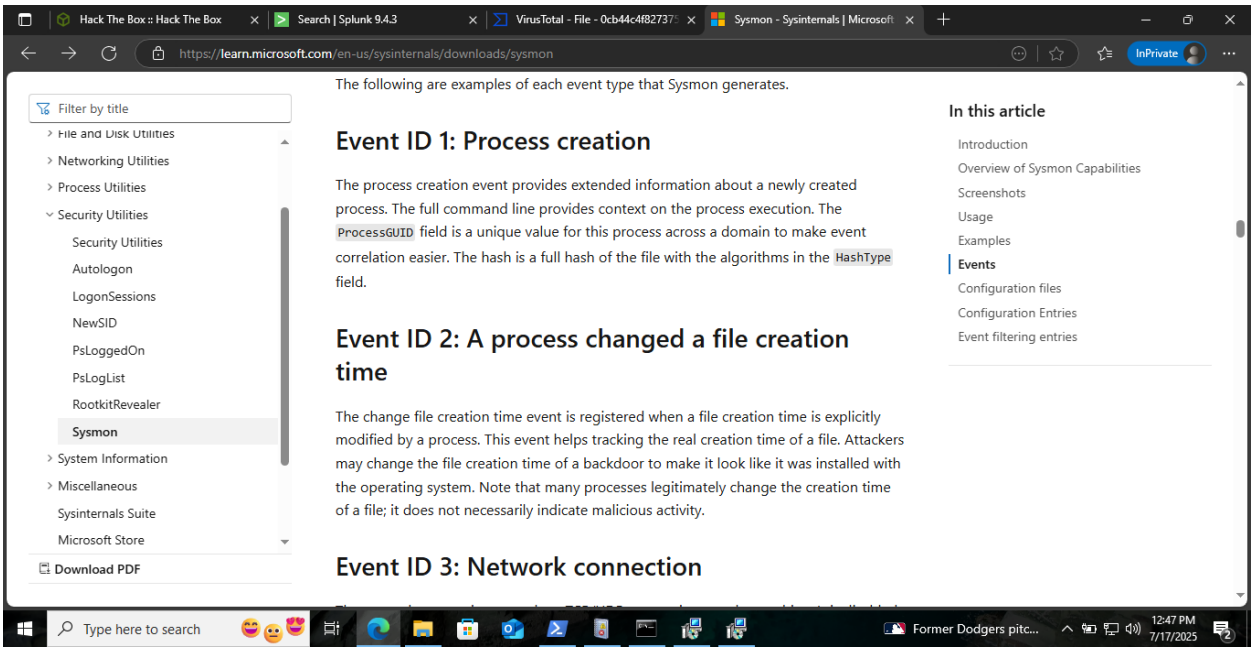

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f827373
Sysmon - Sysinternals | Microsoft
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"&display.page.search.mode=smart&dispatch.sample_ratio=1&workload...
InPrivate
New Search
Save As
Create Table View
Close
index="htb-unit42"
Date time range
9 events (2/14/24 3:41:21.000 AM to 2/14/24 3:41:31.001 AM)
No Event Sampling
Job
Smart Mode
Events (9)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
100 milliseconds per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
EventCode 4
EventType 1
IMPHASH 2
index 1
Keywords 1
Time
Event
2/14/24 3:41:30.000 AM
02/13/2024 07:41:30 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=15
EventType=4
ComputerName=DESKTOP-887GK2L
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118755
Keywords=None
Type here to search
94°F Sunny
12:31 PM
7/17/2025

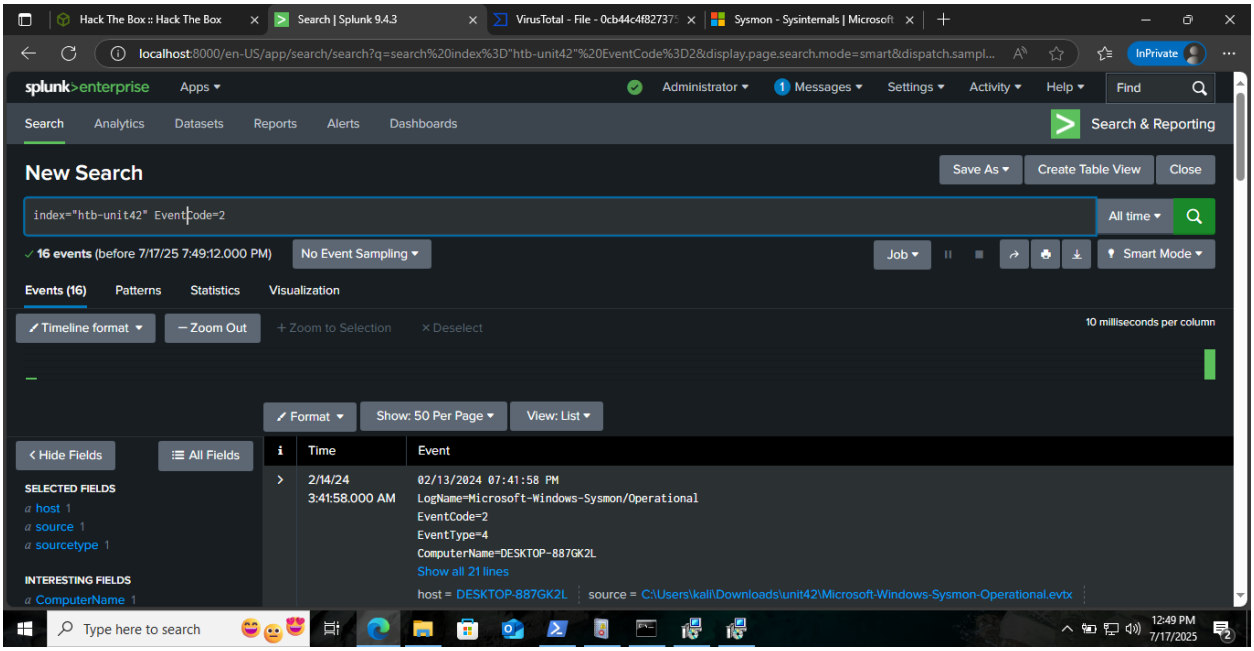

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f827373
Sysmon - Sysinternals | Microsoft
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
InPrivate
Filter by title
File and Disk Utilities
Networking Utilities
Process Utilities
Security Utilities
Security Utilities
Autologon
LogonSessions
NewSID
PsLoggedOn
PsLogList
RootkitRevealer
Sysmon
System Information
Miscellaneous
Sysinternals Suite
Microsoft Store
Download PDF
Event ID 14: RegistryEvent (Key and Value Rename)
Registry key and value rename operations map to this event type, recording the new name of the key or value that was renamed.
Event ID 15: FileCreateStreamHash
This event logs when a named file stream is created, and it generates events that log the hash of the contents of the file to which the stream is assigned (the unnamed stream), as well as the contents of the named stream. There are malware variants that drop their executables or configuration settings via browser downloads, and this event is aimed at capturing that based on the browser attaching a Zone.Identifier "mark of the web" stream.
Event ID 16: ServiceConfigurationChange
This event logs changes in the Sysmon configuration - for example when the filtering rules are updated.
Event ID 17: PipeEvent (Pipe Created)
In this article
Introduction
Overview of Sysmon Capabilities
Screenshots
Usage
Examples
Events
Configuration files
Configuration Entries
Event filtering entries
Type here to search
94°F Sunny
12:31 PM
7/17/2025

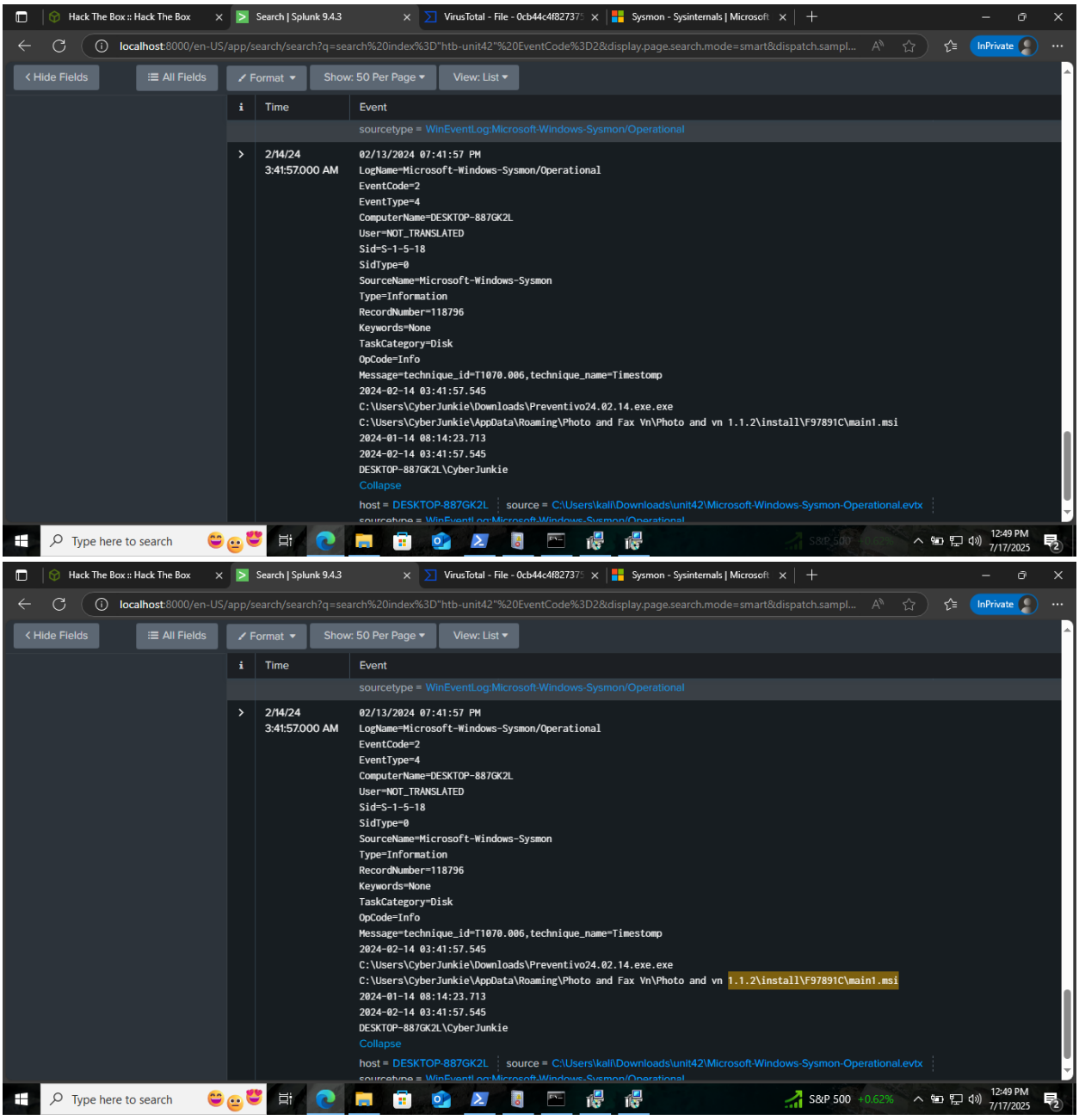


Q4. PDF File Timestomping

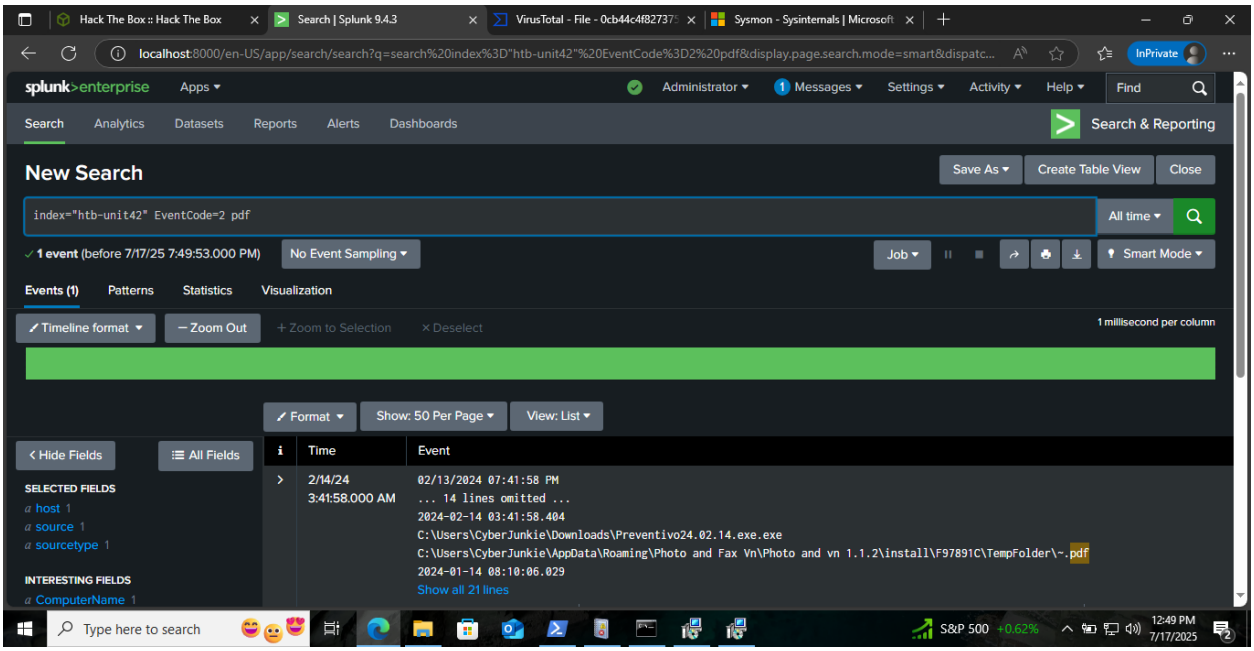
- **Event ID:** 2 (file time modification)
- **Timestamp:** `2024-01-14 08:10:06`

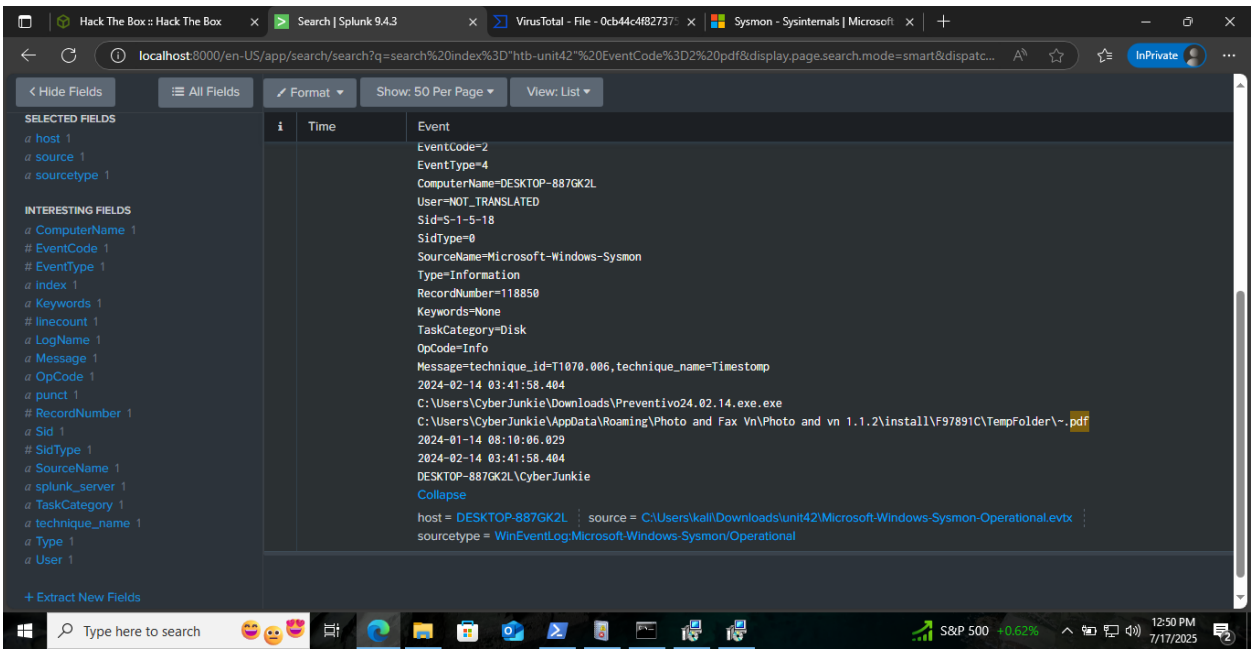

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
InPrivate
Filter by title
File and Disk Utilities
Networking Utilities
Process Utilities
Security Utilities
Security Utilities
Autologon
LogonSessions
NewSID
PsLoggedOn
PsLogList
RootkitRevealer
Sysmon
System Information
Miscellaneous
Sysinternals Suite
Microsoft Store
Download PDF
The following are examples of each event type that Sysmon generates.
Event ID 1: Process creation
The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.
Event ID 2: A process changed a file creation time
The change file creation time event is registered when a file creation time is explicitly modified by a process. This event helps tracking the real creation time of a file. Attackers may change the file creation time of a backdoor to make it look like it was installed with the operating system. Note that many processes legitimately change the creation time of a file; it does not necessarily indicate malicious activity.
Event ID 3: Network connection
In this article
Introduction
Overview of Sysmon Capabilities
Screenshots
Usage
Examples
Events
Configuration files
Configuration Entries
Event filtering entries
Type here to search
Former Dodgers pitc...
12:47 PM
7/17/2025

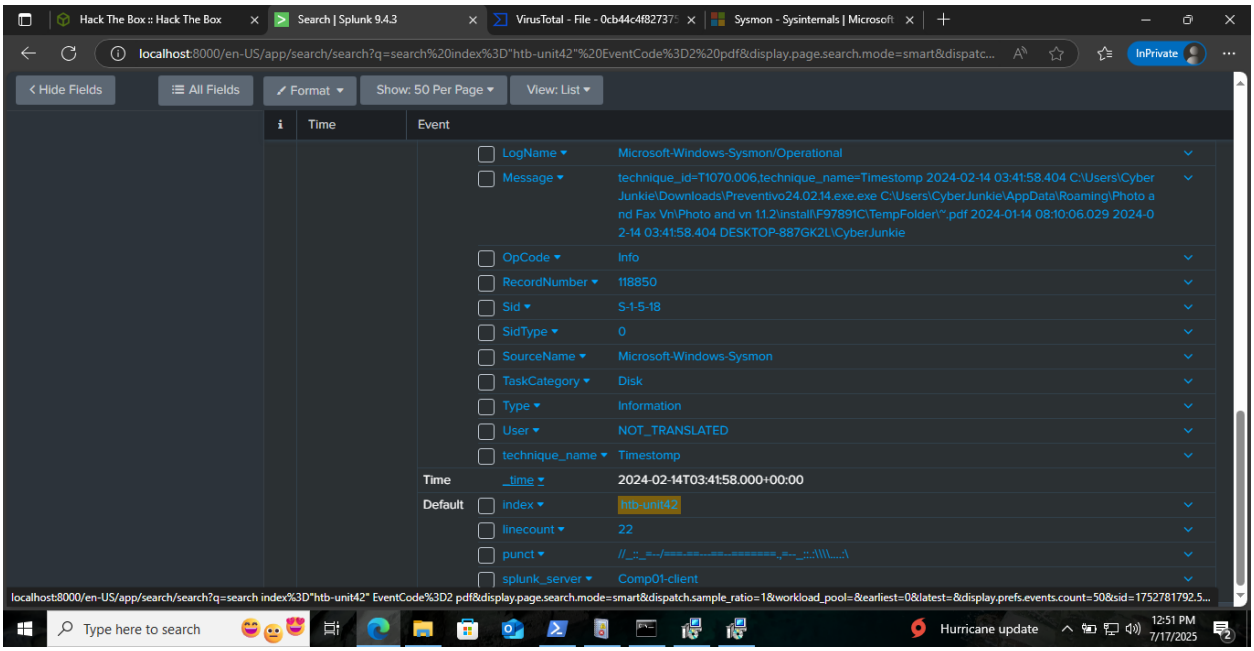

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D2&display.page.search.mode=smart&dispatch.sampl...
InPrivate
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="htb-unit42" EventCode=2
All time
16 events (before 7/17/25 7:49:12.000 PM)
No Event Sampling
Job
Smart Mode
Events (16)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
10 milliseconds per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
Time
Event
2/14/24
3:41:58.000 AM
02/13/2024 07:41:58 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=2
EventType=4
ComputerName=DESKTOP-887GK2L
Show all 21 lines
host = DESKTOP-887GK2L
source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
Type here to search
12:49 PM
7/17/2025

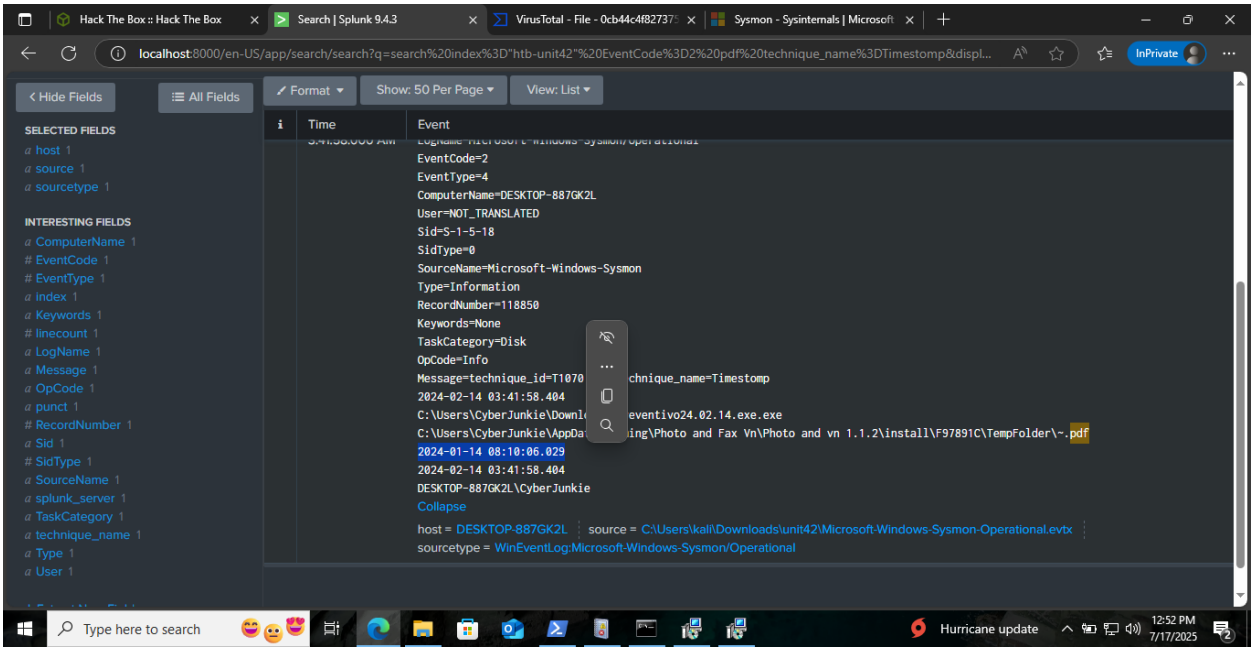

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D2&display.page.search.mode=smart&dispatch.sampl...
InPrivate
Hide Fields
All Fields
Format
Show: 50 Per Page
View: List
Time
Event
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24
3:41:57.000 AM
02/13/2024 07:41:57 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=2
EventType=4
ComputerName=DESKTOP-887GK2L
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118796
Keywords=None
TaskCategory=Disk
OpCode=Info
Message=technique_id=T1070.006,technique_name=Timestomp
2024-02-14 03:41:57.545
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\main1.msi
2024-01-14 08:14:23.713
2024-02-14 03:41:57.545
DESKTOP-887GK2L\CyberJunkie
Collapse
host = DESKTOP-887GK2L
source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
Type here to search
12:49 PM
7/17/2025

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D2&display.page.search.mode=smart&dispatch.sampl...
InPrivate
Hide Fields
All Fields
Format
Show: 50 Per Page
View: List
Time
Event
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
2/14/24
3:41:57.000 AM
02/13/2024 07:41:57 PM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=2
EventType=4
ComputerName=DESKTOP-887GK2L
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118796
Keywords=None
TaskCategory=Disk
OpCode=Info
Message=technique_id=T1070.006,technique_name=Timestomp
2024-02-14 03:41:57.545
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\main1.msi
2024-01-14 08:14:23.713
2024-02-14 03:41:57.545
DESKTOP-887GK2L\CyberJunkie
Collapse
host = DESKTOP-887GK2L
source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
Type here to search
S&P 500 +0.62%
12:49 PM
7/17/2025


Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D2%20pdf&display.page.search.mode=smart&dispatc...
InPrivate
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="htb-unit42" EventCode=2 pdf
All time
1 event (before 7/17/25 7:49:53.000 PM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
Time
Event
2/14/24
3:41:58.000 AM
02/13/2024 07:41:58 PM
... 14 lines omitted ...
2024-02-14 03:41:58.404
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\TempFolder\~.pdf
2024-01-14 08:10:06.029
Show all 21 lines
Type here to search
S&P 500 +0.62%
12:49 PM
7/17/2025

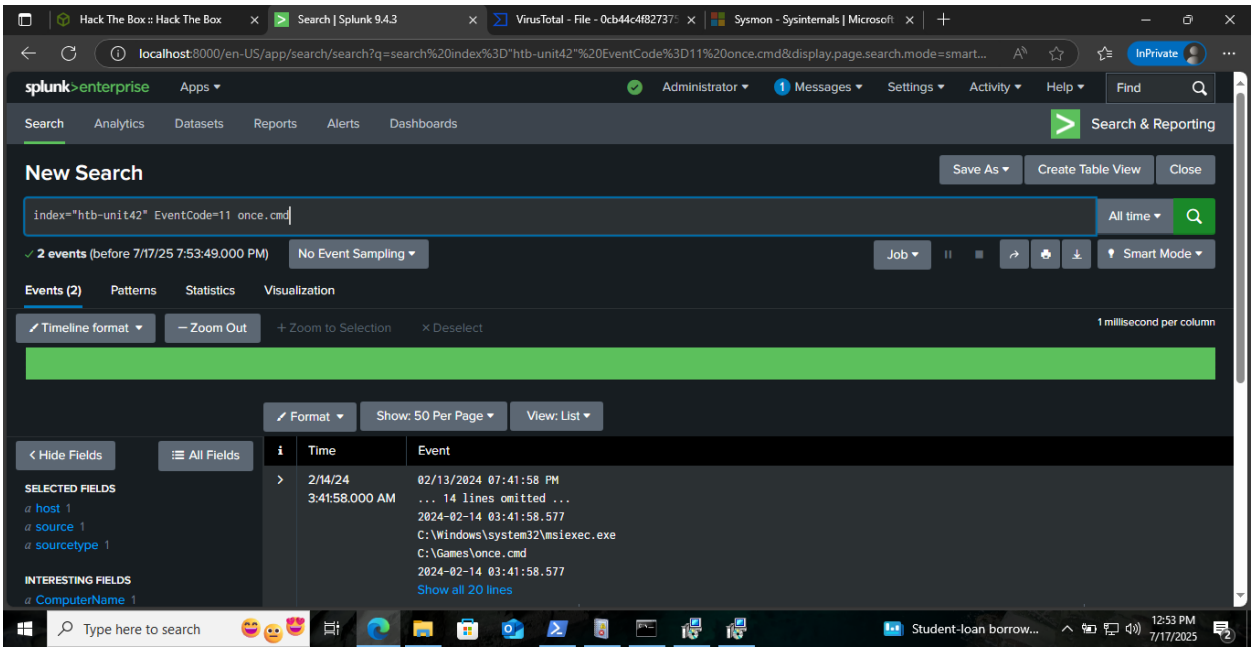

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D2%20pdf&display.page.search.mode=smart&dispatc...
InPrivate
Hide Fields
All Fields
Format
Show: 50 Per Page
View: List
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
EventCode 1
EventType 1
index 1
Keywords 1
linecount 1
LogName 1
Message 1
OpCode 1
punct 1
RecordNumber 1
Sid 1
SidType 1
SourceName 1
splunk_server 1
TaskCategory 1
technique_name 1
Type 1
User 1
Extract New Fields
Time
Event
EventCode=2
EventType=4
ComputerName=DESKTOP-887GK2L
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=118850
Keywords=None
TaskCategory=Disk
OpCode=Info
Message=technique_id=T1070.006,technique_name=Timestomp
2024-02-14 03:41:58.404
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\TempFolder\~.pdf
2024-01-14 08:10:06.029
2024-02-14 03:41:58.404
DESKTOP-887GK2L\CyberJunkie
Collapse
host = DESKTOP-887GK2L
source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
Type here to search
S&P 500 +0.62%
12:50 PM
7/17/2025

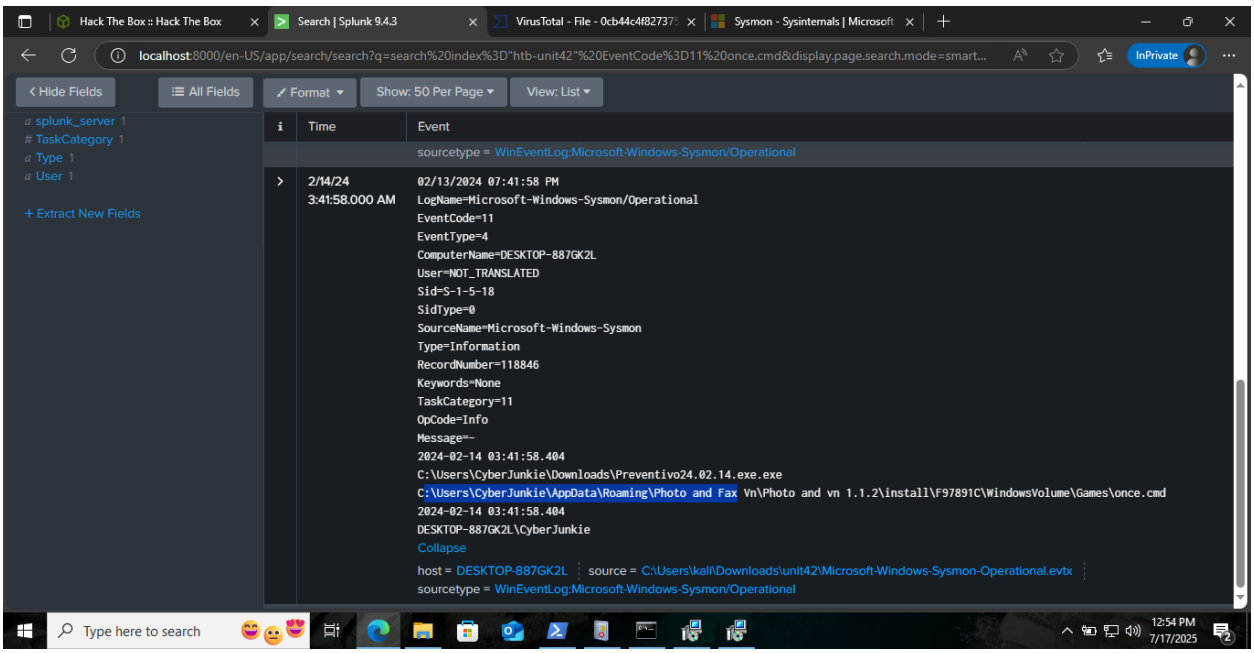




Q5. Malicious Script Path

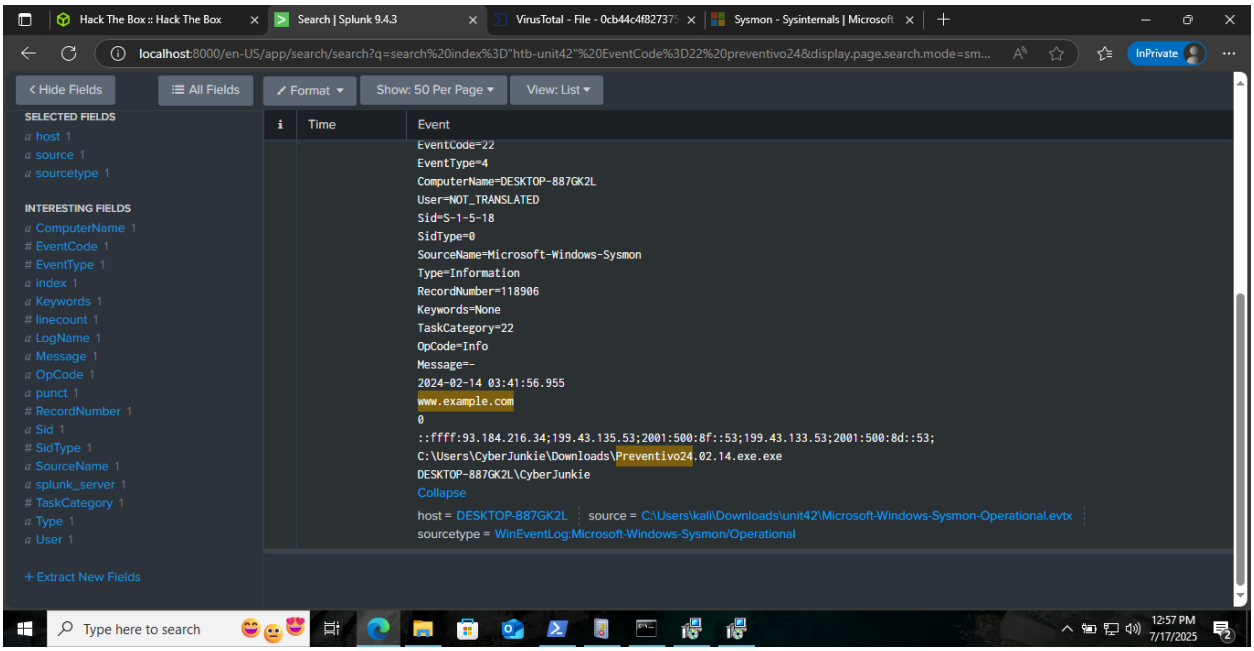
- Detected: `once.cmd` script
- **Path:** `C:\Users\cyberjunkie\AppData\Roaming\Photo & Facts\once.cmd`

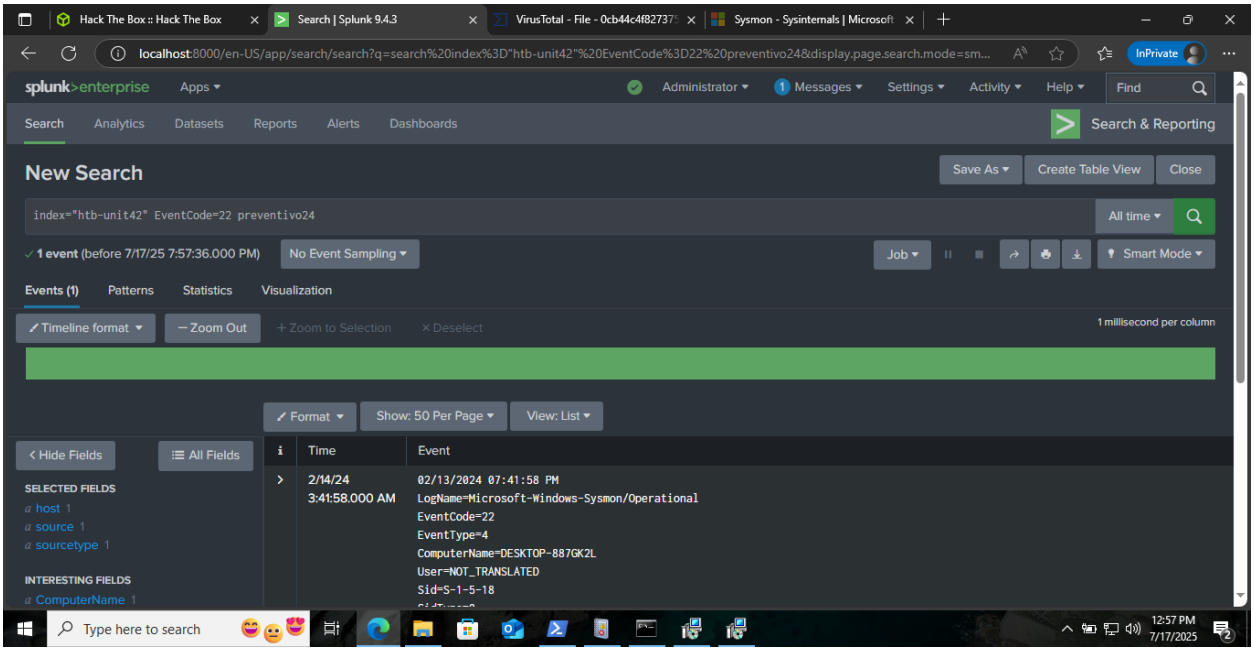




Q6. Dummy Domain Check

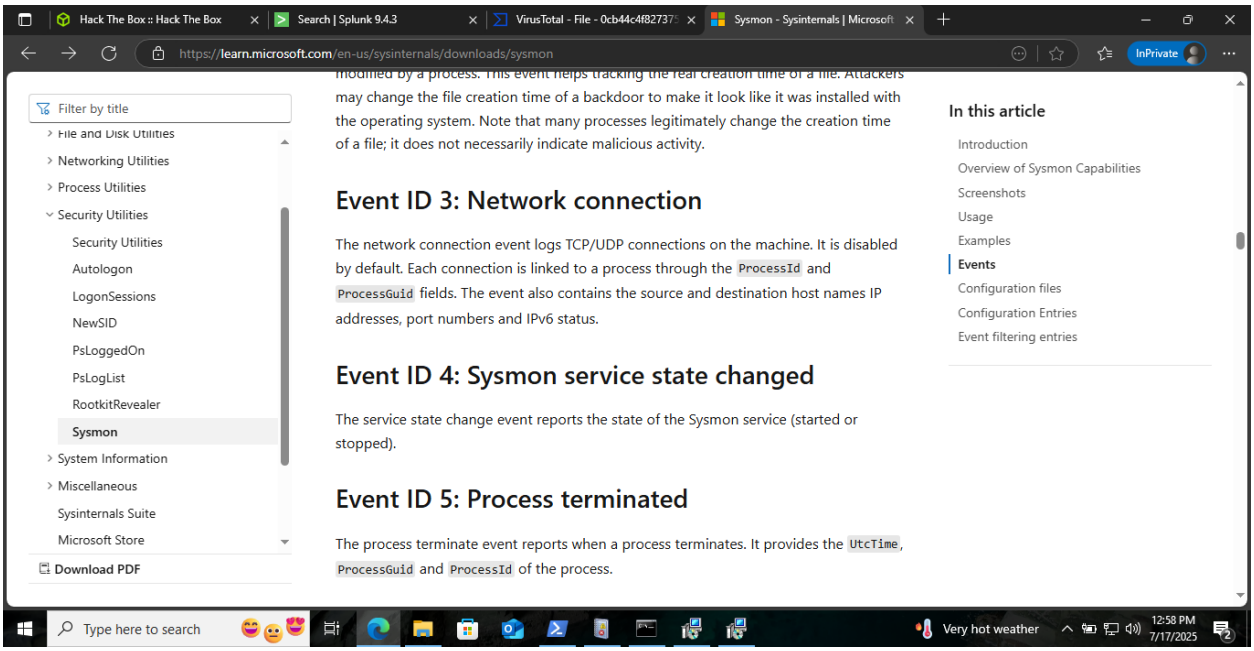
- DNS query to `www.example.com`
- Seen in Event ID 22 (likely used for C2 connectivity test)

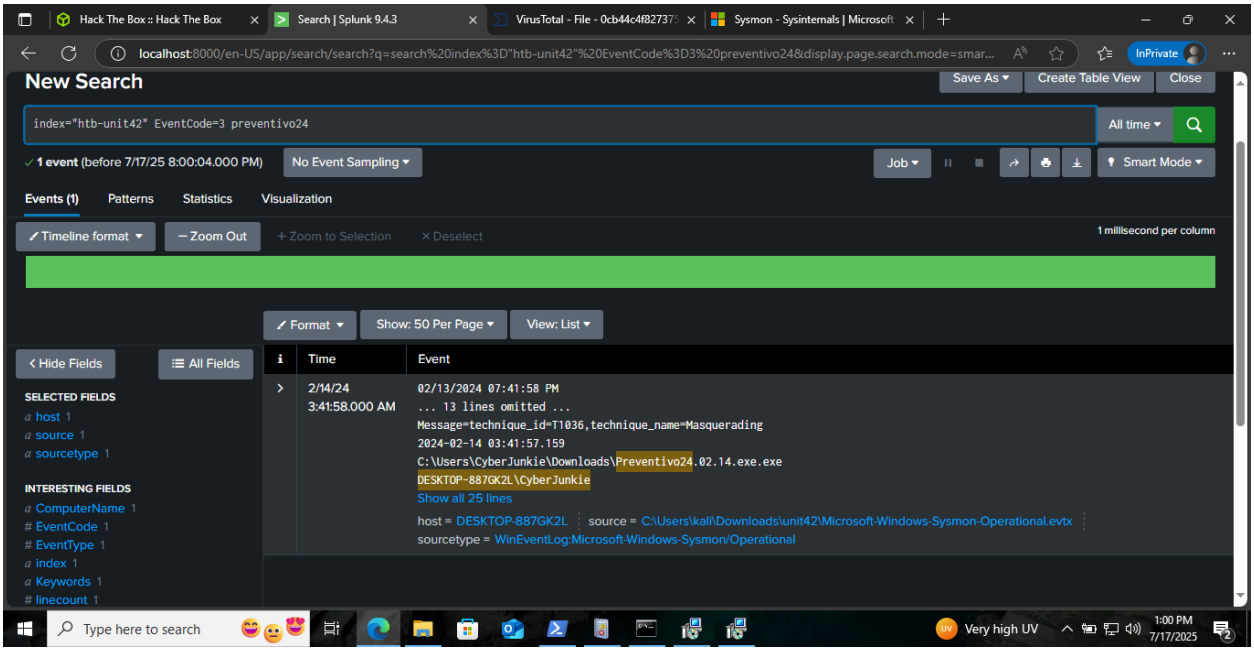


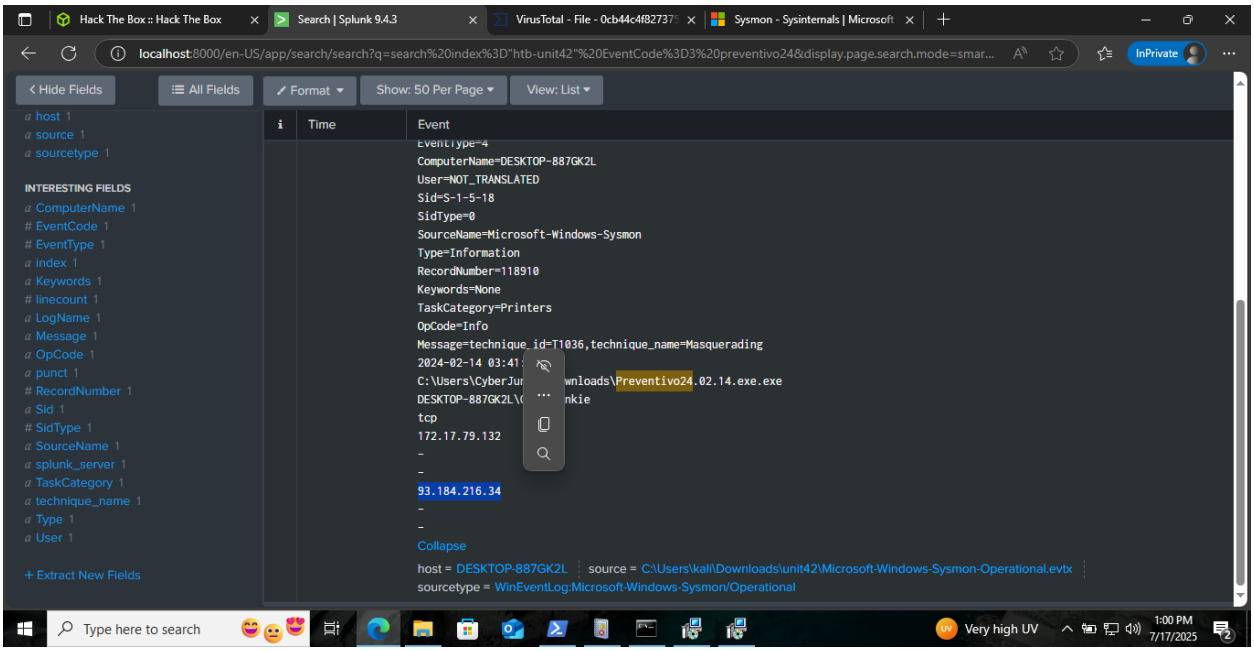


Q7. Malicious IP Contact

- Event ID 3 (network connection)
- **Destination IP:** `93.184.216.34`

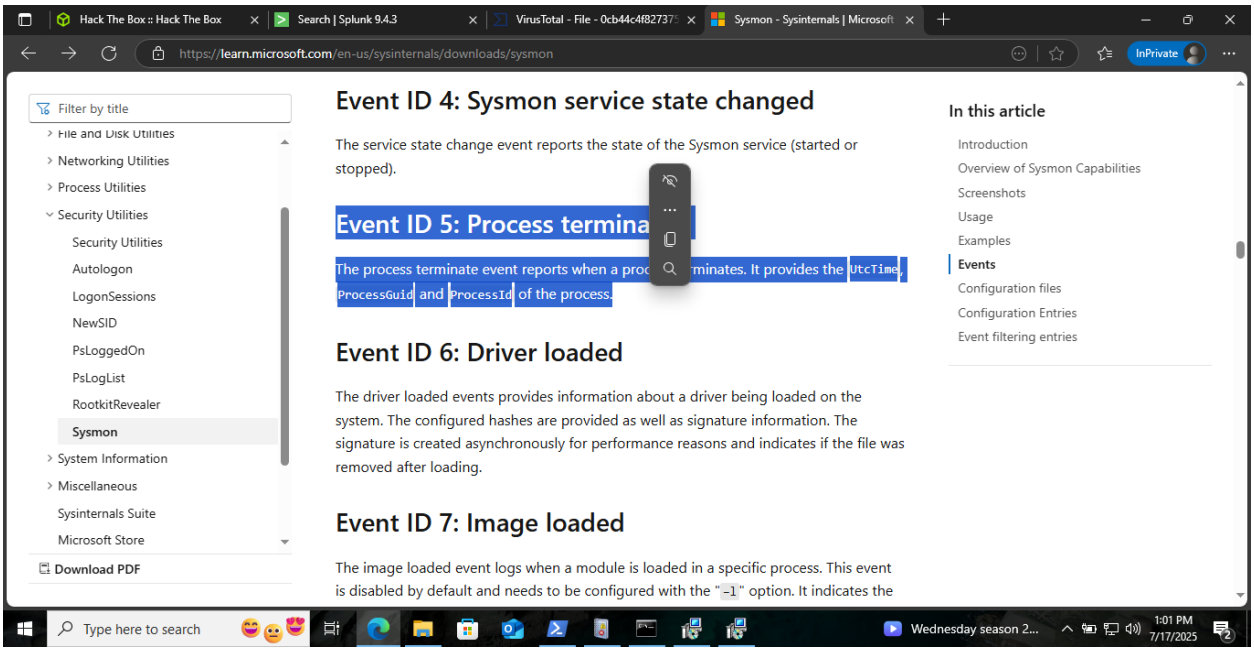

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
InPrivate
Filter by title
File and Disk Utilities
Networking Utilities
Process Utilities
Security Utilities
Security Utilities
Autologon
LogonSessions
NewSID
PsLoggedOn
PsLogList
RootkitRevealer
Sysmon
System Information
Miscellaneous
Sysinternals Suite
Microsoft Store
Download PDF
may change the file creation time of a backdoor to make it look like it was installed with the operating system. Note that many processes legitimately change the creation time of a file; it does not necessarily indicate malicious activity.
Event ID 3: Network connection
The network connection event logs TCP/UDP connections on the machine. It is disabled by default. Each connection is linked to a process through the ProcessId and ProcessGuid fields. The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.
Event ID 4: Sysmon service state changed
The service state change event reports the state of the Sysmon service (started or stopped).
Event ID 5: Process terminated
The process terminate event reports when a process terminates. It provides the UtcTime, ProcessGuid and ProcessId of the process.
In this article
Introduction
Overview of Sysmon Capabilities
Screenshots
Usage
Examples
Events
Configuration files
Configuration Entries
Event filtering entries
Type here to search
Very hot weather
12:58 PM
7/17/2025

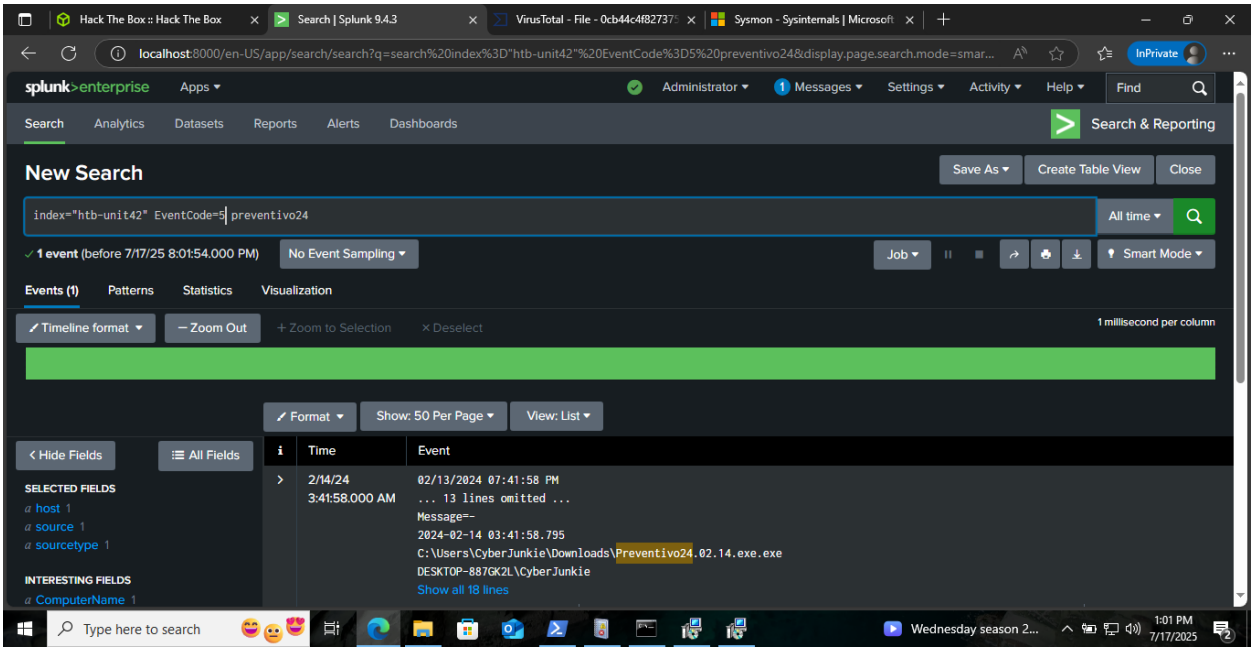

Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D3%20preventivo24&display.page.search.mode=smar...
InPrivate
New Search
Save As
Create Table View
Close
index="htb-unit42" EventCode=3 preventivo24
All time
1 event (before 7/17/25 8:00:04.000 PM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a ComputerName 1
EventCode 1
EventType 1
a index 1
a Keywords 1
linecount 1
Time
Event
2/14/24
3:41:58.000 AM
02/13/2024 07:41:58 PM
... 13 lines omitted ...
Message=technique_id=T1036,technique_name=Masquerading
2024-02-14 03:41:57.159
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
DESKTOP-887GK2L\CyberJunkie
Show all 25 lines
host = DESKTOP-887GK2L
source = C:\Users\kali\Downloads\unit42\Microsoft-Windows-Sysmon-Operational.evtx
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
Type here to search
Very high UV
1:00 PM
7/17/2025

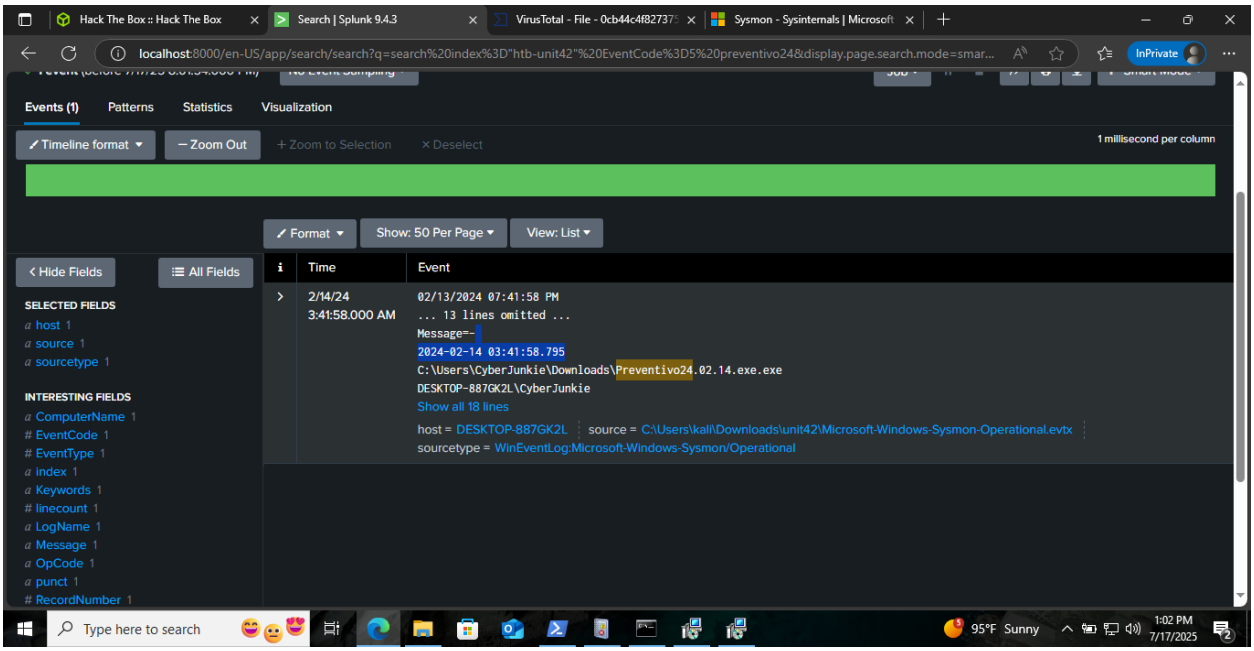


Q8. Process Termination Time

- **Event ID:** 5
- **Time:** `2024-02-14 03:41:58`


Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
InPrivate
Filter by title
File and Disk Utilities
Networking Utilities
Process Utilities
Security Utilities
Security Utilities
Autologon
LogonSessions
NewSID
PsLoggedOn
PsLogList
RootkitRevealer
Sysmon
System Information
Miscellaneous
Sysinternals Suite
Microsoft Store
Download PDF
Event ID 4: Sysmon service state changed
The service state change event reports the state of the Sysmon service (started or stopped).
Event ID 5: Process termina
The process terminate event reports when a proc minates. It provides the UtcTime, ProcessGuid and ProcessId of the process.
Event ID 6: Driver loaded
The driver loaded events provides information about a driver being loaded on the system. The configured hashes are provided as well as signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading.
Event ID 7: Image loaded
The image loaded event logs when a module is loaded in a specific process. This event is disabled by default and needs to be configured with the "-l" option. It indicates the
In this article
Introduction
Overview of Sysmon Capabilities
Screenshots
Usage
Examples
Events
Configuration files
Configuration Entries
Event filtering entries
Type here to search
Wednesday season 2...
1:01 PM
7/17/2025


Hack The Box :: Hack The Box
Search | Splunk 9.4.3
VirusTotal - File - 0cb44c4f82737
Sysmon - Sysinternals | Microsoft
localhost:8000/en-US/app/search/search?q=search%20index%3D"htb-unit42"%20EventCode%3D5%20preventivo24&display.page.search.mode=smar...
InPrivate
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="htb-unit42" EventCode=5 preventivo24
All time
1 event (before 7/17/25 8:01:54.000 PM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
ComputerName 1
Time
Event
2/14/24
3:41:58.000 AM
02/13/2024 07:41:58 PM
... 13 lines omitted ...
Message=-
2024-02-14 03:41:58.795
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
DESKTOP-887GK2L\CyberJunkie
Show all 18 lines
Type here to search
Wednesday season 2...
1:01 PM
7/17/2025



💡 Key Techniques & Concepts Practiced

Tool	Purpose
Sysmon	Deep endpoint visibility via EID 1, 2, 3, 5, 11, 15, 22
Splunk	Time-aligned correlation using SPL queries
VirusTotal	IOC triage, domain/IP/EXE reputation checking

✅ Key Lessons & Recommendations

- **Always validate log ingestion.** Misparsed logs can cause false negatives, wasting analyst time and delaying detection.
- **Use multiple Event IDs together.** Pivoting from process creation → file write → DNS → network activity builds strong timeline context.
- **Practice "threat hypothesis" mindset.** Every query should ask a question: *What could this file be doing? Who ran it? Where did it come from?*
- **Repeat labs regularly.** Just like Stephen says, repetition hardens investigative instincts.

📢 Summary

This lab sharpened my skills in real-world log triage using Sysmon and Splunk. It emphasized the importance of **data integrity, log enrichment, and contextual analysis** — all key skills for SOC Tier 1/2 analysts.