cybereason

- An EDR platform

A report by Pedapati Prem Kumar

INTRODUCTION

Cybereason is an advanced End Point Detection response (EDR) and Extended Detection and Response (XDR) platform that is designed to detect, analyse and respond to cyber threats across endpoints, networks, and the cloud. Cybereason was founded by three former Israeli military intelligence (unit 8200) operatives Lior Div, Yonatan Amit and Yossi Naar in 2012. The company was headquartered in Boston, Massachusetts (USA), with research and development operation in Tel Aviv, Israel. It has grown into major cybersecurity vendor, backed by investors including Soft Bank, CRV and Spark Capital. It leverages behavioral analytics, machine learning and threat intelligence to provide proactive defence against malware, ransomware, and advanced persistent threats (API's). The platform's widely adopted in enterprise environments for its strong correlation capabilities and automated response features.

Key Features:

Malop Operations: Proprietary feature that correlates multiple malicious activities into a single incident (Malop). It also helps security teams prioritize investigations by focusing on completing attack campaigns rather than isolated alerts.

Threat Intelligence Integration: Enriches detections with global threat intelligence feeds. Provides context around the threat actors, TTPs, (tactics, techniques, procedures), and known IOCs.

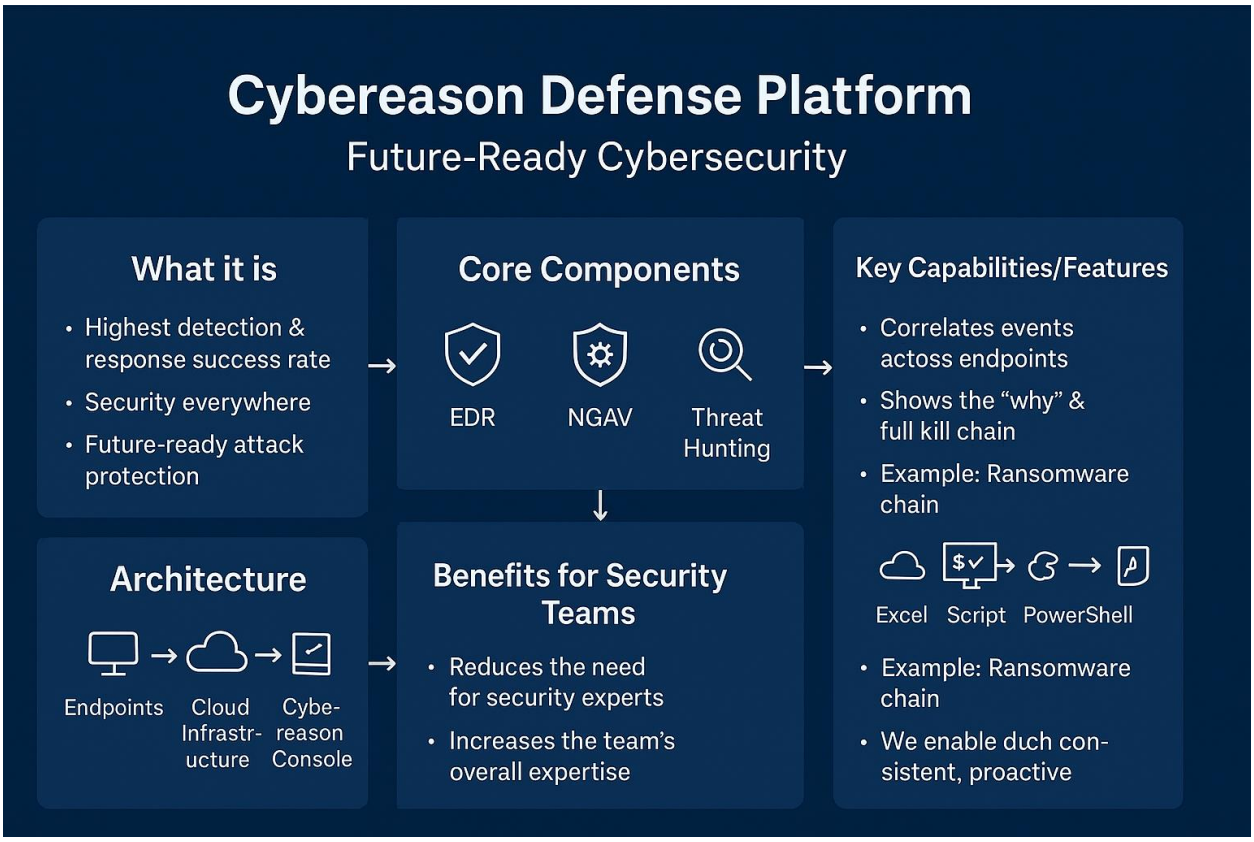
Endpoint Detection and Response: Monitors endpoint activities in real time and detect malicious behaviour using behavioral and machine learning models. Provides detailed attack timelines with visual maps for easier incident analysis.

Extended Detection and Response: Integrates telemetry across endpoint, cloud, identities and networks and provides holistic detection and correlation of attack chains. Enhances visibility into complex attacks like lateral movement and credentials abuse.

Artificial Intelligence and Machine Learning: AI assists threat hunters by flagging anomalies in large datasets. Analysts can run queries across billions of endpoint events, with ML modules surfacing likely malicious activity and reduces manual hunting time and enhances proactive detection.

Attack Storyline Visualization: Reduces manual hunting time and enhances proactive detection and instead of isolated alerts, Cybereason builds a visual timeline of the full attack chain. Each event (initial compromise, lateral movement, credential theft, exfiltration, etc.) is chronologically ordered.

Chronological Event Correlation: Collects detailed telemetry from endpoints (process creation, registry changes, files modifications, network connections) and it also correlates those logs into a unified forensic timeline. Provides precise timestamps for every malicious action, which is critical for investigations.



An overview of Cybereason Defense Platform

The Cybereason EDR solution, built upon Cybereason Technology, is composed of several integrated platform components that work together to provide comprehensive protection from the endpoint to the broader corporate structure. The core of the Cybereason is integrate with next generation antivirus (NGAV) and proactive threat hunting. This combination enables the platform to provide rich, detailed analysis for every part of a malicious operation. There are some optional dashboards that which are used to analyse and respond the attacks.

They are:

1. Discovery Board

2. Malop Inbox

3. Malware Alerts

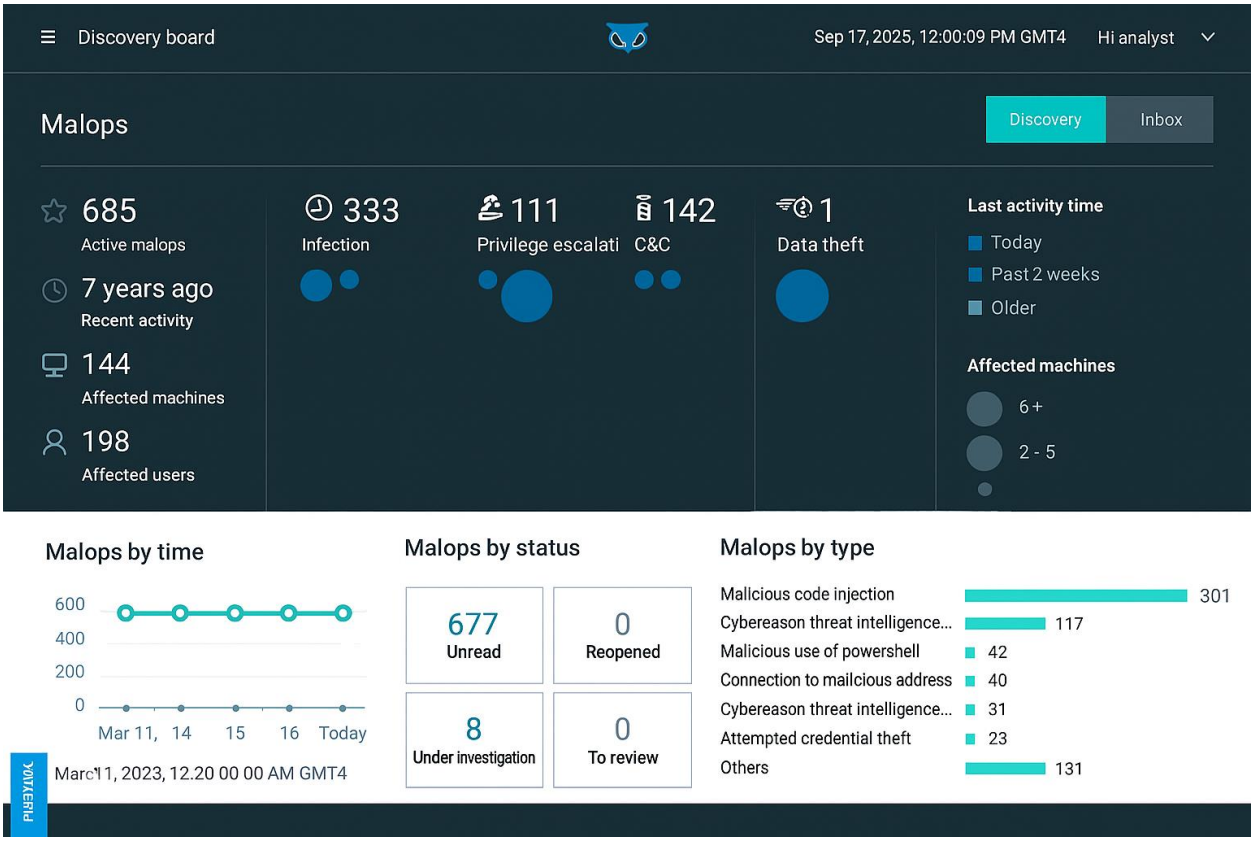
4. Investigation

5. Security Profile

Discovery Board

The Discovery Dashboard is a centralized interface used in Cybereason platform to provide analysts with a clear and consolidated view of potential malicious operations (MalOps) happening within an environment. Its main purpose is to help security teams quickly detect, categorize, and monitor suspicious activities across machines and users. By consolidating threat intelligence, attack stages, and investigation status into one place, the dashboard enables faster incident response, prioritization of threats, and overall better visibility into the security posture of the organisation. In short, it acts as a command center for identifying, tracking, and managing security incidents efficiently. Discovery Board categorizes the malops activities into different malicious activities into stages of the attack which was performed by the attacker.

The Bubbles/Circles in the discovery dashboard are a visual representation of different categories of malicious activities. Their primary purpose is to make complex security data easier to interpret immediately.

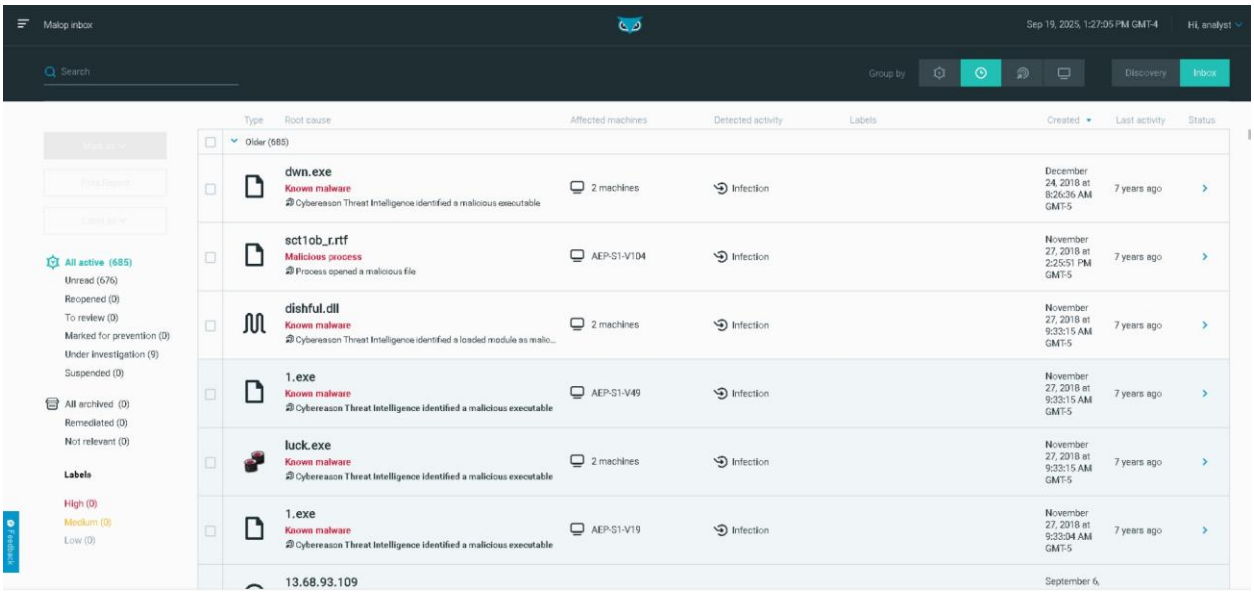


Dashboard Of Discovery Board

The size of the bubble reflects the volume or severity of incidents in that category. Larger bubbles indicate a higher number of detailed numbers and colour of bubble reflects the past/active stage of the attack like dark colour of the bubble represents older attacks and light colour bubbles indicates the recent/present activity.

Malop Inbox

The Malop Index is a central hub for managing ongoing and historical security incidents, giving analysts an easy way to track infections, understand the root cause, and take remediation actions. It highlights the root cause, so we know what triggered the attack in the first place. It helps to group and filter Malops to gain an understanding of your system status. It sorts the list by Type, Root causes, affected machines, detected activity, Labels, creation date, time of last activity, and Status. Malops provide visibility into lateral movement, privilege escalation and other attack techniques, using advanced threat intelligence and behavioral analysis.



Dashboard of Malop Index

As per the picture above we can see the dashboard of the Malop Index which contain several categories and classifications of the attacks on the left side of the dashboard which shows the severity of the attacks – High, Medium and Low.

By clicking on any those attacks that are shown in the malop index can create and displays the graphical visual representation of the attack with the help of artificial intelligence and machine learning algorithms. These Malop Index contains four main tabs which are used to breakdown the attack into various stages and factors that are affected by the system. Those four tabs include:

A**. Overview**

B. Process Profile

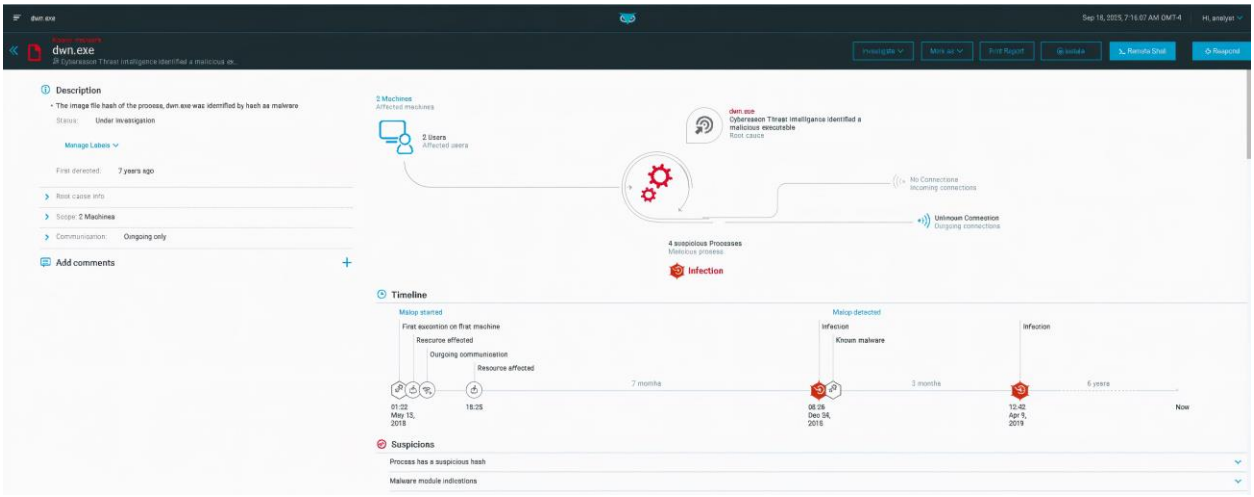
C. Communication Profile

D. Machine Profile

E. Users Profile

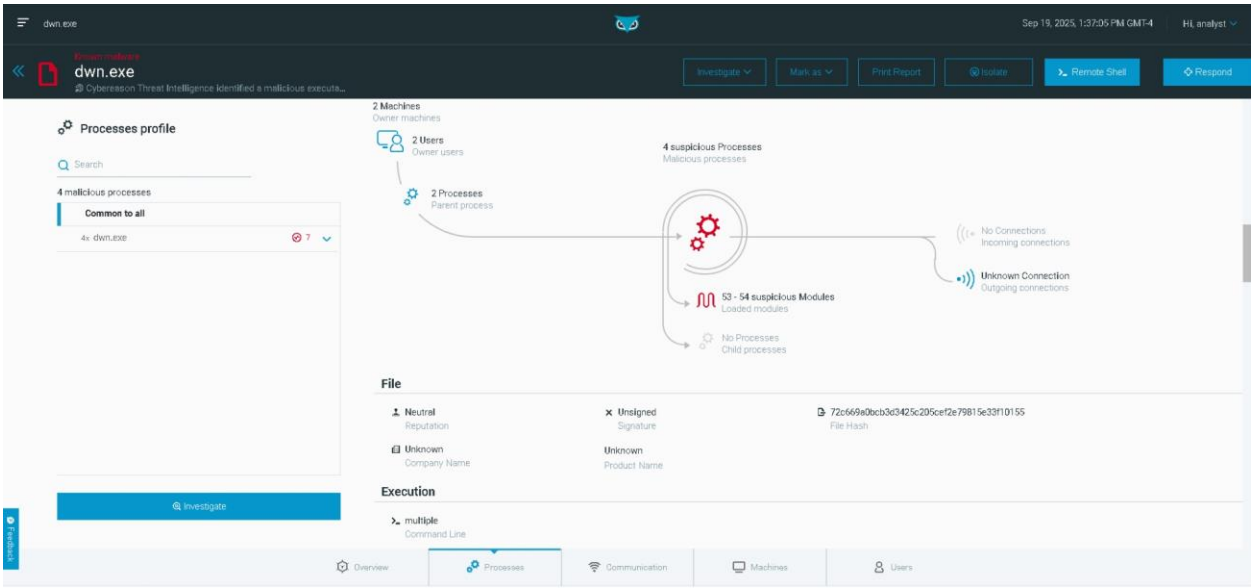
These four tabs describes about various information of the attack at different stages and provides visual data representation of the attack at their perspective stage.

A. Overview: This section contains a detailed description page of the attack which contain information like Root-cause information, Scope of impact, Detection age, Timeline of events, Suspicious indicators and Isolate & Response options.



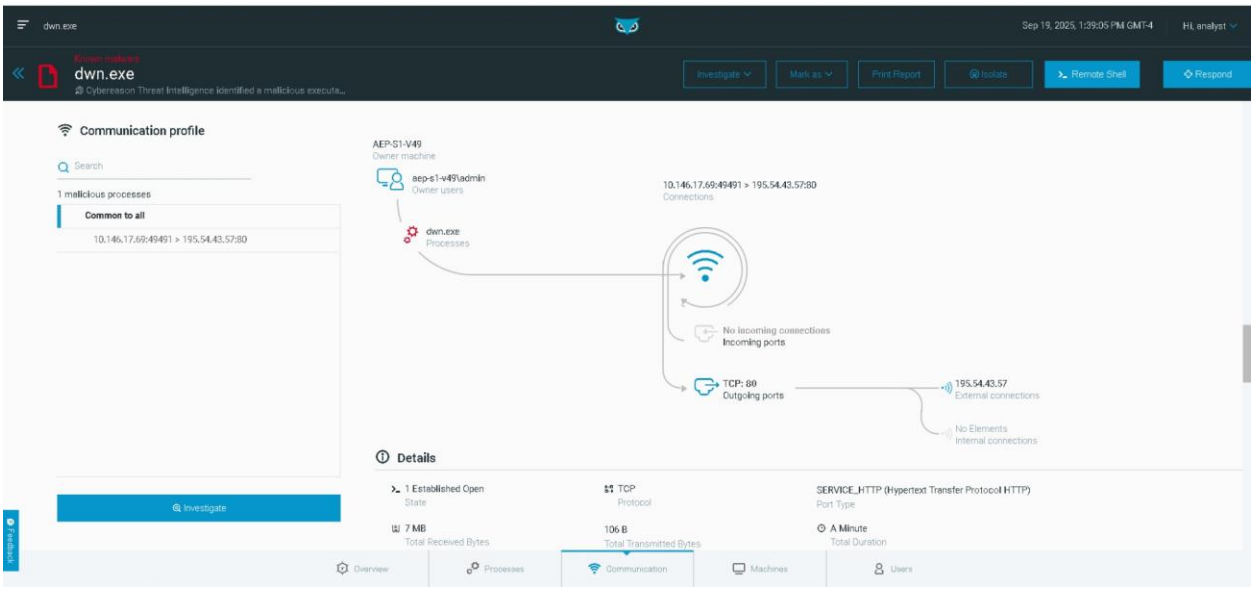
Dashboard of Overview Tab

B. Process Profile: The process profile tab contains details of the attack in a process's perspective. This dashboard shows details of the process that are part of the Malop which includes child processes, IDs, .exe files, execution commands, sessions and suspicious modules that are involved in the attack.



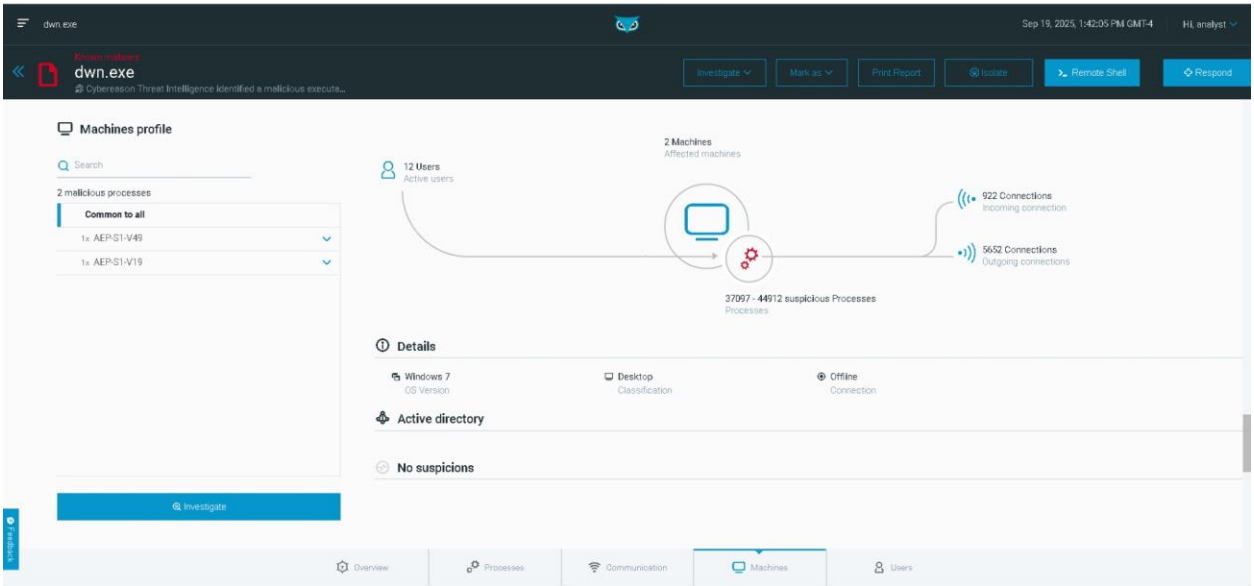
Dashboard of Process Profile

C. Communication Profile: Communication profile tab describes about details in network perspective. It contains details about User connections, ports, protocols, services, Internal/External connections and graphical representation of the attack. It also describes about the domains and data bytes that are transmitted through a network.



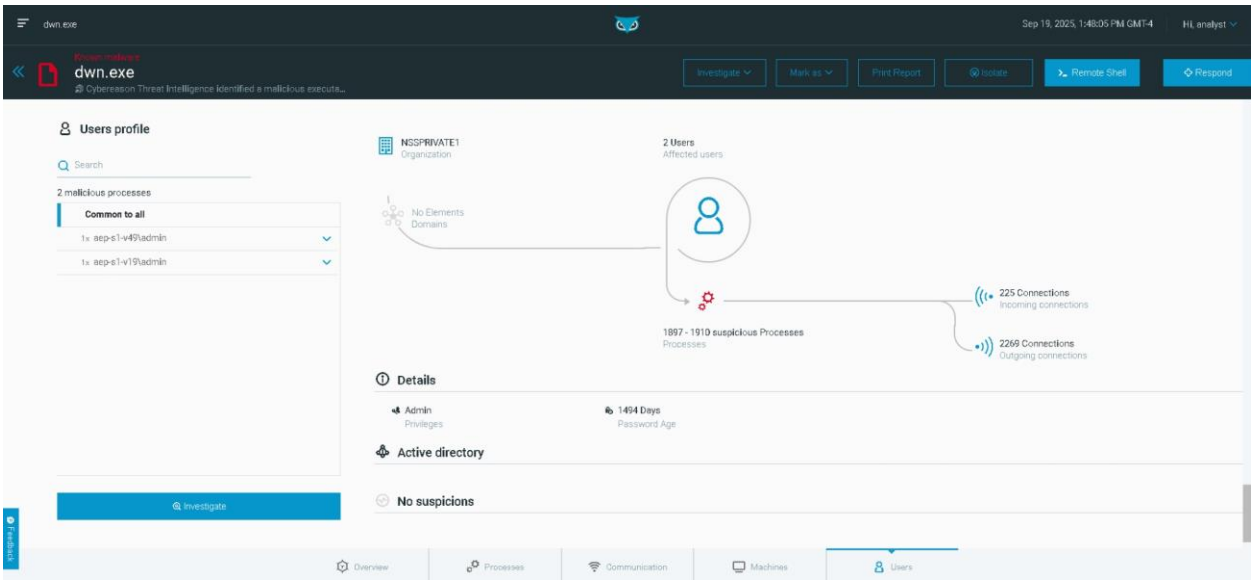
Dashboard of communication profile

D. Machine Profile: Machine profile describes about the machines that are involved and affected in the attack. It contains detailed information like Connections status, Domain controllers, OS, and DNS host name. These all are represented by visual tree representation.



Dashboard of Machine Profile

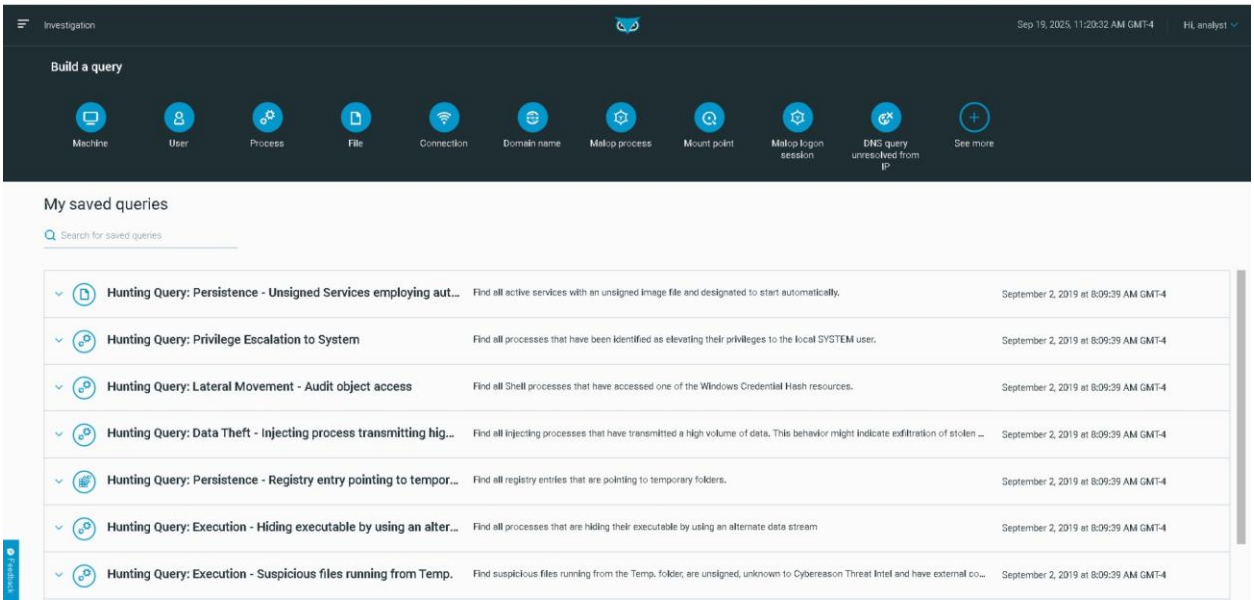
E. Users Profile: The Users profile shows the information about the users that are involved in the attack and associated with it. It shows detailed information of the Malicious users, user connections (incoming/outgoing), Admin privileges and visual graphical representation.



Dashboard of User profile

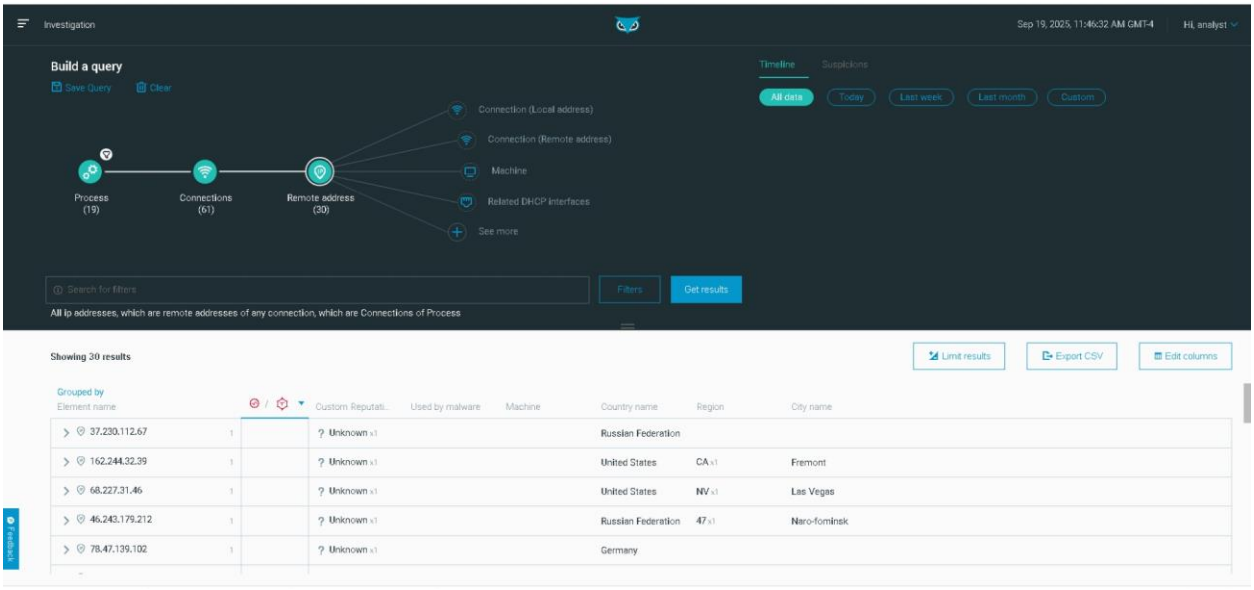
Investigation

Investigation tab in Cybereason EDR platform involves in which security analysts can build or use saved queries to detect malicious activity. It provides hunting queries for persistence mechanisms, privilege escalation, lateral movement and data theft.



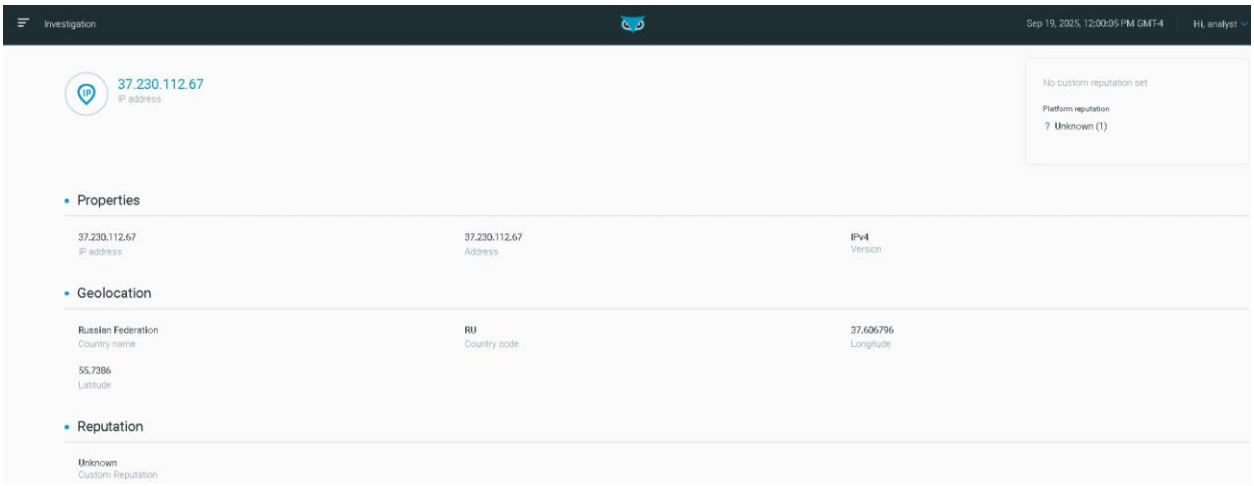
Dashboard of Investigation tab

It is an interactive query-building screen which contain build a query workflow, connection analysis, timeline-suspicion filters, IP addresses and user-time analysis.



Dashoboard of Build a query

By clicking on any of these element results that are processed by the investigation will show the details of the attack. It will completely elaborate the information like geolocation of the country, country code, IP address, longitude and latitude of the location.



Dashboard of Element (machine)

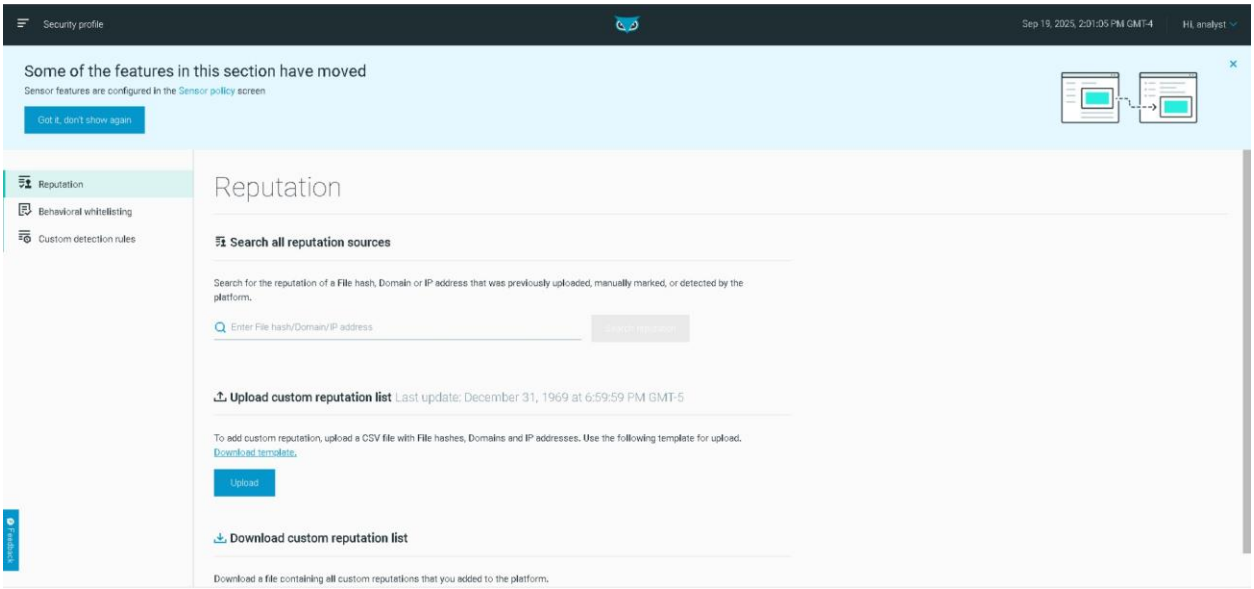
The investigation highlights communication between internal processes and multiple external destinations, some located in regions often associated with heightened cybersecurity risk. While no effective malicious attribution is provided in the current findings, the presence of unknown reputations suggests the need for further enrichment, monitoring, and potential escalation for deeper threat intelligence validation. This ensures that suspicious or high-risk communications are not overlooked. It allows analysts to build queries that trace how internal processes interact with external destinations, enabling the destination that could signal malware activity, command-and –control connections or attempts at data exfiltration.

By mapping communication flows and correlating them with contextual information such as geolocation and usage analysts gain visibility into whether connections are legitimate or potentially harmful. The platform also supports deeper forensic analysis by providing detailed insights into specific external entities, including their properties, origin and reputation status, which helps in assessing risk and correlating findings with threat intelligence feeds. This dual capability of broad mapping and detailed examination enhances proactive threat hunting, incident response, and compliance reporting. It not only enables faster detection of anomalies but also equips teams to make informed decisions on blocking, monitoring, or escalating suspicious activities.

Ultimately its application lies in strengthens an organisati0ons ability to investigate complex security incidents, uncover hidden threats, and maintain resilience against evolving cyberattacks.

SECURITY PROFILE

Security profile section is designed to help analysis manage and analyze the trustworthiness of different digital entities such as file hashes, domains, and IP addresses. At the top, there is a notification banner indicating that some features related to sensors have been moved to a different configuration area that shows various functions like search all reputation sources, upload custom reputation list, and download custom reputation list.



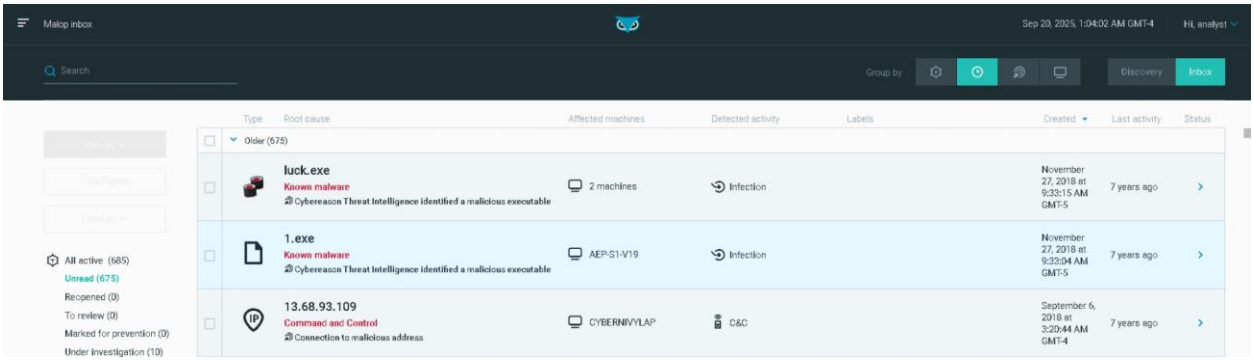
Dashboard of Security Profile

Analyst can input a file hash, domain, or IP address to check its reputation within the platform. This helps in quickly identifying whether an entity has been flagged as safe, suspicious, or automated detections. Analysts can report a file containing all custom reputations that have been uploaded to the platform, making it easier to share, review, or migrate reputation data.

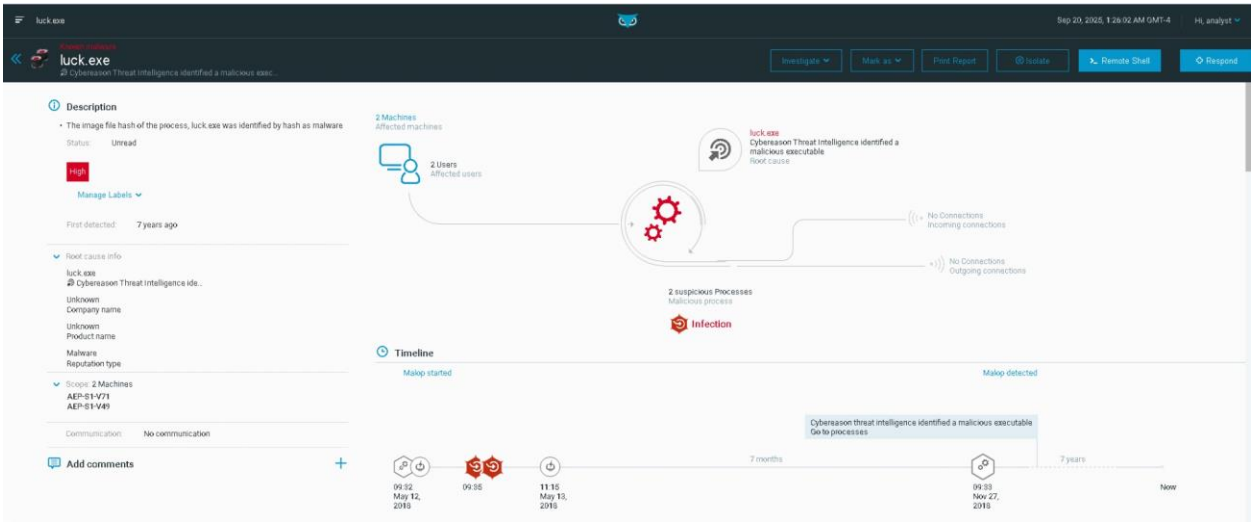
Download custom reputation list enables analysts to export a file containing all custom reputations that have been uploaded to the platforms, making it easier to share, review, or migrate reputation data.

1. Add details of 3 investigation added in malop inbox.

These are 3 investigations that are visualized in malop inbox. In these 3 Logs contain two executable files which contain malware activities and one command & control activity.



1.1 The first investigation luck.exe is identified as malicious executable file which affected the systems and admin users to achieve privilege escalation.



Detected Activity- Malware infection

Affected Machines – AEP-S1-V49, AEP-S1-V71

Affected Users – aep-s1-v49\admin, aep-s1-v71\admin

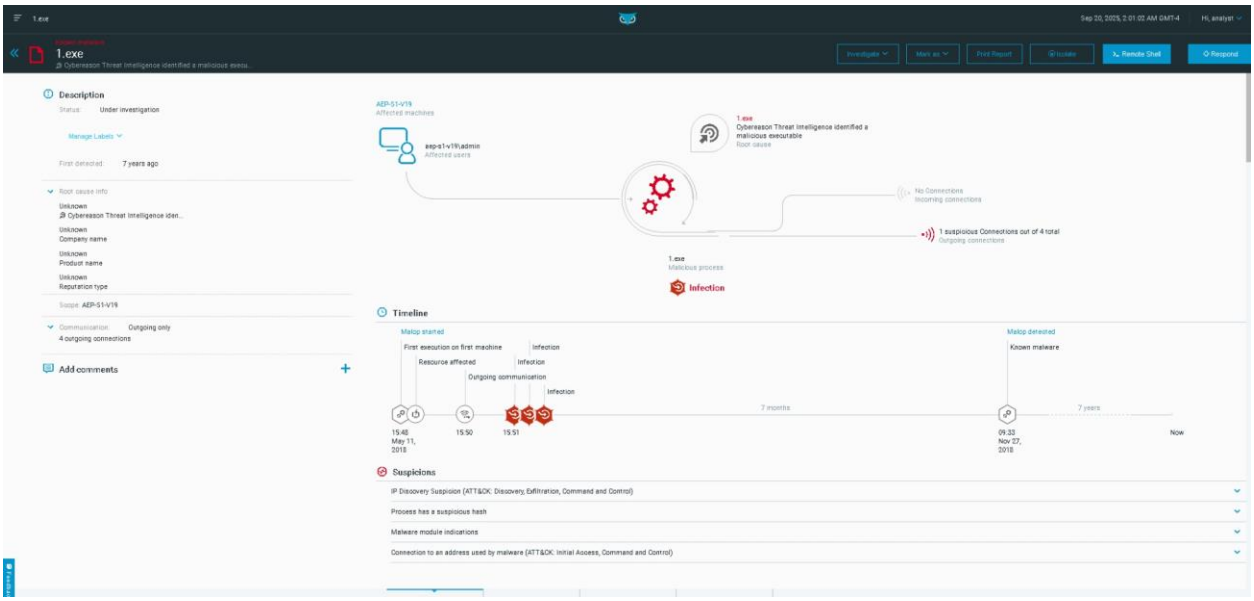
Parent Process – luck.exe

Child Processes - winspool.drv, VERSION.dll

Privileges- Admin level

Date and Time – May 12, 2018, at 9:32:07 AM GMT-4

1.2 The second investigation is malicious executable file 1.exe which is classified into Initial access and Command & control attack with help of MITRE ATT&CK framework.



Detected Activity – Malware Infection

Affected Machine – AEP-S1-V19

Affected users – aep-s1-v19\admin

Parent Process – cmd.exe

Suspicious Modules – AUTHZ.dll{floating}, SETUPAPI.dll{floating}, Securit.dll(floating}

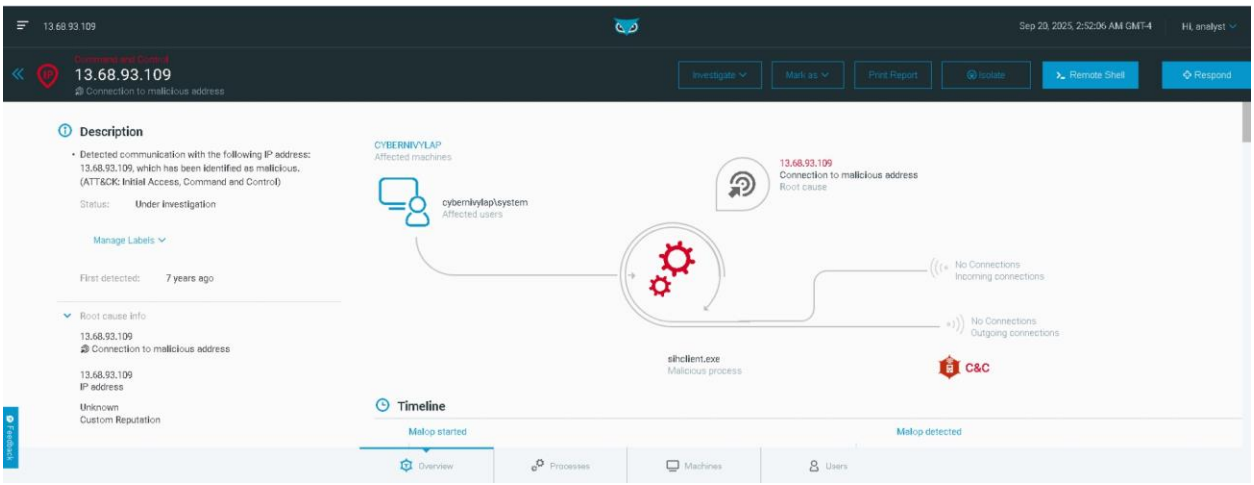
Privileges – Admin

Date and Time – May 12 ,2018 At 11:59:37 AM GMT-4

MITRE ATT&CK – Initial access and Command & Control

1.3 The third investigation is Command and Control stage log which showed the remote connection to unknown address and gained remote access to the owner machine by executing the commands. Detected the communication with the following Ip address 13.68.93.109 and 108.177.15.108 which has been identified as malicious. (MITRE ATTA&K – Initial Access, Command and Control connection, Exfiltration)

An unresolved DNS query sls.update.microsoft.com {communication error} is detected which is used to establish the connection and made an error while connection to malicious address. By analysing the whole attack, we found that location of remote address was united states which they used ports like SMTP and HTTP.



Detection Activity – Remote Access (Initial access, Command and Control)

Machine effected – CYBERNIVYLAP

Malicious Process – svhost.exe, sihclient.exe, minidump.exe,

Affected User- cybernivylap\system

MITRE ATT&CK – Initial Accesses, Command and Control, Exfiltration

Remote Addresses – 13.68.93.109 and 108.177.15.108

Location of remote address – United states

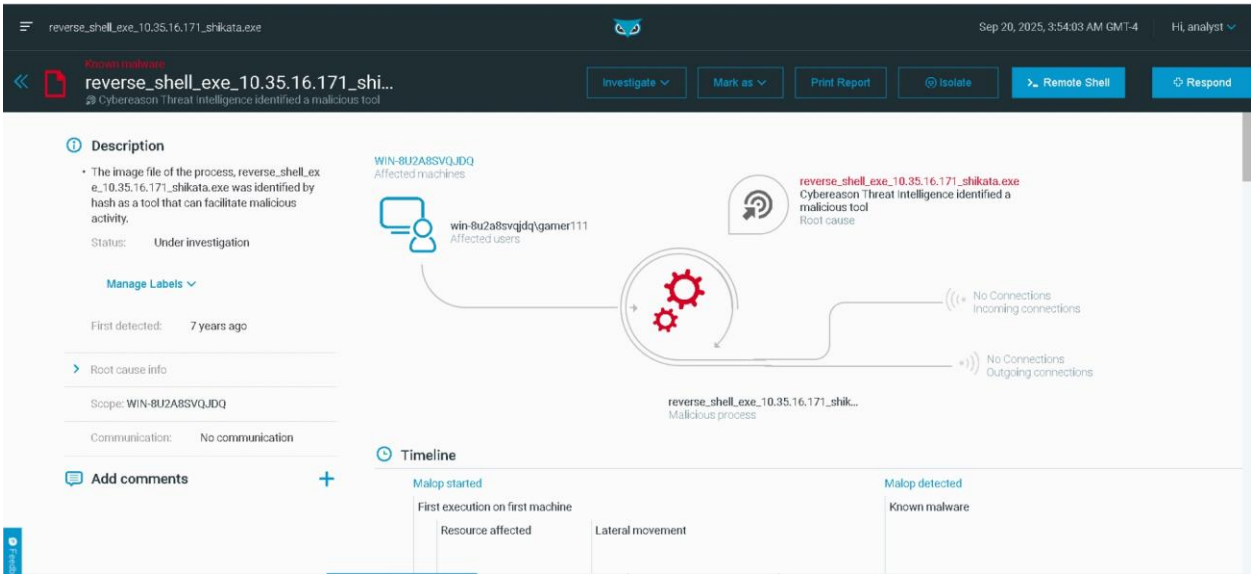
Data Transferred – 9kB and 1367 bytes

Date and Time of start – August 28,2018 at 3:58:29 AM GMT-4

Date and Time of End – September 6,2018 at 4:32:59 AM GMT-4

2. Create a detailed report on detected alert as per lateral movement, C&C and Detected ransomware program

2.1 Lateral Movement – reverse_shell_exe_10.35.16.171_shikata.exe **t**he image file of the process is identified by the hash tool that can facilitate malicious activity.



Detected Activity – Lateral Movement

Affected Machine - –WIN-8U2A8SVQJDQ

Affected User – win-8u2a8svqjdq\gamer111

Parent Process – svhost.exe

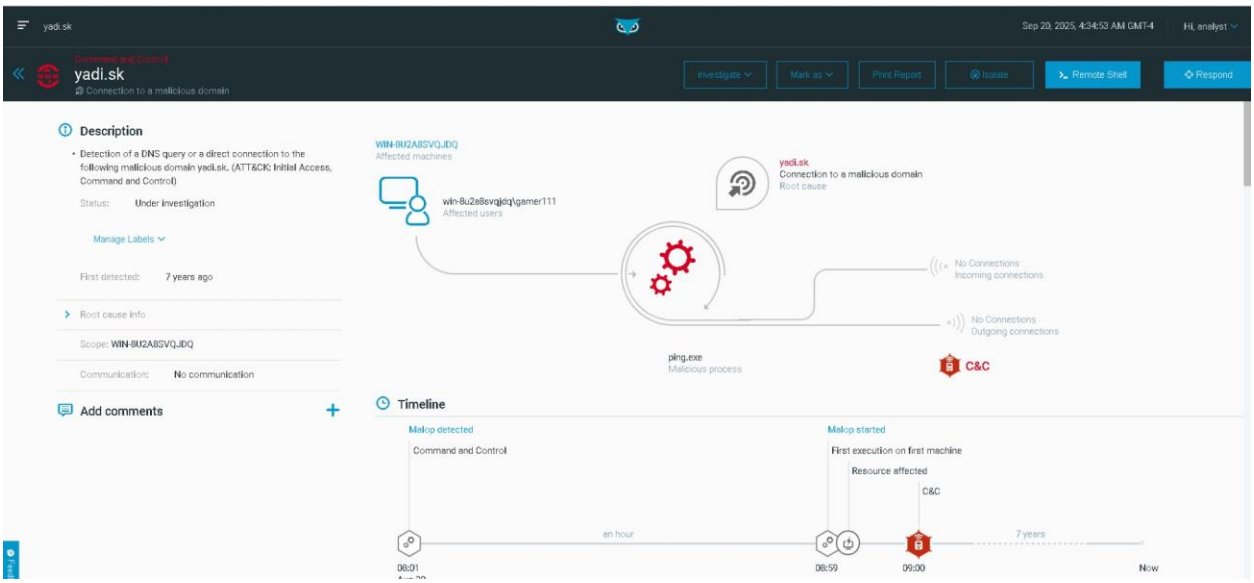
Malicious Process - reverse_shell_exe_10.35.16.171_shikata.exe

Connection – 192.168.203.129:62709 to 5.196.73.76:80

Date and time – September 5, 2018, 03:30 AM GMT-4

2.2 Command and Control – yadi.sk is a malicious domain that is used to establish a connection in command line with the help of **ping.exe** malicious process.

This process timeline shows the attack timeline of the command-and-control activity. As of redirecting the session to the malicious domain they executed ping.exe to load the domain.



Detection Activity – Command and Control

Affected Machine – WIN-8U2A8SVQJDQ

Affected User - win-8u2a8svqjdq\gamer111

Parent Process – cmd.exe

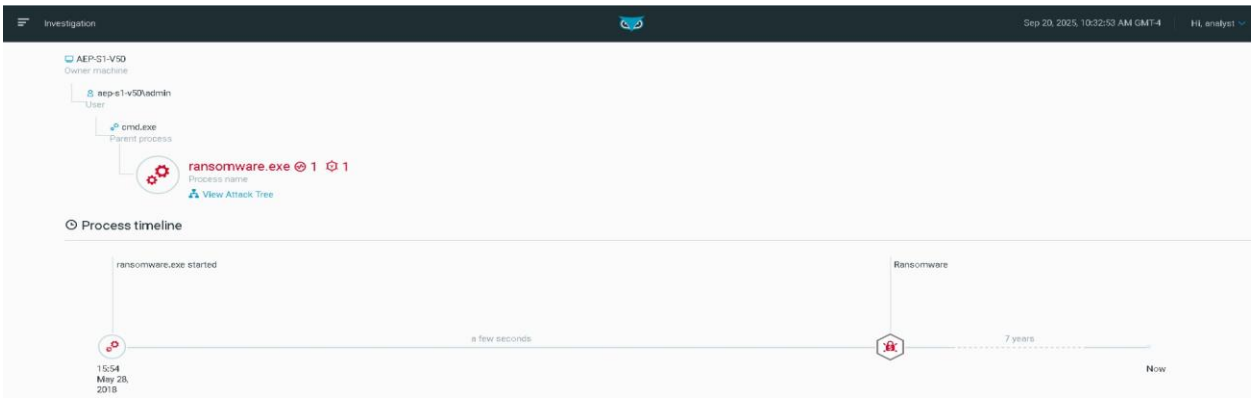
Malicious Process – ping.exe

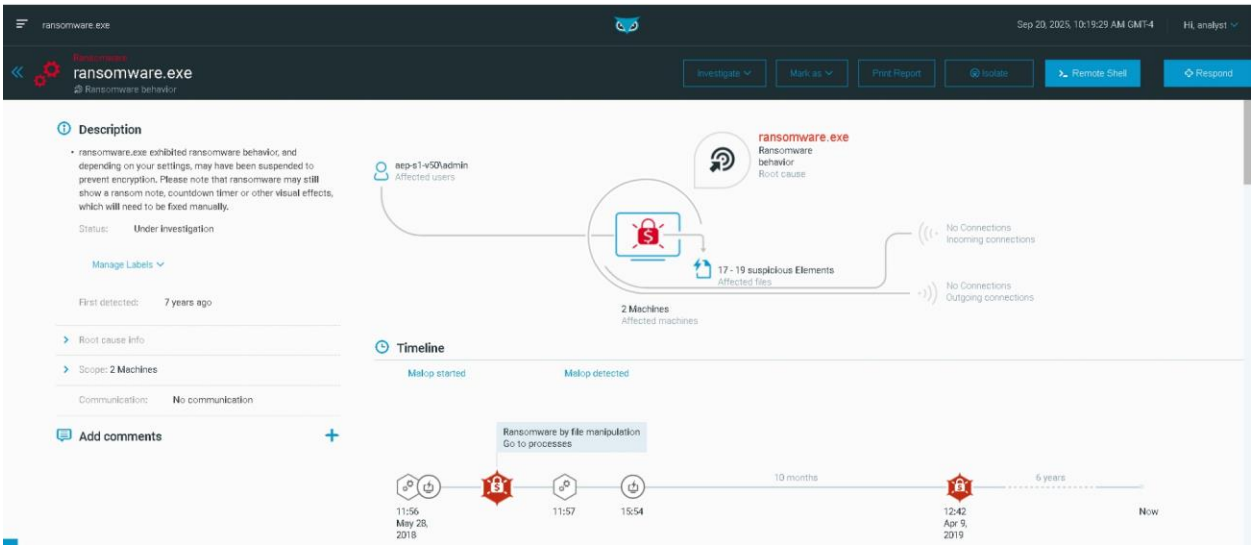
Malicious Domain – yadi.sk

Command line – ping yadi.sk

Date and time – Start = August 20, 2018, 08:59:45 AM GMT-4; End = 08:59:48 AM GMT-4

2.3 Detected Ransomware Program – ransomware.exe is an execuatble program which showed ransomware behavior that is used to encrypt the data in 2 systems and blocked to avoid encryption of the data.





Detected Activity – Ransomware Program

Affected Machines – AEP-S1-V50 and AEP-S1-V72

Affected Users – aep-s1-v50\admin and aep-s1-v72\admin

Parent process – cmd.exe

Malicious process – ransomware.exe

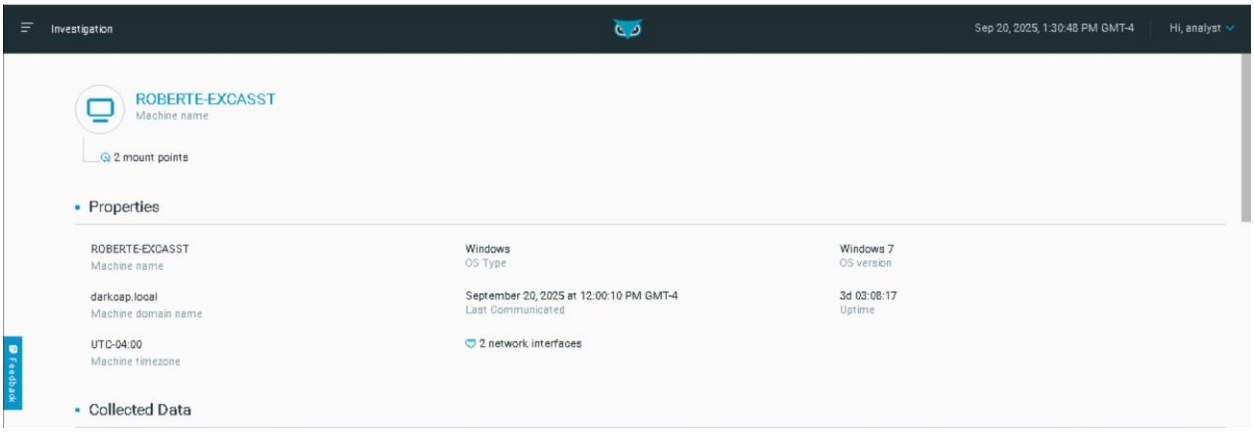
Command line – c:\users\admin\Desktop\ransomware.exe

Privileges – Admin level

Date and time – May 28 2018, 11:56:54 AM GMT-4

3. In Malop box write a detailed report on alert detected in Robert-excasst system.

The machine ROBERTE-EXCASST is an active endpoint running windows 7 within the darkcup.local domain. It is currently connected to the Cybereason platform, not isolated, and last communication very recently.



Machine Name – ROBERTE EXCASST

Machine Domian Name - darkcap.local

Suspicious process - cmd.exe, chrome.exe, svhost.exe, logonui.exe, taskhost.exe

Last communicated - September 20, 2025, at 12:00 PM GMT-4

Remote Address – 172.217.165.202

No. Of Users – 8

Privileges – Admin

MITRE ATT&CK – Lateral movement, Command and Control,

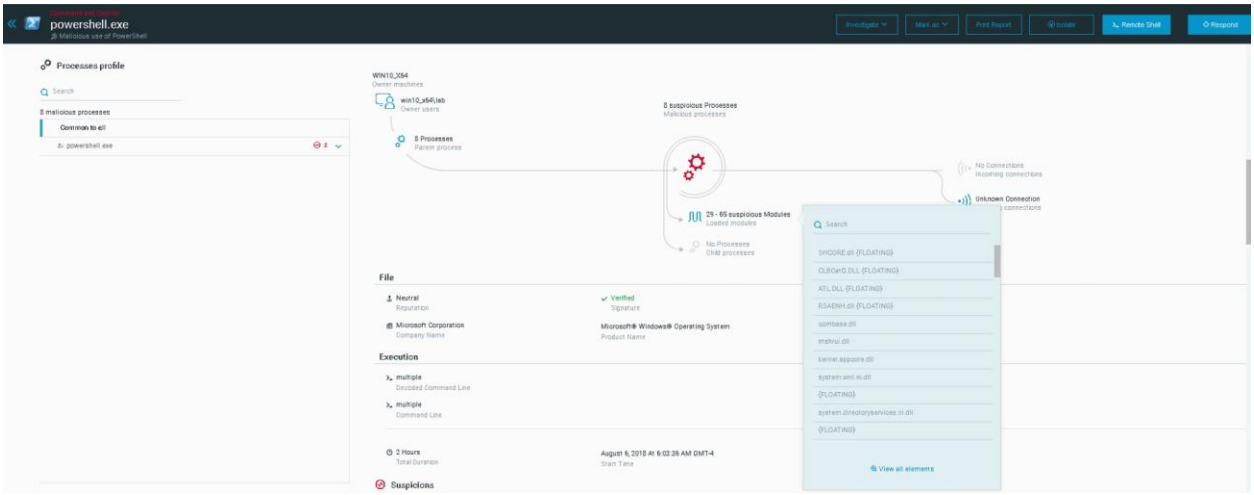
Drivers and Registries – 155 drivers and 5561 entries

This information shows that the Roberte Excasst system was affected by various malicious process and also had several remote connections that indicates the involvement of the unauthorised entry to the system network. Several executable files are analysed and alerted the execution of the files to run commands on the poweshell and command line prompt to achieve lateral movemnet within the network.

In conclusion the Roberte excasst machine is affected by Lateral movement, Command and Control attack and remote connections to remote adresses.

4. Add details of any 5 modules based on PowerShell attack on machines/process.

There are several modules that are found on power shell attack. These modules play a specific task at each stage of the attack to achieve the motive of the attacks.



4.1 SHCORE.dll{floating}

Module Name: SHCORE.dll{floating}

Module Size: 733184 bytes

Machine name: WIN10_X64

Status: Floating module (not permanently mapped in process memory.

Evidence: This DLL was never loaded in standard loader database. It indicates suspicious behavior because legitimate DLLs are loaded by system loader.

4.2 CLBCatQ.DLL {FLOATING}

Module Name: CLBCatQ.DLL {FLOATING}

Module Size: 675840 bytes

Machine name: WIN10_X64

Function: Attackers may inject into it or replace it to execute code stealthy.

Status: Floating module (not permanently mapped in process memory)

Evidence: This DLL was never loaded in standard loader database. It indicates suspicious behavior because legitimate DLLs are loaded by system loader.

4.3 system.xml.dll

Module Name: system.xml.dll

Module size: 1.38 MB

Machine Name: WIN10_X64

Registry entry: False registry entry

Function: Commonly used by the attackers to avoid detection of the malware.

Evidence: Mimics System.xml.dll, a core .NET assembly to avoid suspicion and act as dropper for ransomware, spyware and remote access.

4.4 CRYPTBASE.dll

Module name: CRYPTBASE.dll

Machine name: WIN10_x64

Module size: 45056 Bytes

Regisrty entry: False Registry entry

Function: It is legitimate windows system file associated with cryptographic services.

Status: Floating module (unmapped or detached form the disk)

Evidence: This module is never loaded in standard loader database which indicates DLL injection, relocating and tampering.

4.5 Powershell.exe

Module name: Powershell.exe

Machine name: WIN10_X64

Module size: 469.00 KB

Registry entry: False Registry entry

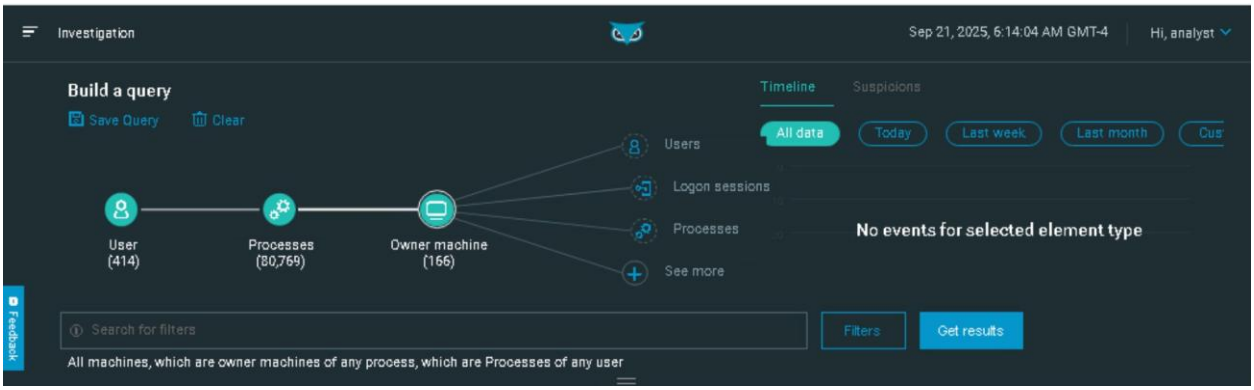
File Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Function: It can execute scripts, download payloads and manipulate system settings

Status: Running malicious scripts without dropping new files

Evidence: This module was never loaded in standard loader database which shows suspicious malicious activity.

5. Investigation option in the side bar - user & process option and add any 3 system details.



Investigation panel is used to build a query to retrieve the data of the selected logs and make it easier to read the logs. Here are some systems that are shown in dteailed using user and process tree.

5.1 CYBERNOAPLAP

System name: CYBERNOAPLAP

Organization: DETECTION TEAM

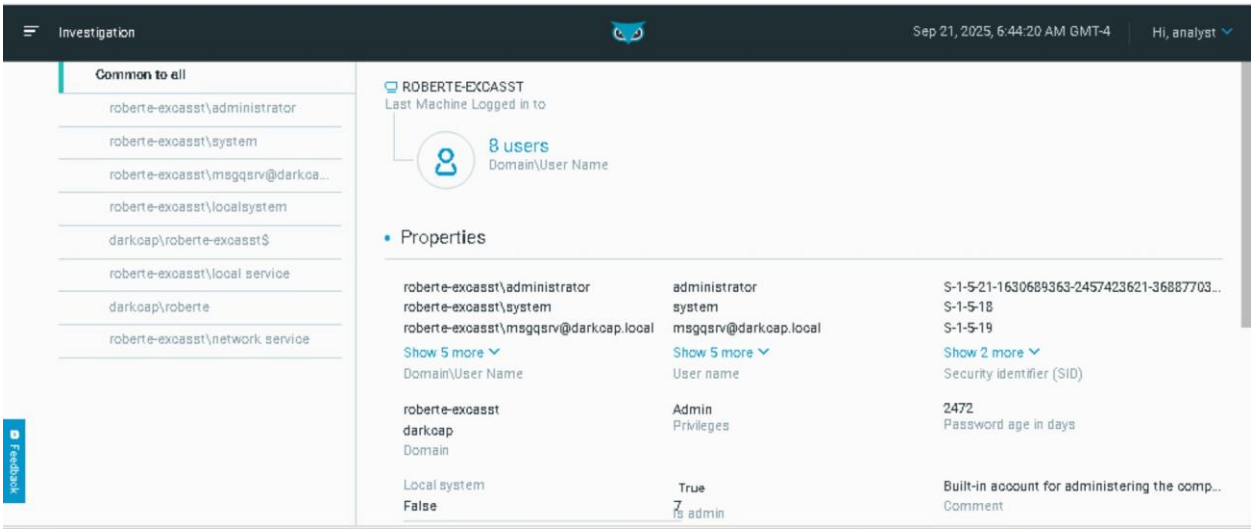
User domain\Username: cyberdomain\noa.pinkas

Privileges: User

Processes: 439 processes and 4 Suspicious processes

Detected activity: Malware (powershe.exe)

5.2 ROBERTE-EXCASSST SYSTEM



Machine name: ROBERTE-EXCASST

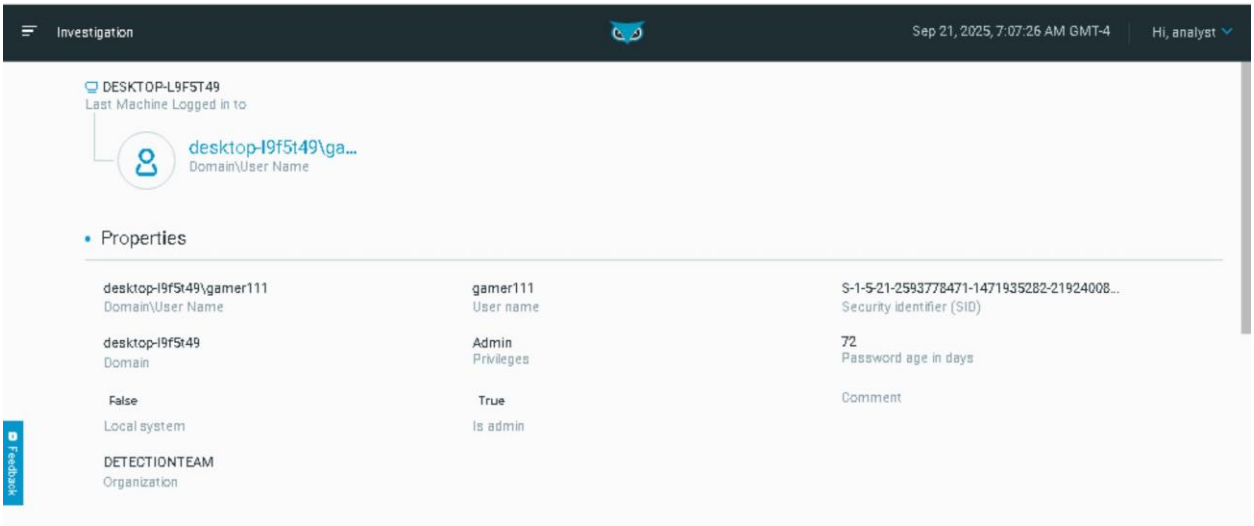
Organisation: CRTRAINING

Domain\Username: roberte-excasst\administrator, roberte-excasst\system, roberte-excasst\ msgqsrv@darkcap.local, roberte-excasst\localsystem, roberte-excasst\localservice, roberte-excasst\network service, darkcap\roberte-excasst and darkcap\roberte.

Privileges: Admin

Processes: 738 processes

5.3 DESKTOP-L9F5T49



Machine name: DESKTOP-L9F5T49

Organisation: DETECTION TEAM

Domain\Username: desktop-l9f5t49\gamer111

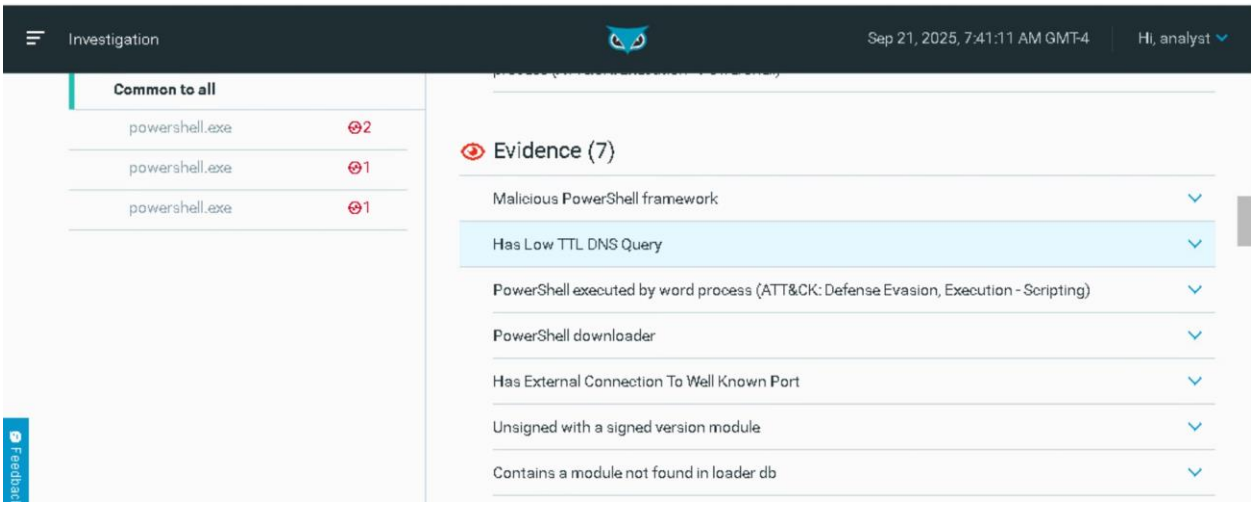
Privileges: Admin

Processes: 7 processes and 2 suspicious processes

Detected activity: Malware (shinobot.exe)

6. Find evidence points details of any 2 PowerShell based attack.

6.1 Evidence of PowerShell attack (1)



Each item listed under Evidence points to suspicious or malicious behavior associated with powershell.

1. **Malicious powershell framework:** Suggest use of a known offensive framework like Empire, Powersploit, or Nishang. These are often used for post- exploitation.

2. **Has Low TTL DNS Query**: Indicates potential DNS tunneling or command and Control(C2) communication. Low TTL values are often used to avoid caching and maintain real-time control.

3. **PowerShell executed by word process
 (ATT&CK DEFENSE Evasion, Execution scripting):** A word document triggering PowerShell is a classic sign of macro-based malware or phishing. This maps to MITRE ATT&CK techniques for evasion and script-based execution.

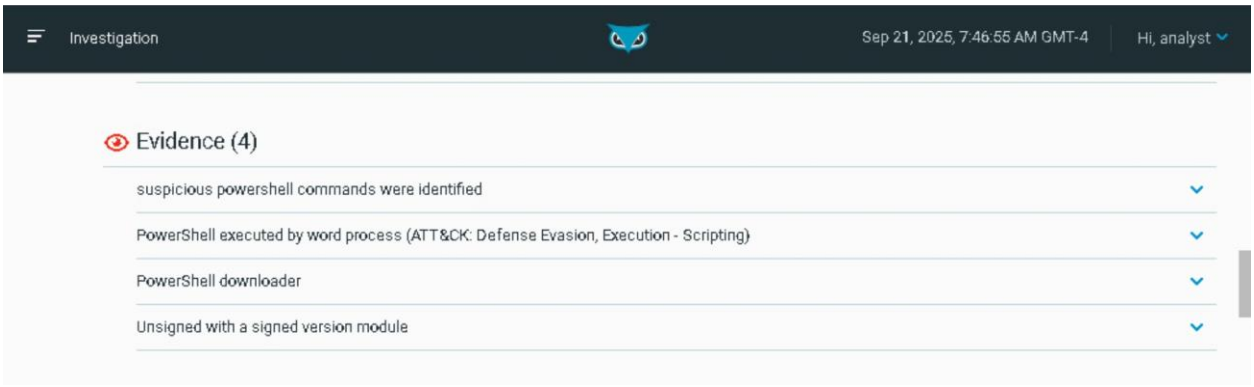
4. **PowerShell downloader:** A script used to fetch and execute payloads from external sources often the first stage in malware delivery.

5. **Has External Connection to Well Known Port:** Indicates out band traffic to a known port (e.g., 443 for HTTPS), possibly for C2 for data exfiltration.

6. **Unsigned with a signed version module:** Suggests tampering or replacement of legitimate modules with unsigned ones used to bypass trust mechanisms.

7. **Contains a module not found in loader bin:** Implies the presence of unauthorised or injected modules, possibly used for stealth or persistence.

6.2 Evidence of PowerShell attack (2)



1. **Suspicious PowerShell commands were identified:** Indicates detection of potentially malicious or obfuscated PowerShell commands. These may include encoded payloads, privilege escalation attempts, or lateral movements scripts.

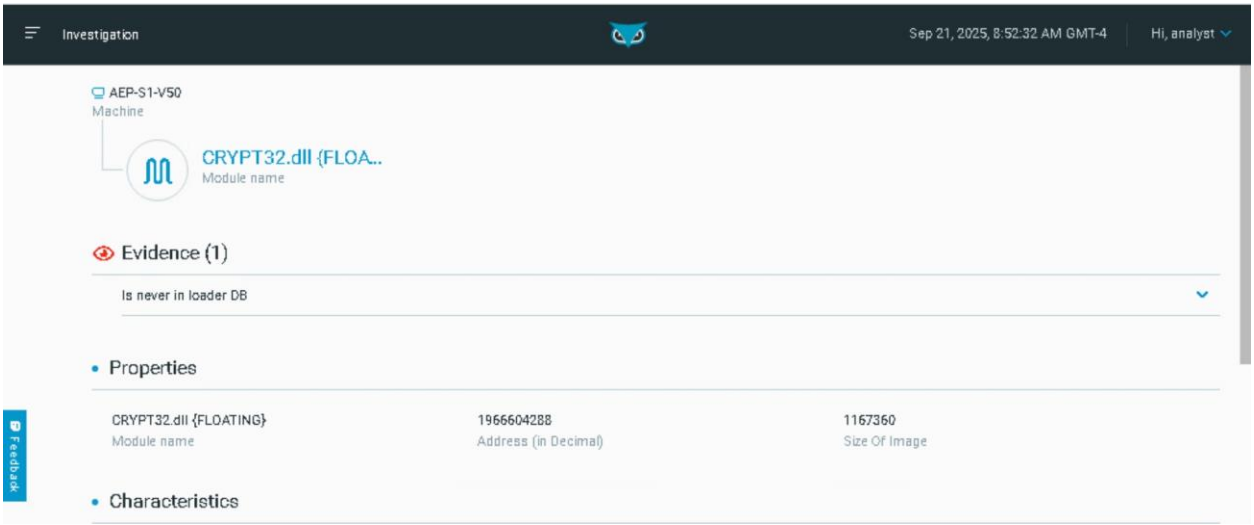
2. **PowerShell executed by word process (ATT&CK Defense Evasion, Execution- scripting):** A non- standard process (wvcd) initiated PowerShell, suggesting process hollowing, masquerading, or indirect execution.

3. **PowerShell Downloader:** Script used PowerShell to fetch remote content typically malware or additional payloads. This is a common initial access or staging technique.

4. **unsigned with a Signed Version Module:** Indicates module swapping or DL

7. Find 3 suspicious DLL process details of any 2-ransomware alert.

7.1 CRYPT32.dll {FLOATING}



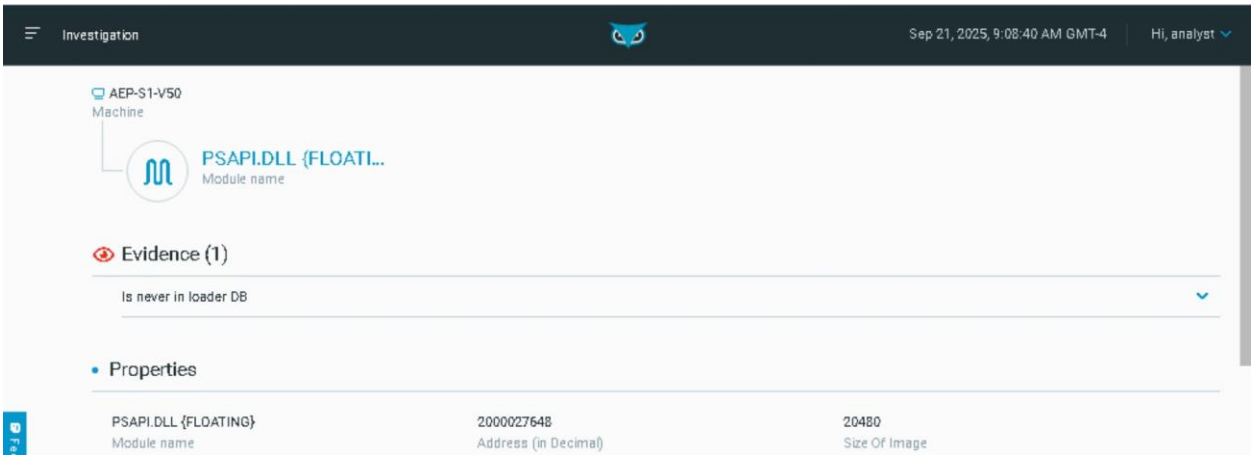
Module name: CRYPT32.dll {FLOATING}

Status: Floating (not loaded from standard location or not verified against known baseline.)

Evidence: This version of CRYPT32.DLL has never been seen before in the loader database, Suggests the module may be unauthorised or injected manually and obfuscated attack.

Date and Time: September 21, 2015, 8:53:21 AM GMT +4

7.2 PSAPI.DLL{FLOATING}



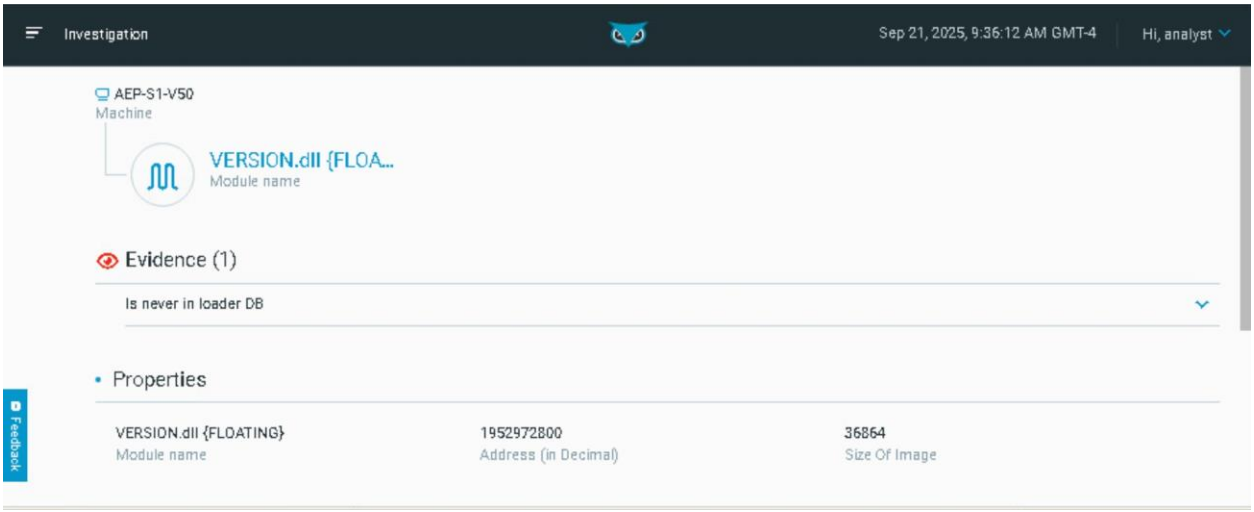
Module name: PSAPI.DLL {FLOATING}

Status: Floating {status may imply its loaded in memory without proper registration or linkage}

Evidence: Not found in loader database which may indicate non-standard DLL injection or obfuscated malicious payload.

Date and Time: September 21, 2015, 08:08:40 AM (GMT +4)

7.3 VERSION.dll {FLOATING}



Module name: VERSION.dll {FLOATING}

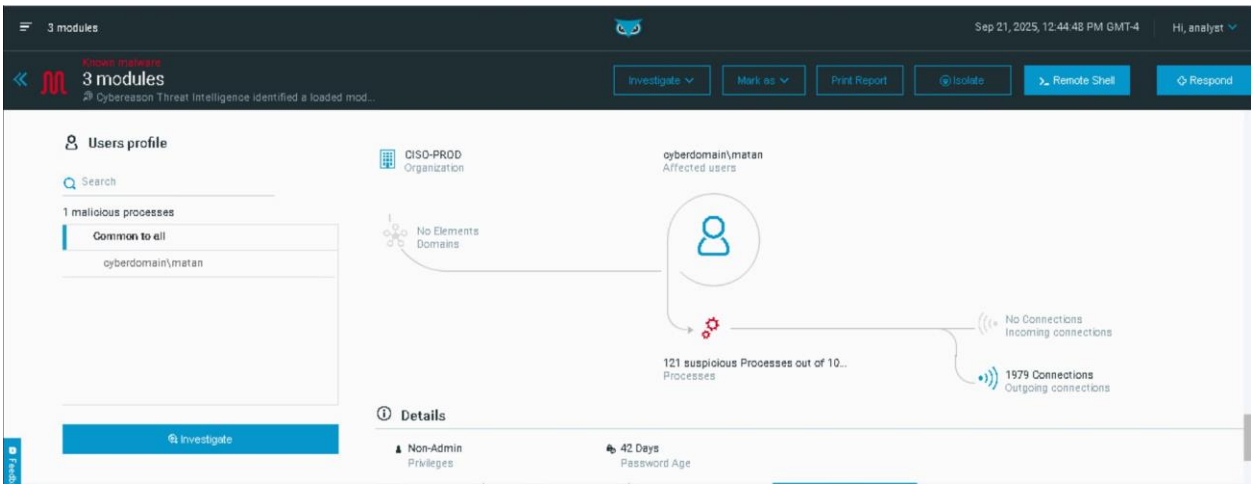
Status: Floating (This DLL is not loaded through standard mechanisms)

Evidence: This module is not listed in the loader database, it may have been injected manually (e.g., via reflective DLL injection or process hollowing).

Date and Time: May 29, 2018, at 4:06:56 AM GMT-4

8. Find the 2 effected users name of phishing attack/any malware attack.

8.1 Affected user of malware attack

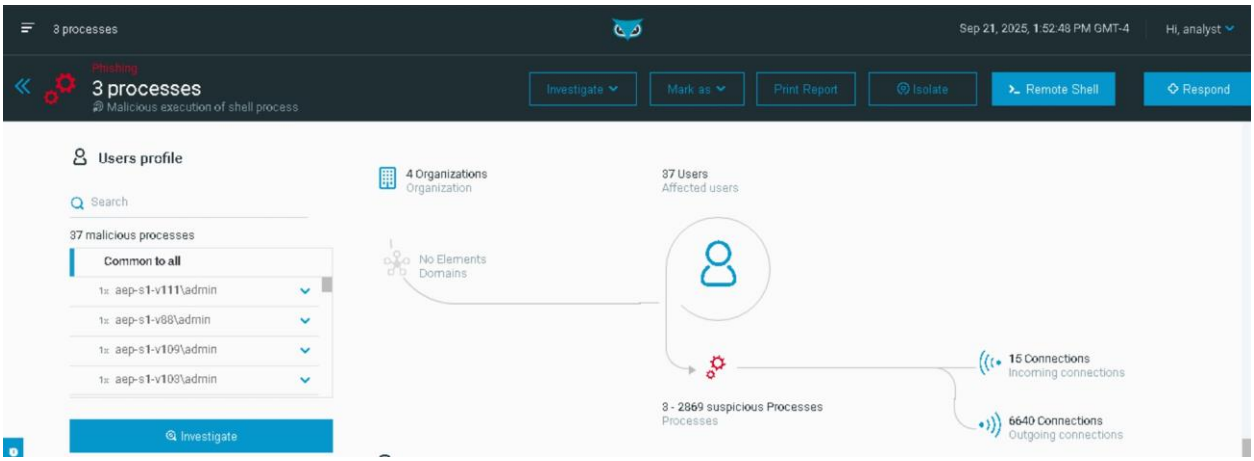


Username: matan (cyberdomain\matan)

Processes: powershell.exe, excel.exe and cmd.exe

Activity: Malware attack

8.2 Affected user of phishing attack.

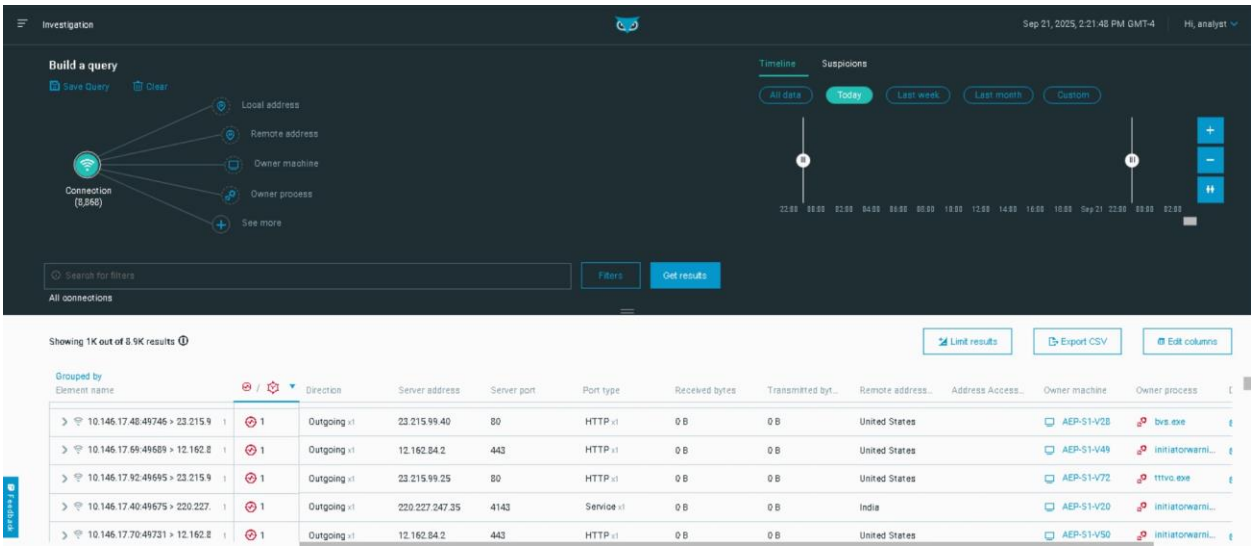


Username: admin(aep-s1-v111\admin)

Processes: cmd.exe and powershell.exe

Activity: Phishing attack

9. Find out 5 outgoing connections IP address based on any 2-malware alert.



1. Connection – 10.146.17.48:49746 > 23.215.99.40:80

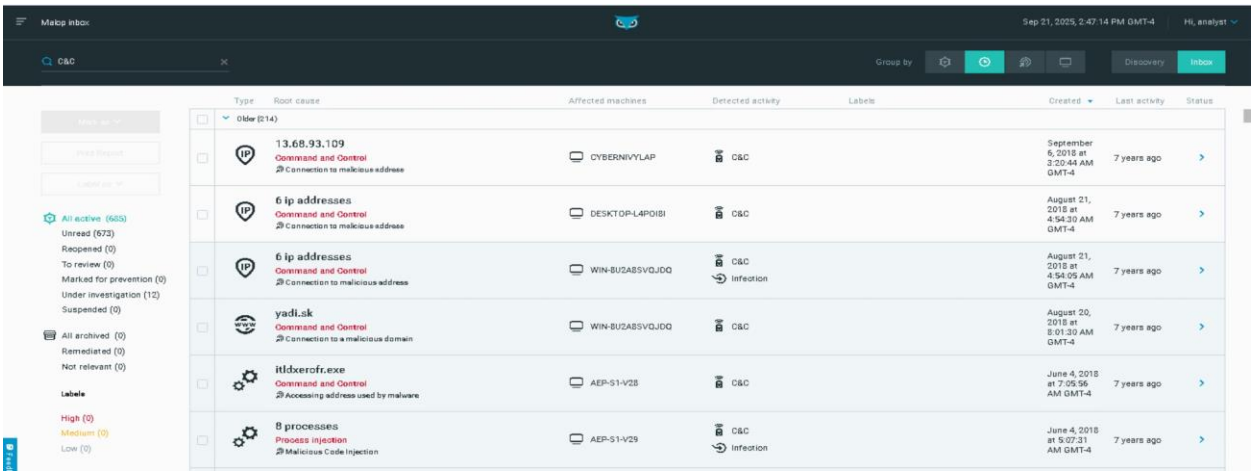
2. Connection - 10.146.17.69:49689 > 12.162.84.2:443

3. Connection – 10.146.17.92:49695 > 23.215.99.25:80

4. Connection – 10.146.17.40:49675 > 220.227.247.35:4143

5. Connection – 10.146.17.70:49731 > 12.162.84.2:443

10. Create a full list of number of all alerts in C&C category.



1. 13.68.93.109 - Connection to malicious domain.

2. itldxerofr.exe - Accessing address used by malware.

3. 204.95.99.109 - Connection to malicious address and domain.

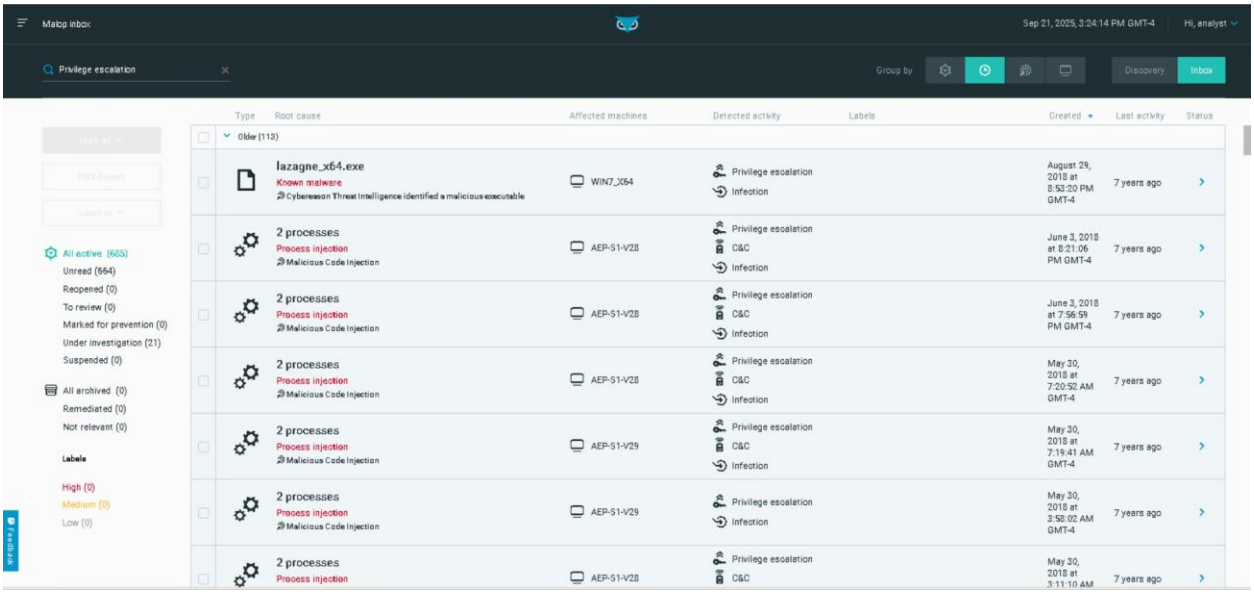
4. tttvc.exe - Accessing address used by malware.

5. 67.176.238.209 - connected to malicious address and has been identified as C&C activity.

6. bvs.exe - Accessing address used by malware.

7. xuzf1ja2bm.exe - It has an unknown reputation and connecting to the address that is used by malware. (ATT&CK: Initial Access, Command and Control).

11. Create a list of number of alerts in privilege access stage category.



1. lazagane_x64.exe - The process has a module that was identified malicious software address.

2. server.exe - The process has identified as malicious executable. (ATT&CK; privilege escalation).

3.default.exe - It exhibited ransomware behavior, and depending upon settings, may have been suspended to prevent encryption. (ATT&CK; privilege escalation).

4. explorer.exe - Process has loaded a meterpreter agent.