
TREND MICRO™
Detect and respond to threats with ease and confidence
NO TIME TO EXPLAIN!
Jesper Mikkelsen

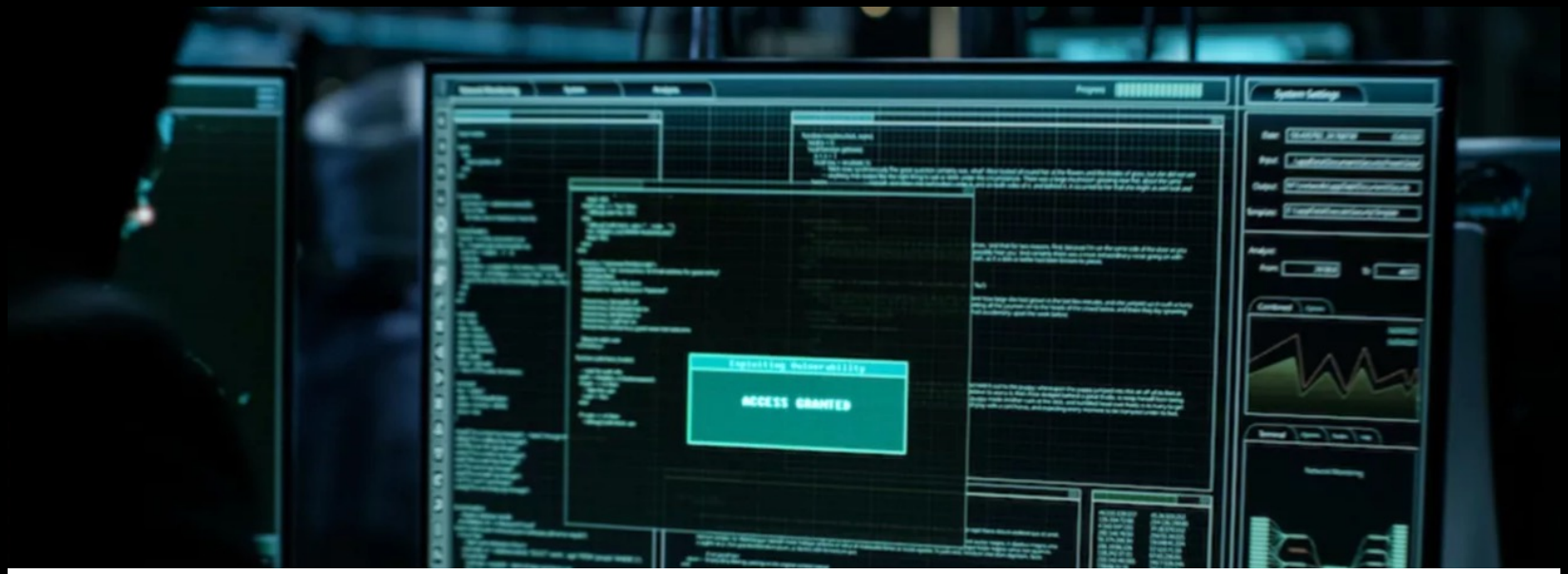
```
root@admin : % cat presenter.json |jq
> name           : "Jesper Mikkelsen"
> title          : "Technical Director Nordics"
> expirance      : "20 years +"
> time_at_trend  : "10 years +"

root@admin : %
```


The challenges in IT – Security. Today and tomorrow..


TICK TOCK...

TREND MICRO™



Exploits & Vulnerabilities

Threat Actor Groups, Including Black Basta, are Exploiting Recent ScreenConnect Vulnerabilities

This blog entry gives a detailed analysis of these recent ScreenConnect vulnerabilities. We also discuss our discovery of threat actor groups, including Black Basta and Bl00dy Ransomware gangs, that are actively exploiting CVE-2024-1708 and CVE-2024-1709 based on our telemetry.

Feb 27, 2024

Exploits & Vulnerabilities

CVE-2024-21412: DarkGate Operators Exploit Microsoft Windows SmartScreen Bypass in Zero-Day Campaign

In addition to our Water Hydra APT zero day analysis, the Zero Day Initiative (ZDI) observed a DarkGate campaign which we discovered in mid-January 2024 where DarkGate operators exploited CVE-2024-21412.

Microsoft Confirms Russian Hackers Stole Source Code, Some Customer Secrets

Mar 09, 2024 Newsroom Cyber Attack / Threat Intelligence

Microsoft on Friday revealed that the Kremlin-backed threat actor known as **Midnight Blizzard** (aka APT29 or Cozy Bear) managed to gain access to some of its source code repositories and internal systems following a hack that came to light in January 2024.

Micro

Secre

omer

Palo Alto Networks zero-day exploited since March to backdoor firewalls

By **Lawrence Abrams**

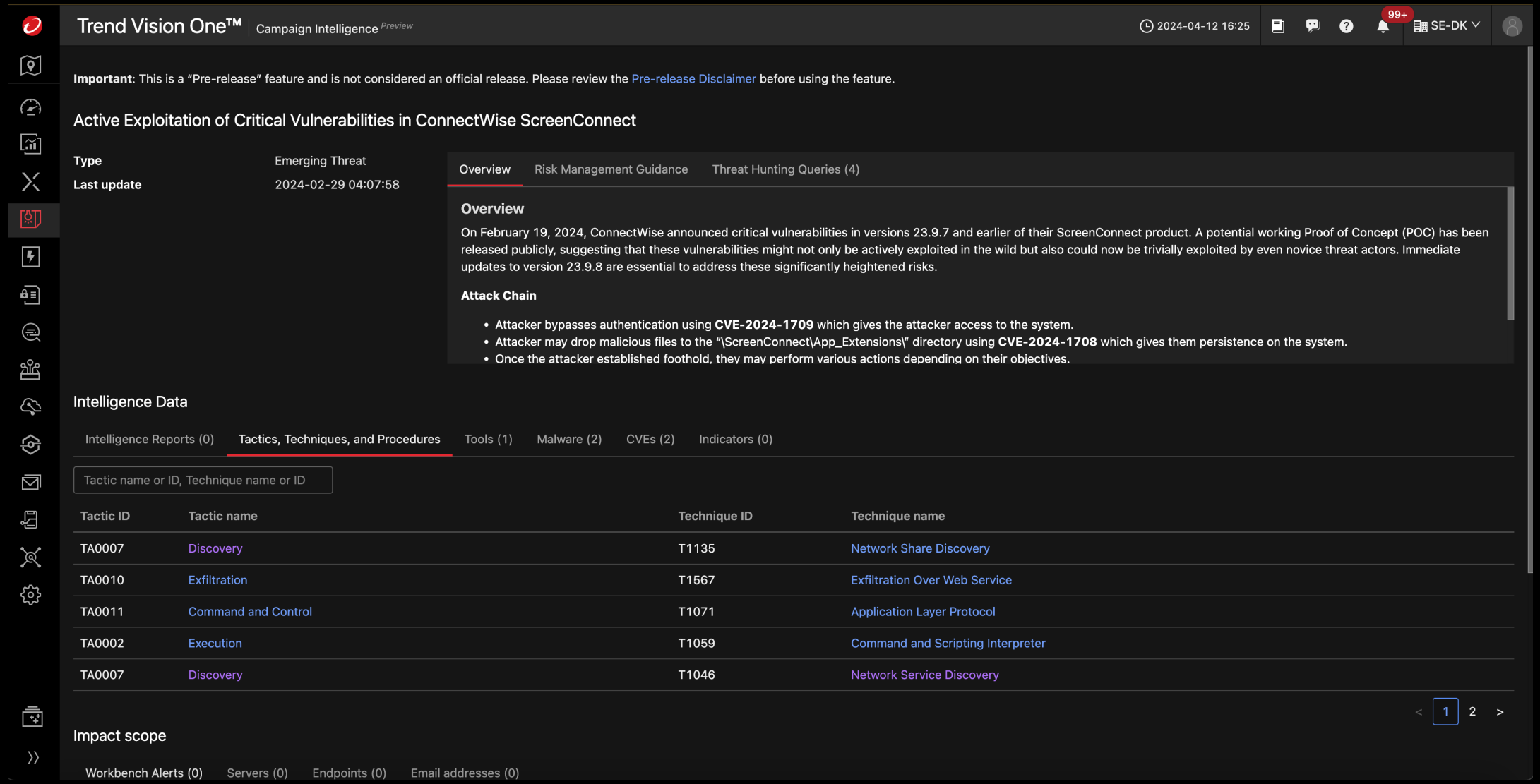
April 13, 2024 08:35 AM 0

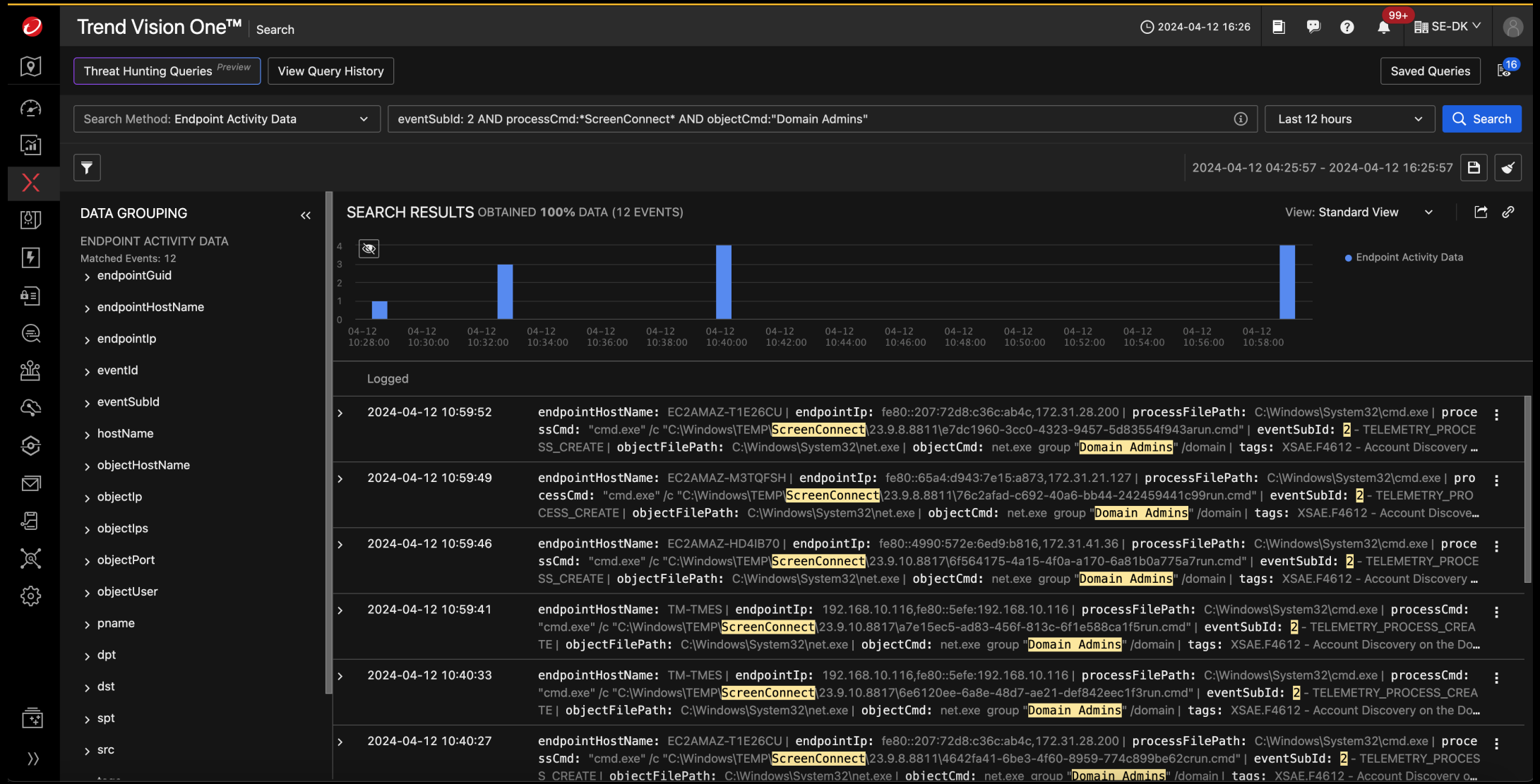
Suspected state-sponsored hackers have been exploiting a zero-day vulnerability in Palo Alto Networks firewalls tracked as CVE-2024-3400 since March 26, using the compromised devices to breach internal networks, steal data and credentials.

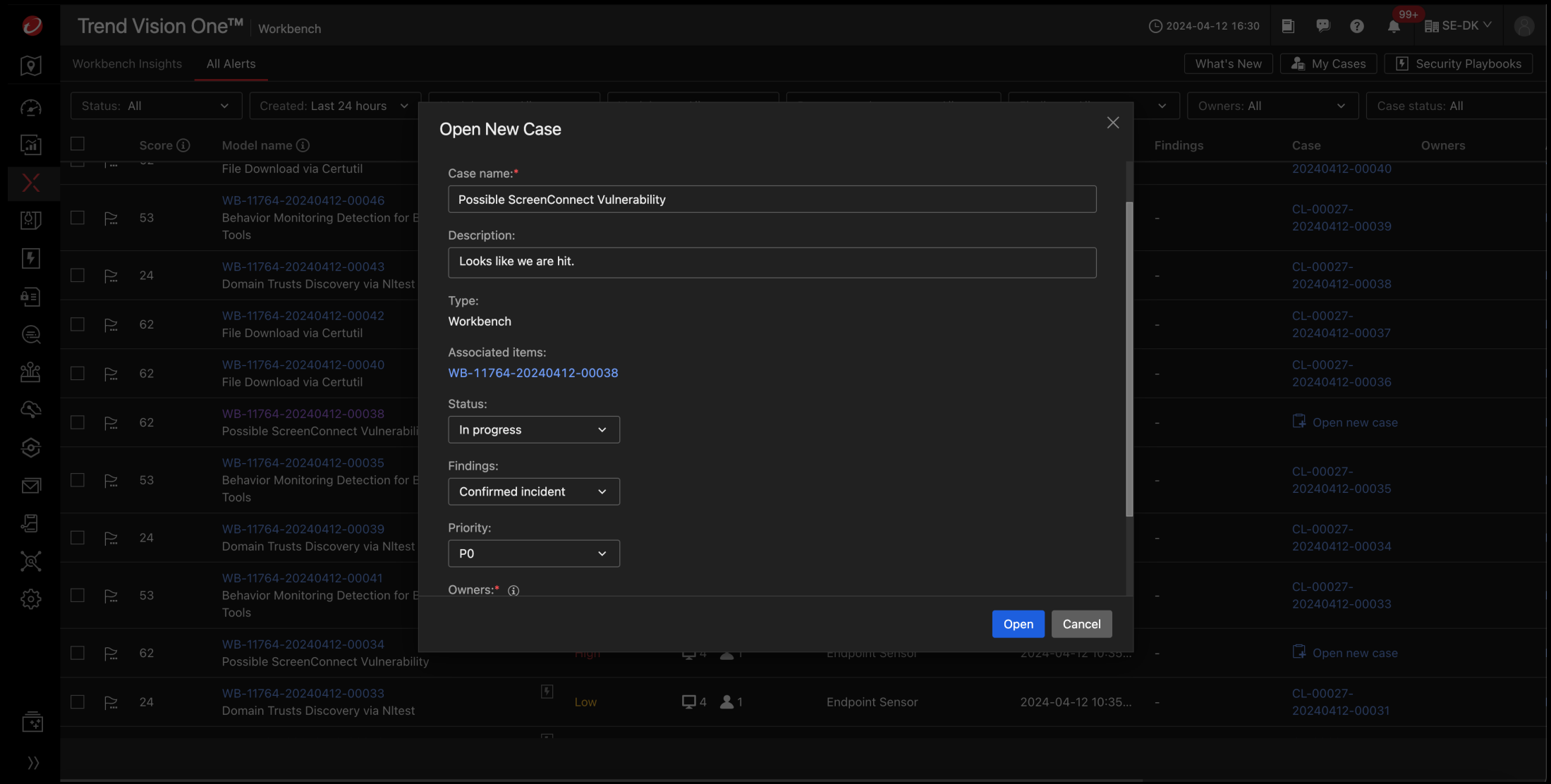
TREND MICRO

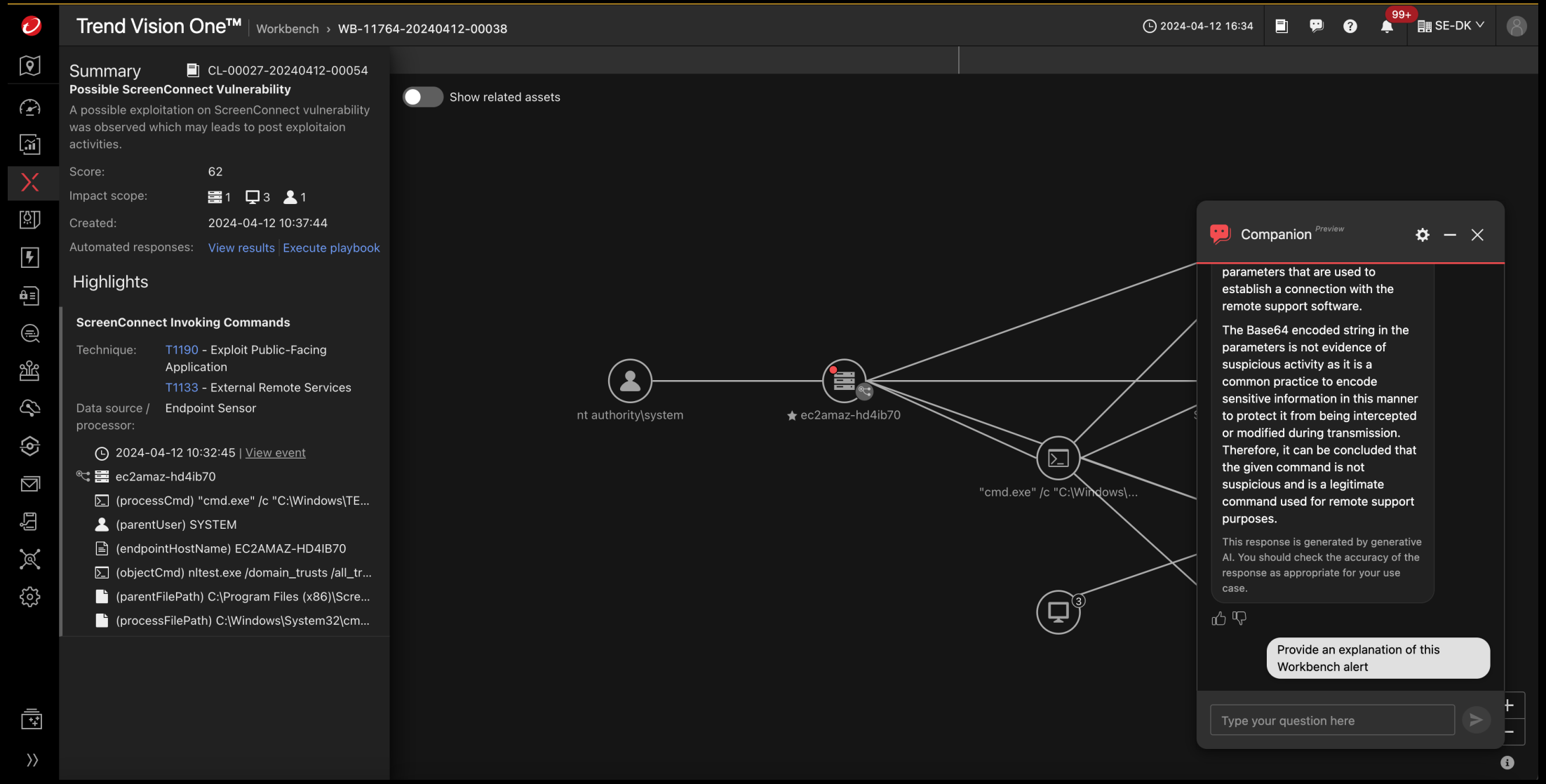
A real world example.
When things go bad… fast.

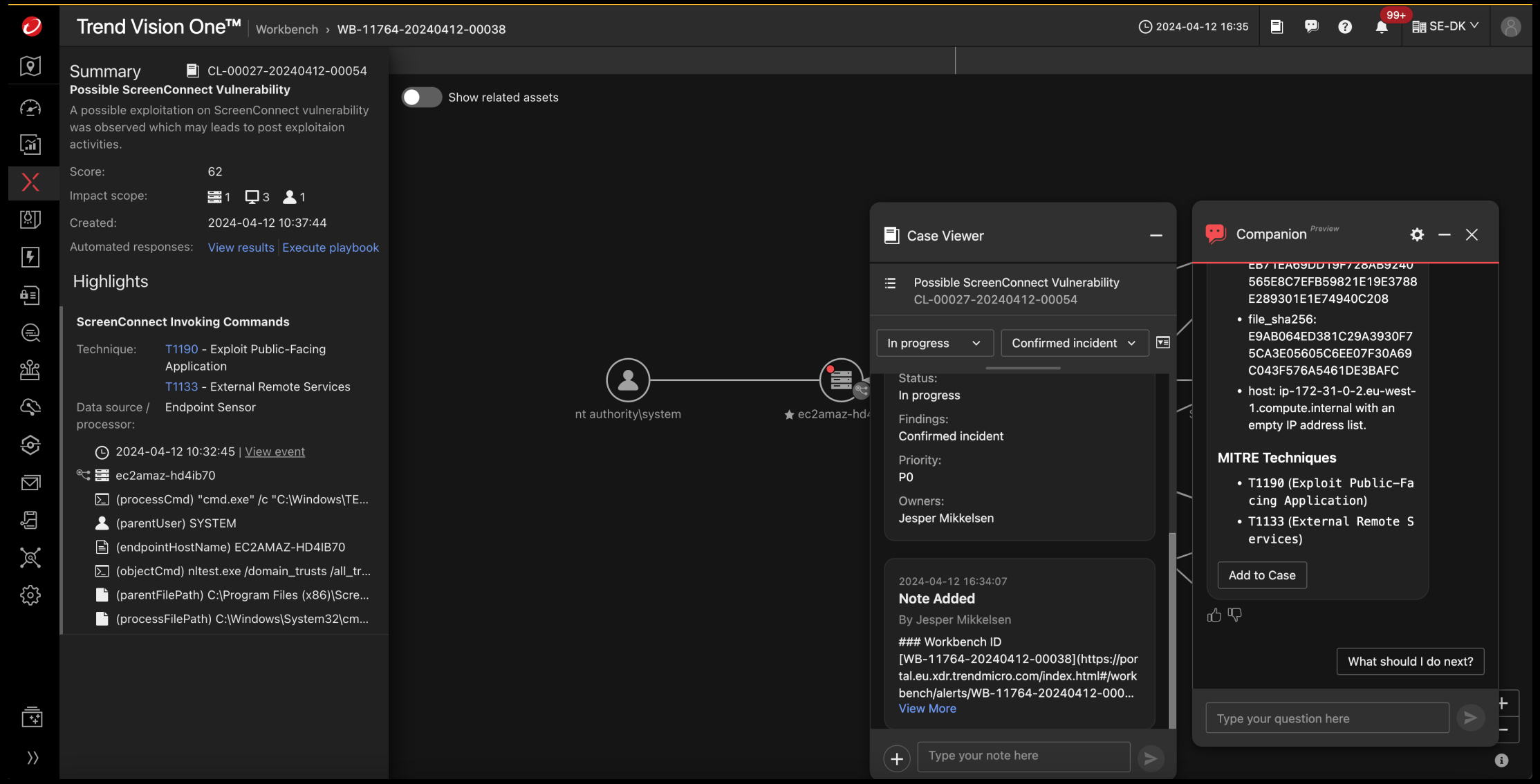
BASED ON A TRUE STORY

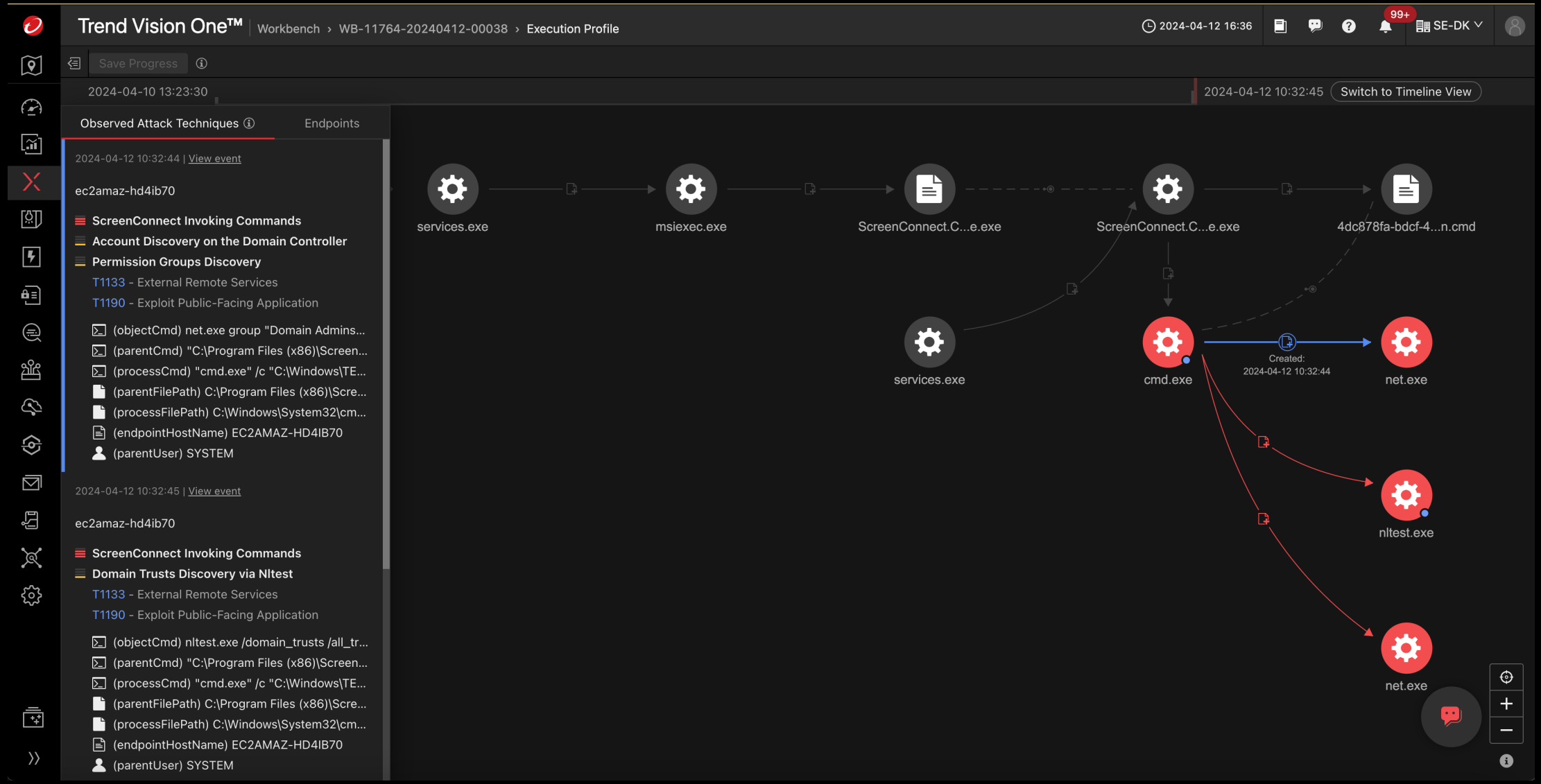

Trend Vision One™ | Campaign Intelligence Preview
2024-04-12 16:25
99+
SE-DK
Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.
Active Exploitation of Critical Vulnerabilities in ConnectWise ScreenConnect
Type
Emerging Threat
Last update
2024-02-29 04:07:58
Overview
Risk Management Guidance
Threat Hunting Queries (4)
Overview
On February 19, 2024, ConnectWise announced critical vulnerabilities in versions 23.9.7 and earlier of their ScreenConnect product. A potential working Proof of Concept (POC) has been released publicly, suggesting that these vulnerabilities might not only be actively exploited in the wild but also could now be trivially exploited by even novice threat actors. Immediate updates to version 23.9.8 are essential to address these significantly heightened risks.
Attack Chain
Attacker bypasses authentication using CVE-2024-1709 which gives the attacker access to the system.
Attacker may drop malicious files to the "\ScreenConnect\App_Extensions\" directory using CVE-2024-1708 which gives them persistence on the system.
Once the attacker established foothold, they may perform various actions depending on their objectives.
Intelligence Data
Intelligence Reports (0)
Tactics, Techniques, and Procedures
Tools (1)
Malware (2)
CVEs (2)
Indicators (0)
Tactic name or ID, Technique name or ID
Tactic ID
Tactic name
Technique ID
Technique name
TA0007
Discovery
T1135
Network Share Discovery
TA0010
Exfiltration
T1567
Exfiltration Over Web Service
TA0011
Command and Control
T1071
Application Layer Protocol
TA0002
Execution
T1059
Command and Scripting Interpreter
TA0007
Discovery
T1046
Network Service Discovery
< 1 2 >
Impact scope
Workbench Alerts (0)
Servers (0)
Endpoints (0)
Email addresses (0)

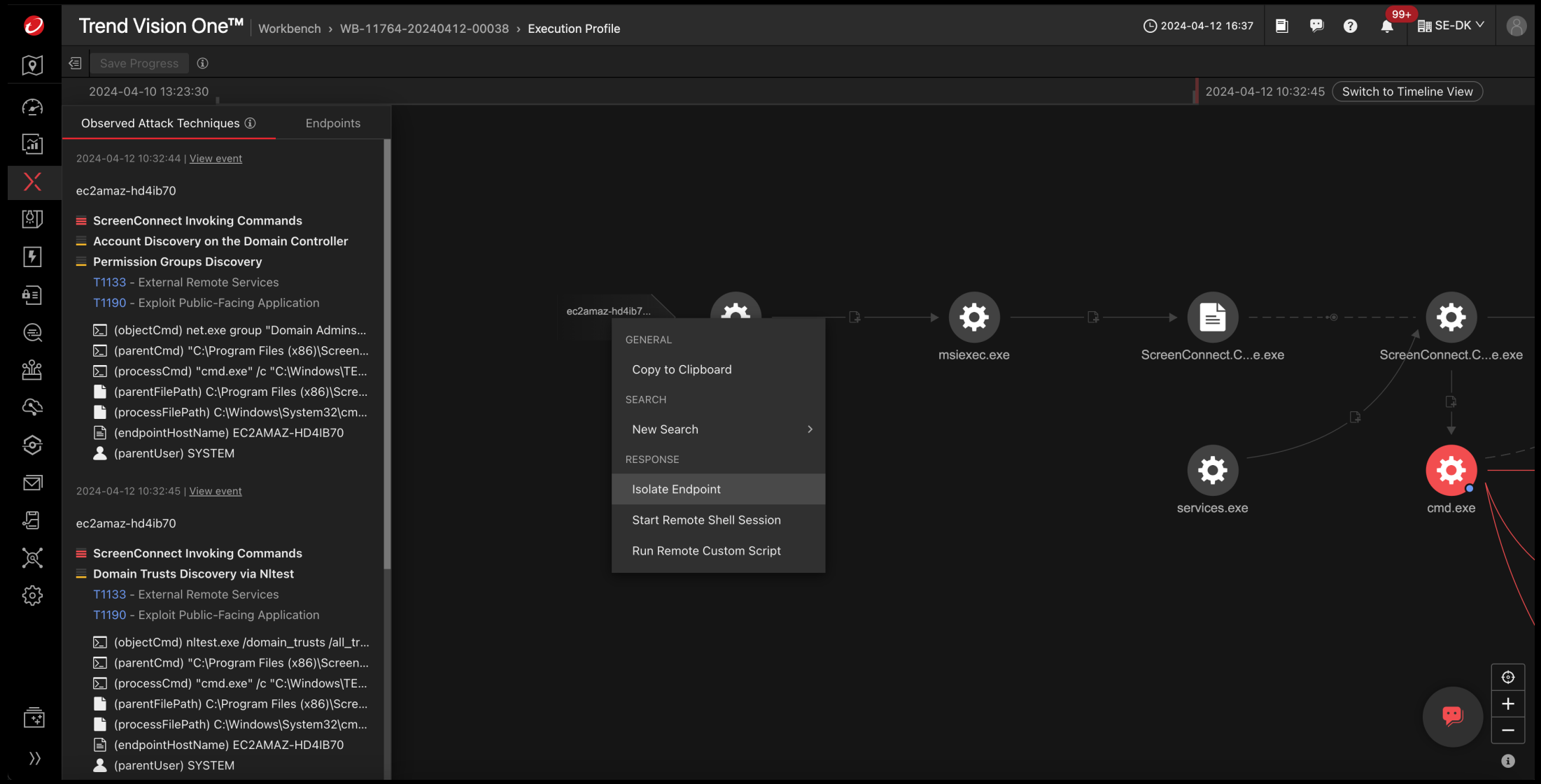

Trend Vision One™ | Search
2024-04-12 16:26
99+
SE-DK
Threat Hunting Queries Preview
View Query History
Saved Queries
16
Search Method: Endpoint Activity Data
eventSubId: 2 AND processCmd:*ScreenConnect* AND objectCmd:"Domain Admins"
Last 12 hours
Search
2024-04-12 04:25:57 - 2024-04-12 16:25:57
DATA GROUPING
ENDPOINT ACTIVITY DATA
Matched Events: 12
endpointGuid
endpointHostName
endpointIp
eventId
eventSubId
hostName
objectHostName
objectIp
objectIps
objectPort
objectUser
pname
dpt
dst
spt
src
SEARCH RESULTS OBTAINED 100% DATA (12 EVENTS)
View: Standard View
Endpoint Activity Data
Logged
2024-04-12 10:59:52 endpointHostName: EC2AMAZ-T1E26CU | endpointIp: fe80::207:72d8:c36c:ab4c,172.31.28.200 | processFilePath: C:\Windows\System32\cmd.exe | processCmd: "cmd.exe" /c "C:\Windows\TEMP\ScreenConnect\23.9.8.8811\e7dc1960-3cc0-4323-9457-5d83554f943arun.cmd" | eventSubId: 2 - TELEMETRY_PROCESS_CREATE | objectFilePath: C:\Windows\System32\net.exe | objectCmd: net.exe group "Domain Admins" /domain | tags: XSAE.F4612 - Account Discovery …
2024-04-12 10:59:49 endpointHostName: EC2AMAZ-M3TQFSH | endpointIp: fe80::65a4:d943:7e15:a873,172.31.21.127 | processFilePath: C:\Windows\System32\cmd.exe | processCmd: "cmd.exe" /c "C:\Windows\TEMP\ScreenConnect\23.9.8.8811\76c2afad-c692-40a6-bb44-242459441c99run.cmd" | eventSubId: 2 - TELEMETRY_PROCESS_CREATE | objectFilePath: C:\Windows\System32\net.exe | objectCmd: net.exe group "Domain Admins" /domain | tags: XSAE.F4612 - Account Discove…
2024-04-12 10:59:46 endpointHostName: EC2AMAZ-HD4IB70 | endpointIp: fe80::4990:572e:6ed9:b816,172.31.41.36 | processFilePath: C:\Windows\System32\cmd.exe | processCmd: "cmd.exe" /c "C:\Windows\TEMP\ScreenConnect\23.9.10.8817\6f564175-4a15-4f0a-a170-6a81b0a775a7run.cmd" | eventSubId: 2 - TELEMETRY_PROCESS_CREATE | objectFilePath: C:\Windows\System32\net.exe | objectCmd: net.exe group "Domain Admins" /domain | tags: XSAE.F4612 - Account Discovery …
2024-04-12 10:59:41 endpointHostName: TM-TMES | endpointIp: 192.168.10.116,fe80::5efe:192.168.10.116 | processFilePath: C:\Windows\System32\cmd.exe | processCmd: "cmd.exe" /c "C:\Windows\TEMP\ScreenConnect\23.9.10.8817\a7e15ec5-ad83-456f-813c-6f1e588ca1f5run.cmd" | eventSubId: 2 - TELEMETRY_PROCESS_CREATE | objectFilePath: C:\Windows\System32\net.exe | objectCmd: net.exe group "Domain Admins" /domain | tags: XSAE.F4612 - Account Discovery on the Do…
2024-04-12 10:40:33 endpointHostName: TM-TMES | endpointIp: 192.168.10.116,fe80::5efe:192.168.10.116 | processFilePath: C:\Windows\System32\cmd.exe | processCmd: "cmd.exe" /c "C:\Windows\TEMP\ScreenConnect\23.9.10.8817\6e6120ee-6a8e-48d7-ae21-def842eec1f3run.cmd" | eventSubId: 2 - TELEMETRY_PROCESS_CREATE | objectFilePath: C:\Windows\System32\net.exe | objectCmd: net.exe group "Domain Admins" /domain | tags: XSAE.F4612 - Account Discovery on the Do…
2024-04-12 10:40:27 endpointHostName: EC2AMAZ-T1E26CU | endpointIp: fe80::207:72d8:c36c:ab4c,172.31.28.200 | processFilePath: C:\Windows\System32\cmd.exe | processCmd: "cmd.exe" /c "C:\Windows\TEMP\ScreenConnect\23.9.8.8811\4642fa41-6be3-4f60-8959-774c899be62crun.cmd" | eventSubId: 2 - TELEMETRY_PROCESS_CREATE | objectFilePath: C:\Windows\System32\net.exe | objectCmd: net.exe group "Domain Admins" /domain | tags: XSAE.F4612 - Account Discovery o…


Trend Vision One™ | Workbench
2024-04-12 16:30
99+
SE-DK
Workbench Insights
All Alerts
What's New
My Cases
Security Playbooks
Status: All
Created: Last 24 hours
Owners: All
Case status: All
Score
Model name
Findings
Case
Owners
Open New Case
Case name:*
Possible ScreenConnect Vulnerability
Description:
Looks like we are hit.
Type:
Workbench
Associated items:
WB-11764-20240412-00038
Status:
In progress
Findings:
Confirmed incident
Priority:
P0
Owners:*
Open
Cancel
Open new case

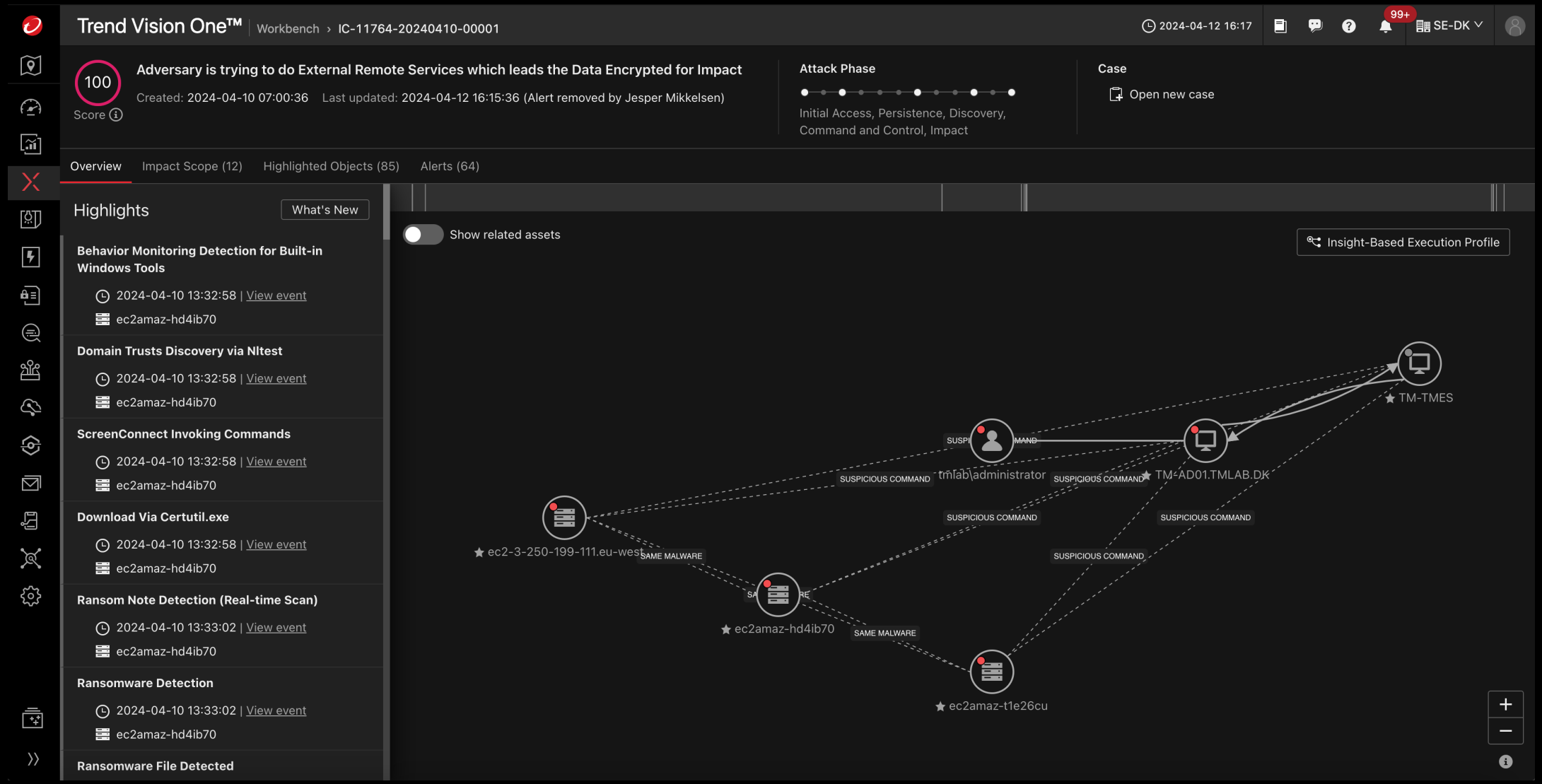

Trend Vision One™
Workbench › WB-11764-20240412-00038
2024-04-12 16:34
99+
SE-DK
Summary
CL-00027-20240412-00054
Possible ScreenConnect Vulnerability
A possible exploitation on ScreenConnect vulnerability was observed which may leads to post exploitaion activities.
Score: 62
Impact scope: 1 3 1
Created: 2024-04-12 10:37:44
Automated responses: View results | Execute playbook
Highlights
ScreenConnect Invoking Commands
Technique: T1190 - Exploit Public-Facing Application
T1133 - External Remote Services
Data source / processor: Endpoint Sensor
2024-04-12 10:32:45 | View event
ec2amaz-hd4ib70
(processCmd) "cmd.exe" /c "C:\Windows\TE...
(parentUser) SYSTEM
(endpointHostName) EC2AMAZ-HD4IB70
(objectCmd) nltest.exe /domain_trusts /all_tr...
(parentFilePath) C:\Program Files (x86)\Scre...
(processFilePath) C:\Windows\System32\cm...
Show related assets
nt authority\system
ec2amaz-hd4ib70
"cmd.exe" /c "C:\Windows\...
Companion Preview
parameters that are used to establish a connection with the remote support software.
The Base64 encoded string in the parameters is not evidence of suspicious activity as it is a common practice to encode sensitive information in this manner to protect it from being intercepted or modified during transmission. Therefore, it can be concluded that the given command is not suspicious and is a legitimate command used for remote support purposes.
This response is generated by generative AI. You should check the accuracy of the response as appropriate for your use case.
Provide an explanation of this Workbench alert
Type your question here

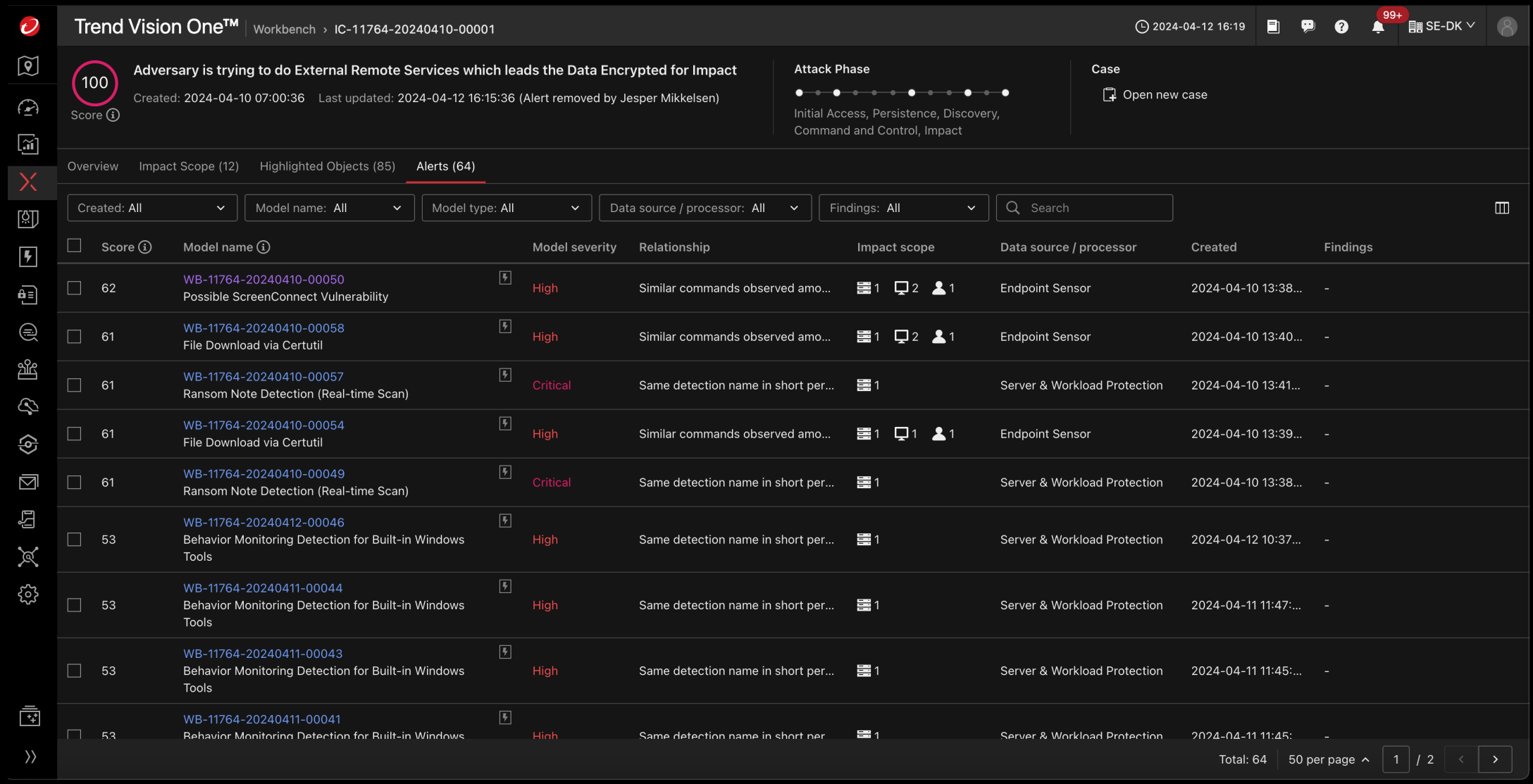

Trend Vision One™ | Workbench › WB-11764-20240412-00038
2024-04-12 16:35
99+
SE-DK
Summary
CL-00027-20240412-00054
Possible ScreenConnect Vulnerability
A possible exploitation on ScreenConnect vulnerability was observed which may leads to post exploitaion activities.
Score: 62
Impact scope: 1 3 1
Created: 2024-04-12 10:37:44
Automated responses: View results | Execute playbook
Highlights
ScreenConnect Invoking Commands
Technique: T1190 - Exploit Public-Facing Application
T1133 - External Remote Services
Data source / processor: Endpoint Sensor
2024-04-12 10:32:45 | View event
ec2amaz-hd4ib70
(processCmd) "cmd.exe" /c "C:\Windows\TE...
(parentUser) SYSTEM
(endpointHostName) EC2AMAZ-HD4IB70
(objectCmd) nltest.exe /domain_trusts /all_tr...
(parentFilePath) C:\Program Files (x86)\Scre...
(processFilePath) C:\Windows\System32\cm...
Show related assets
nt authority\system
Case Viewer
Possible ScreenConnect Vulnerability
CL-00027-20240412-00054
In progress
Confirmed incident
Status:
In progress
Findings:
Confirmed incident
Priority:
P0
Owners:
Jesper Mikkelsen
2024-04-12 16:34:07
Note Added
By Jesper Mikkelsen
Workbench ID
[WB-11764-20240412-00038](https://portal.eu.xdr.trendmicro.com/index.html#/workbench/alerts/WB-11764-20240412-000...
View More
Type your note here
Companion Preview
565E8C7EFB59821E19E3788
E289301E1E74940C208
file_sha256:
E9AB064ED381C29A3930F7
5CA3E05605C6EE07F30A69
C043F576A5461DE3BAFC
host: ip-172-31-0-2.eu-west-1.compute.internal with an empty IP address list.
MITRE Techniques
T1190 (Exploit Public-Facing Application)
T1133 (External Remote Services)
Add to Case
What should I do next?
Type your question here

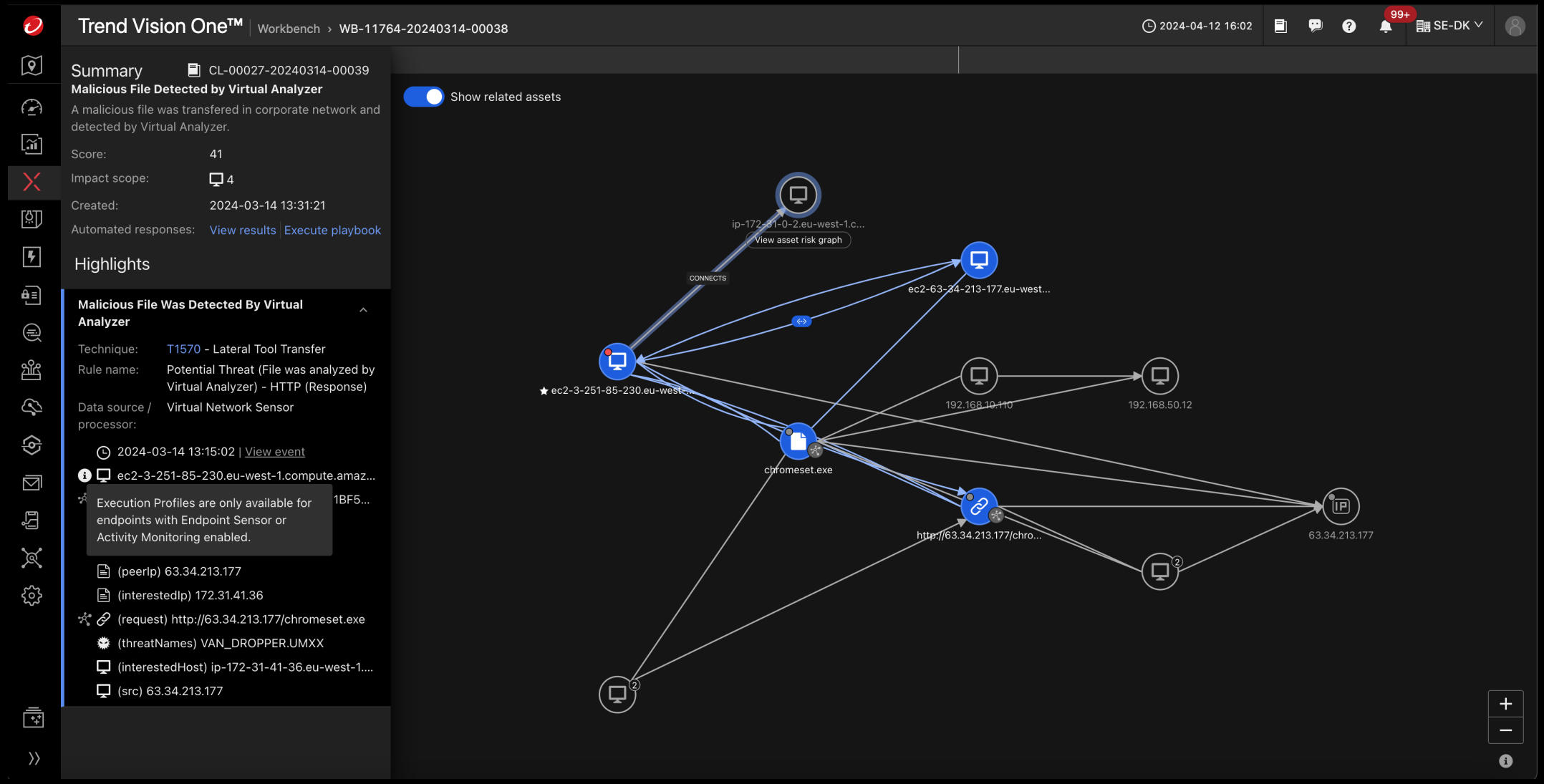

Trend Vision One™
Workbench › WB-11764-20240412-00038 › Execution Profile
2024-04-12 16:36
99+
SE-DK
Save Progress
2024-04-10 13:23:30
2024-04-12 10:32:45
Switch to Timeline View
Observed Attack Techniques
Endpoints
2024-04-12 10:32:44 | View event
ec2amaz-hd4ib70
ScreenConnect Invoking Commands
Account Discovery on the Domain Controller
Permission Groups Discovery
T1133 - External Remote Services
T1190 - Exploit Public-Facing Application
(objectCmd) net.exe group "Domain Admins...
(parentCmd) "C:\Program Files (x86)\Screen...
(processCmd) "cmd.exe" /c "C:\Windows\TE...
(parentFilePath) C:\Program Files (x86)\Scre...
(processFilePath) C:\Windows\System32\cm...
(endpointHostName) EC2AMAZ-HD4IB70
(parentUser) SYSTEM
2024-04-12 10:32:45 | View event
ec2amaz-hd4ib70
ScreenConnect Invoking Commands
Domain Trusts Discovery via Nltest
T1133 - External Remote Services
T1190 - Exploit Public-Facing Application
(objectCmd) nltest.exe /domain_trusts /all_tr...
(parentCmd) "C:\Program Files (x86)\Screen...
(processCmd) "cmd.exe" /c "C:\Windows\TE...
(parentFilePath) C:\Program Files (x86)\Scre...
(processFilePath) C:\Windows\System32\cm...
(endpointHostName) EC2AMAZ-HD4IB70
(parentUser) SYSTEM
services.exe
msiexec.exe
ScreenConnect.C...e.exe
ScreenConnect.C...e.exe
4dc878fa-bdcf-4...n.cmd
services.exe
cmd.exe
Created:
2024-04-12 10:32:44
net.exe
nltest.exe
net.exe

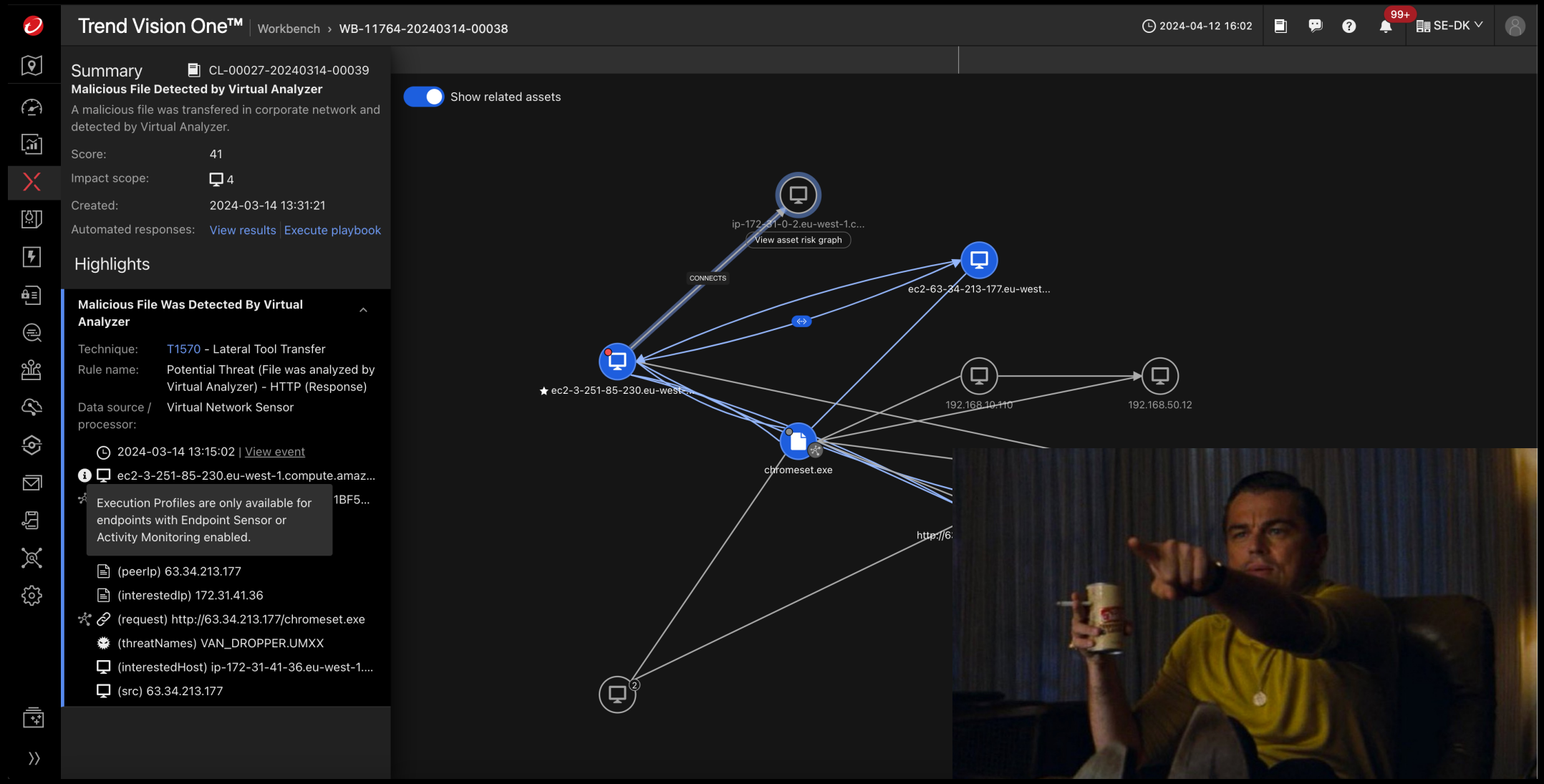

Trend Vision One™
Workbench › WB-11764-20240412-00038 › Execution Profile
2024-04-12 16:37
99+
SE-DK
Save Progress
2024-04-10 13:23:30
2024-04-12 10:32:45
Switch to Timeline View
Observed Attack Techniques
Endpoints
2024-04-12 10:32:44 | View event
ec2amaz-hd4ib70
ScreenConnect Invoking Commands
Account Discovery on the Domain Controller
Permission Groups Discovery
T1133 - External Remote Services
T1190 - Exploit Public-Facing Application
(objectCmd) net.exe group "Domain Admins...
(parentCmd) "C:\Program Files (x86)\Screen...
(processCmd) "cmd.exe" /c "C:\Windows\TE...
(parentFilePath) C:\Program Files (x86)\Scre...
(processFilePath) C:\Windows\System32\cm...
(endpointHostName) EC2AMAZ-HD4IB70
(parentUser) SYSTEM
2024-04-12 10:32:45 | View event
ec2amaz-hd4ib70
ScreenConnect Invoking Commands
Domain Trusts Discovery via Nltest
T1133 - External Remote Services
T1190 - Exploit Public-Facing Application
(objectCmd) nltest.exe /domain_trusts /all_tr...
(parentCmd) "C:\Program Files (x86)\Screen...
(processCmd) "cmd.exe" /c "C:\Windows\TE...
(parentFilePath) C:\Program Files (x86)\Scre...
(processFilePath) C:\Windows\System32\cm...
(endpointHostName) EC2AMAZ-HD4IB70
(parentUser) SYSTEM
ec2amaz-hd4ib7...
GENERAL
Copy to Clipboard
SEARCH
New Search
RESPONSE
Isolate Endpoint
Start Remote Shell Session
Run Remote Custom Script
msiexec.exe
ScreenConnect.C...e.exe
ScreenConnect.C...e.exe
services.exe
cmd.exe

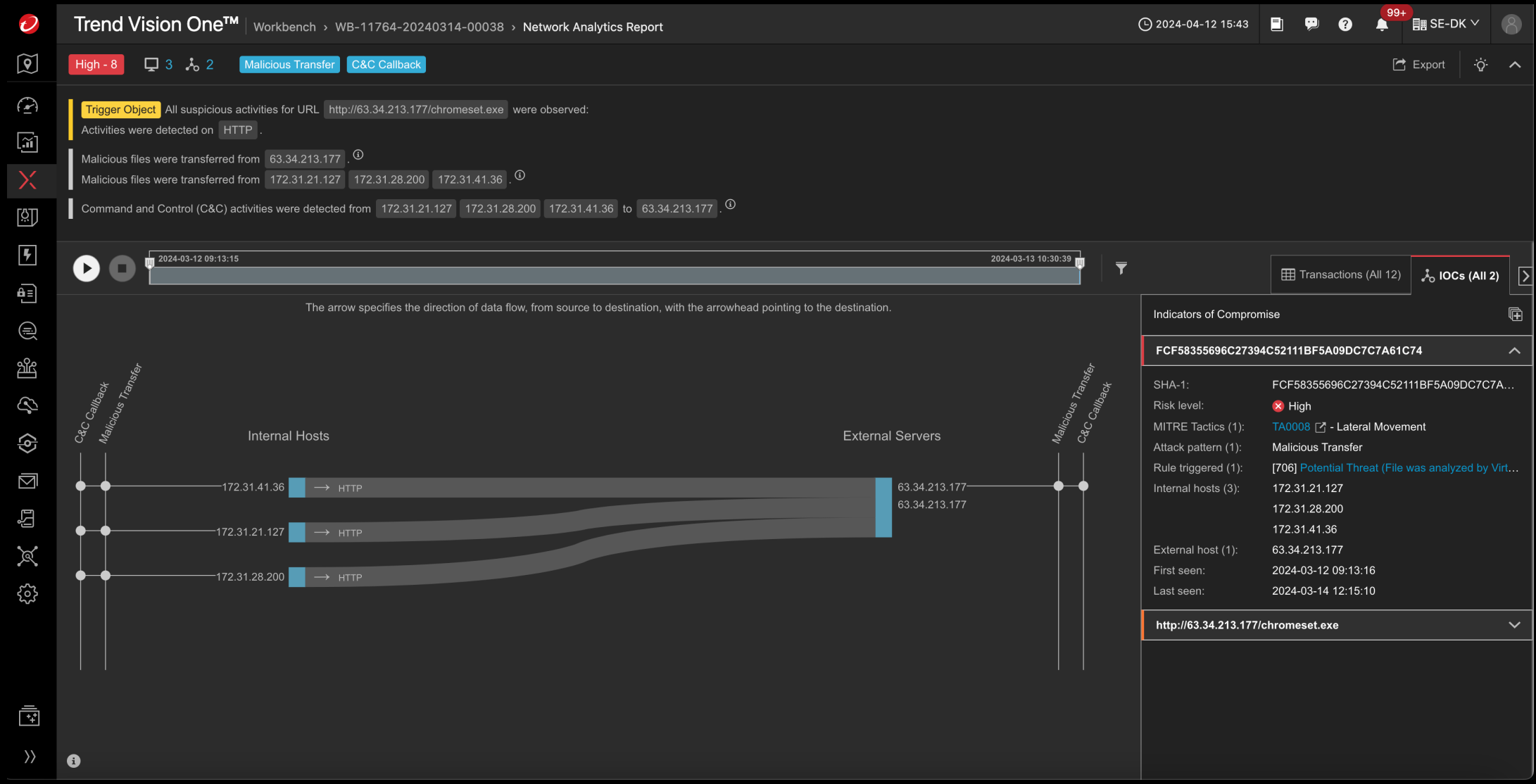
And in case the team missed something?


Trend Vision One™
Workbench › IC-11764-20240410-00001
2024-04-12 16:17
99+
SE-DK
100
Score
Adversary is trying to do External Remote Services which leads the Data Encrypted for Impact
Created: 2024-04-10 07:00:36 Last updated: 2024-04-12 16:15:36 (Alert removed by Jesper Mikkelsen)
Attack Phase
Initial Access, Persistence, Discovery, Command and Control, Impact
Case
Open new case
Overview
Impact Scope (12)
Highlighted Objects (85)
Alerts (64)
Highlights
What's New
Behavior Monitoring Detection for Built-in Windows Tools
2024-04-10 13:32:58 | View event
ec2amaz-hd4ib70
Domain Trusts Discovery via Nltest
2024-04-10 13:32:58 | View event
ec2amaz-hd4ib70
ScreenConnect Invoking Commands
2024-04-10 13:32:58 | View event
ec2amaz-hd4ib70
Download Via Certutil.exe
2024-04-10 13:32:58 | View event
ec2amaz-hd4ib70
Ransom Note Detection (Real-time Scan)
2024-04-10 13:33:02 | View event
ec2amaz-hd4ib70
Ransomware Detection
2024-04-10 13:33:02 | View event
ec2amaz-hd4ib70
Ransomware File Detected
Show related assets
Insight-Based Execution Profile
TM-TMES
tmlab\administrator
TM-AD01.TMLAB.DK
ec2-3-250-199-111.eu-west
ec2amaz-hd4ib70
ec2amaz-t1e26cu
SUSPICIOUS COMMAND
SAME MALWARE


Trend Vision One™
Workbench › IC-11764-20240410-00001
2024-04-12 16:19
99+
SE-DK
100
Score
Adversary is trying to do External Remote Services which leads the Data Encrypted for Impact
Created: 2024-04-10 07:00:36 Last updated: 2024-04-12 16:15:36 (Alert removed by Jesper Mikkelsen)
Attack Phase
Initial Access, Persistence, Discovery, Command and Control, Impact
Case
Open new case
Overview
Impact Scope (12)
Highlighted Objects (85)
Alerts (64)
Created: All
Model name: All
Model type: All
Data source / processor: All
Findings: All
Search
Score
Model name
Model severity
Relationship
Impact scope
Data source / processor
Created
Findings
62 WB-11764-20240410-00050 Possible ScreenConnect Vulnerability High Similar commands observed amo... 1 2 1 Endpoint Sensor 2024-04-10 13:38... -
61 WB-11764-20240410-00058 File Download via Certutil High Similar commands observed amo... 1 2 1 Endpoint Sensor 2024-04-10 13:40... -
61 WB-11764-20240410-00057 Ransom Note Detection (Real-time Scan) Critical Same detection name in short per... 1 Server & Workload Protection 2024-04-10 13:41... -
61 WB-11764-20240410-00054 File Download via Certutil High Similar commands observed amo... 1 1 1 Endpoint Sensor 2024-04-10 13:39... -
61 WB-11764-20240410-00049 Ransom Note Detection (Real-time Scan) Critical Same detection name in short per... 1 Server & Workload Protection 2024-04-10 13:38... -
53 WB-11764-20240412-00046 Behavior Monitoring Detection for Built-in Windows Tools High Same detection name in short per... 1 Server & Workload Protection 2024-04-12 10:37... -
53 WB-11764-20240411-00044 Behavior Monitoring Detection for Built-in Windows Tools High Same detection name in short per... 1 Server & Workload Protection 2024-04-11 11:47:... -
53 WB-11764-20240411-00043 Behavior Monitoring Detection for Built-in Windows Tools High Same detection name in short per... 1 Server & Workload Protection 2024-04-11 11:45:... -
53 WB-11764-20240411-00041 Behavior Monitoring Detection for Built-in Windows High Same detection name in short per 1 Server & Workload Protection 2024-04-11 11:45: -
Total: 64
50 per page
1 / 2


Trend Vision One™
Workbench › WB-11764-20240314-00038
2024-04-12 16:02
99+
SE-DK
Summary
CL-00027-20240314-00039
Malicious File Detected by Virtual Analyzer
A malicious file was transfered in corporate network and detected by Virtual Analyzer.
Score: 41
Impact scope: 4
Created: 2024-03-14 13:31:21
Automated responses: View results | Execute playbook
Highlights
Malicious File Was Detected By Virtual Analyzer
Technique: T1570 - Lateral Tool Transfer
Rule name: Potential Threat (File was analyzed by Virtual Analyzer) - HTTP (Response)
Data source / processor: Virtual Network Sensor
2024-03-14 13:15:02 | View event
ec2-3-251-85-230.eu-west-1.compute.amaz...
Execution Profiles are only available for endpoints with Endpoint Sensor or Activity Monitoring enabled.
(peerIp) 63.34.213.177
(interestedIp) 172.31.41.36
(request) http://63.34.213.177/chromeset.exe
(threatNames) VAN_DROPPER.UMXX
(interestedHost) ip-172-31-41-36.eu-west-1....
(src) 63.34.213.177
Show related assets
ip-172-31-0-2.eu-west-1.c...
View asset risk graph
CONNECTS
ec2-63-34-213-177.eu-west...
ec2-3-251-85-230.eu-west-...
192.168.10.110
192.168.50.12
chromeset.exe
http://63.34.213.177/chro...
63.34.213.177


Trend Vision One™
Workbench › WB-11764-20240314-00038
2024-04-12 16:02
99+
SE-DK
Summary
CL-00027-20240314-00039
Malicious File Detected by Virtual Analyzer
A malicious file was transfered in corporate network and detected by Virtual Analyzer.
Score: 41
Impact scope: 4
Created: 2024-03-14 13:31:21
Automated responses: View results | Execute playbook
Highlights
Malicious File Was Detected By Virtual Analyzer
Technique: T1570 - Lateral Tool Transfer
Rule name: Potential Threat (File was analyzed by Virtual Analyzer) - HTTP (Response)
Data source / processor: Virtual Network Sensor
2024-03-14 13:15:02 | View event
ec2-3-251-85-230.eu-west-1.compute.amaz...
Execution Profiles are only available for endpoints with Endpoint Sensor or Activity Monitoring enabled.
(peerIp) 63.34.213.177
(interestedIp) 172.31.41.36
(request) http://63.34.213.177/chromeset.exe
(threatNames) VAN_DROPPER.UMXX
(interestedHost) ip-172-31-41-36.eu-west-1....
(src) 63.34.213.177
Show related assets
ip-172-31-0-2.eu-west-1.c...
View asset risk graph
CONNECTS
ec2-63-34-213-177.eu-west...
ec2-3-251-85-230.eu-west-...
192.168.10.110
192.168.50.12
chromeset.exe


Trend Vision One™
Workbench › WB-11764-20240314-00038 › Network Analytics Report
2024-04-12 15:43
99+
SE-DK
High - 8
3
2
Malicious Transfer
C&C Callback
Export
Trigger Object All suspicious activities for URL http://63.34.213.177/chromeset.exe were observed:
Activities were detected on HTTP .
Malicious files were transferred from 63.34.213.177 .
Malicious files were transferred from 172.31.21.127 172.31.28.200 172.31.41.36 .
Command and Control (C&C) activities were detected from 172.31.21.127 172.31.28.200 172.31.41.36 to 63.34.213.177 .
2024-03-12 09:13:15
2024-03-13 10:30:39
Transactions (All 12)
IOCs (All 2)
The arrow specifies the direction of data flow, from source to destination, with the arrowhead pointing to the destination.
C&C Callback
Malicious Transfer
Internal Hosts
External Servers
Malicious Transfer
C&C Callback
172.31.41.36
172.31.21.127
172.31.28.200
HTTP
HTTP
HTTP
63.34.213.177
63.34.213.177
Indicators of Compromise
FCF58355696C27394C52111BF5A09DC7C7A61C74
SHA-1: FCF58355696C27394C52111BF5A09DC7C7A...
Risk level: High
MITRE Tactics (1): TA0008 - Lateral Movement
Attack pattern (1): Malicious Transfer
Rule triggered (1): [706] Potential Threat (File was analyzed by Virt...
Internal hosts (3): 172.31.21.127
172.31.28.200
172.31.41.36
External host (1): 63.34.213.177
First seen: 2024-03-12 09:13:16
Last seen: 2024-03-14 12:15:10
http://63.34.213.177/chromeset.exe

MxDR Security Incident Analysis Report

Case Number: **31415926**

Prepared for **GREENTHIS**

Thank you!

Jesper Mikkelsen

Technical Director Nordics.