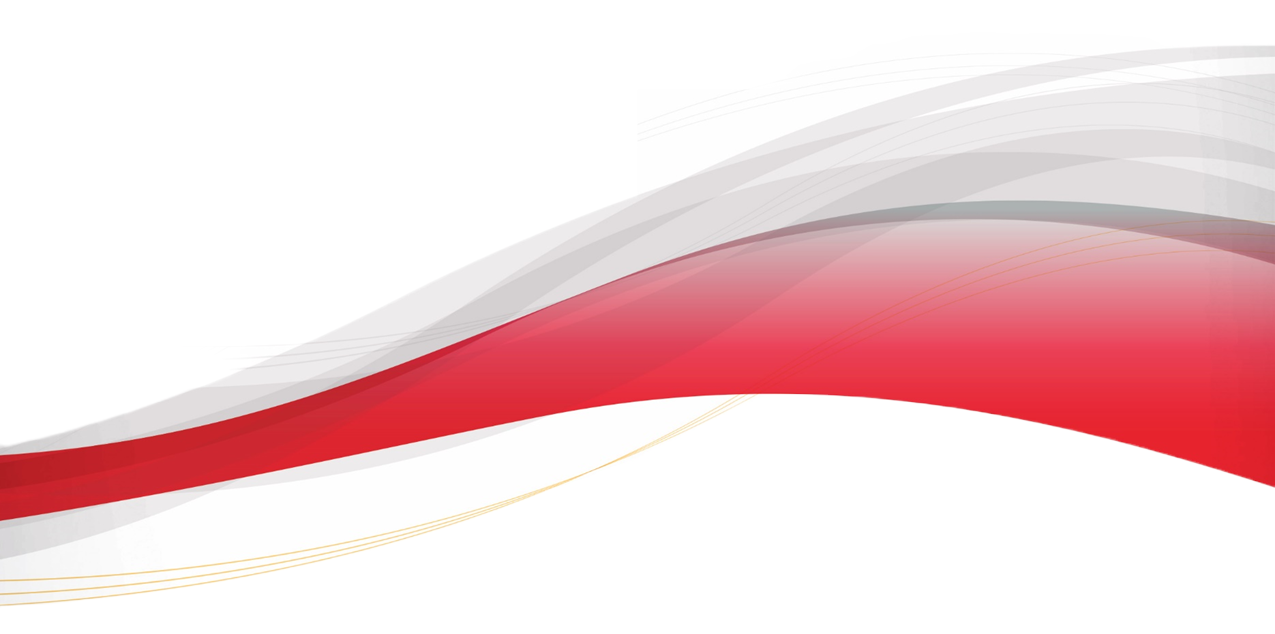
Trend Micro Health Check  
Endpoint Security for



Review of EVENTUS Apex One On-Premises Implementation



Document Version:   
  
Version Release Date: Invalid date  
  
Prepared By:   
  
Approved By:   
  
Trend Micro India Pvt Ltd

**Document Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Version** |  | **Version Date** | Invalid date |
| **Title** | Review of EVENTUS Apex One On-Premises Implementation | | |

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Ver. Date** | **Revised by** | **Description** |
| 1.0 |  |  | Initial Draft |
| 1.1 |  |  | Final Report |

Content

# 1 Introduction

All best practice statements in this document are formed from base principles with the products, and many years of experience within Trend Micro, however all recommendations herein should be validated as being acceptable to meet business, regulation, and security requirements of EVENTUS to have a successful outcome.

This document provides best practice recommendations in comparison to the published Best Practice product guides from Trend Micro to the configuration at EVENTUS. Trend Micro recommends that EVENTUS evaluate each recommended setting to verify it is suitable within their environment.

This document follows an established "Red, Amber, Green" methodology for highlighting gaps in best practice.

|  |  |  |
| --- | --- | --- |
| **Status** | **Description** | **Key** |
| Good | Meets Trend Micro Minimum Requirements / Best Practice recommendations |  |
| Concern | May have a security and/or operational impact on the organization |  |
| Critical | Likely to have a high security and/or operational impact on the organization |  |
| Info | Tips and Recommendations |  |

**Note:** Status items are in context to the configuration of the Trend Micro product only and do not consider any other external mitigating feature that EVENTUS may have in place and context as if EVENTUS did not have any mitigation of any description.

Configuration is subject to the requirements of each organization. Trend Micro acknowledges that deviations from published Best Practices are within the scope of EVENTUS by their specific environment and are subject to internal security requirements. Also, Trend Micro's Best Practice recommendation is subject to change at any time.

## 1.1 Health Check Attendees

|  |  |
| --- | --- |
| Location | Remotely |
| Customer Attendance |  |
| Trend Micro Attendance |  |

# 2 Executive Summary

Trend Micro performed a Health Check on Invalid date for EVENTUS to ensure Trend Micro Product(s) are configured as per best practice and provide gap analysis feedback.

This high-level summary provides an overview of the status of your Apex One and Apex Central deployment. Detailed instructions and references can be found within the individual sections further down in the report.

(input) Agents have outdated Program versions out of (input) agents.

(input) endpoints are required to restart for the update.

(input) endpoints (input-name-of-endpoints) are required to restart for cleanup.

(input) agents (input) are using the Windows servers platform.

(input) agents are installed on the Windows 7 (Legacy OS) platform.

(input) endpoints are without policy.

Active Directory Sync is configured in Apex Central.

Reports are configured in Apex Central.

Syslog is configured in Apex Central.

We have captured 30 Days of logs on 4th Mar 2024 detections are below:

690 Virus/Malware Detected

113 Spyware/Grayware Detected

3346 Web Reputation Detected

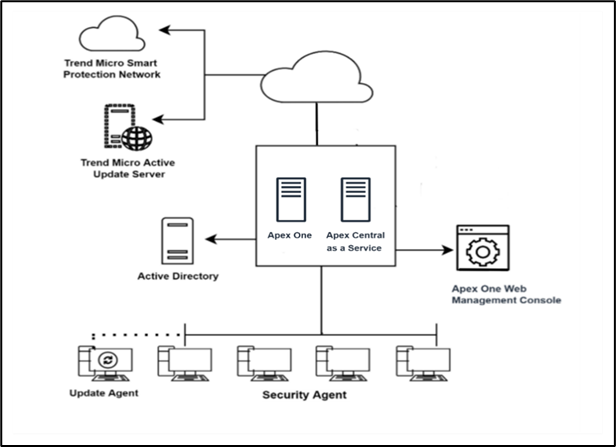
279557 Intrusion Prevention Detected

72 Device Control Detected

50 C&C Callback Detected

104 Behaviour Monitoring Detected

# 3 Product Architecture



# 4 Apex One & Apex Central

Trend Micro Apex One protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. Apex One Server consists of Apex One agent program that resides at the endpoint OS and a server OS. The Apex One Security agent guards the endpoint and reports its security status to the server. Through the web-based management console, the Apex One server makes it easy to set coordinated security policies and deploy updates to every agent.

Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Apex Central web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

## 4.1 Apex One Configuration Overview

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Trend Recommended | Deployed | Status |
| **Apex one Administration Configuration Health-Overview** | |  |  |
| System Health-Overview | Minimum Requirements |  |  |
| Memory | 8 GB (This would depend on the number of agents customer deployed. Please refer sizing guide) | 8 |  |
| Operating System | Supported OS | Windows Server 2019 |  |
| CPU | 0 cores | 0 cores |  |
| Hostname / IP |  | 00.00.00.00 |  |
| Apex One Build Version | 1234 | 1234 |  |
| Agent Management tree | AD / Custom / NetBIOS grouping | AD |  |
| License | Within Term | Invalid date |  |
| Deployed Agents | Total Purchased Licensed Seat is 0 | 0 |  |
| Certified Safe Software Service | Enable Certified Safe Software Service | Enabled |  |
| Patterns Update Status | Up to Date | Up to Date- 0 Outdated- 0 |  |
| Apex Central Integration | Register Apex One to Apex Central | Yes |  |
| Global Agents Settings | Enable Clean / Delete Infected Files within Compressed Files | Yes |  |
| Enable resume schedule scan options under global agent settings | Resume an Interrupted Scheduled Scan- Enabled and Resume a missed Scheduled Scan at the same time the next day- Enabled |  |
| Enable Smart Protection Service Proxy | Enabled |  |
| Agent scheduled updates | Enabled | Enabled- Daily |  |
| Smart Protection Server | Integrated/Standalone SPS Server/Global SPS | Integrated SPS |  |
| Notification | Enabled | Enabled |  |

## 4.2 Policy Overview: NAME-OF-POLICY Policy

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Trend Recommended | Deployed | Status |
| **Policy Configuration - Overview NAME-OF-POLICY Policy** | | | |
| Agent Scan Mode | Smart scan | Smart Scan |  |
| Manual Scan - Policy | Files to Scan > All Scannable files | All Scannable files |  |
| Scan Hidden Folders | Enabled |  |
| Select - Scan compressed files. > Maximum layers: 2 | Select- Scan compressed files. > Maximum layers: 2 |  |
| Select - Scan OLE objects. > Maximum layers: 3 | Select- Scan OLE objects. > Maximum layers: 3 |  |
| Enable - Detect exploit code in the OLE file | Enabled Detect exploit code in the OLE files. |  |
| Virus/Malware Scan Settings Only > Scan boot area | Enabled - Scan boot area |  |
| CPU Usage > Medium | Medium |  |
| Manual Scan - Actions | Virus/Malware > Use a specific action for each virus/malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine | | Other Malware: Clean & Quarantine | | Used specific action for each Virus/Malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine & Quarantine | | Select - Other Malware: Clean & Quarantine | |  |
| Select - Back up files before cleaning. | Enabled - Back up files before cleaning. |  |
| Enable - Damage Cleanup Services with Advanced Clean up | Enabled - Damage Clean up Services with Advanced clean-up |  |
| Enable - Run cleanup when Probable virus/malware is detected | Enabled - Run cleanup when probable virus/malware is detected |  |
| Enable - Spyware/Grayware > Clean: Apex One terminates Processes. | Enabled - Spyware/Grayware > Clean: Apex One terminates processes. |  |
| Real-Time Scan Policy Settings | Enable - Virus/Malware Scan | Enabled |  |
| Enable - Spyware/Grayware scan | Enabled - Spyware/Grayware scan |  |
| User Activity on Files > Scan files being created/modified and retrieved | User Activity on Files > Scan files being created/modified and retrieved |  |
| Files to Scan > All Scannable files | All Scannable files |  |
| Enable - Scan the boot sector of the USB storage device after plugging it in. | Enabled - Scan the boot sector of the USB storage device after plugging it in. |  |
| Enable - Scan all files in a removable storage device after plugging in. | Enabled - Scan all files in a removable storage device after plugging in. |  |
| Enable - Quarantine malware variants detected in memory. | Enabled - Quarantine malware variants detected in memory. |  |
| Select - Scan compressed files. > Maximum layers: 2 | Selected - Scan compressed files. > Maximum layers: 2 |  |
| Select - Scan OLE objects. > Maximum layers: 3 | Selected - Scan OLE objects. > Maximum layers: 3 |  |
| Enable - Detect exploit code in the OLE files. | Enabled - Detect exploit code in the OLE files. |  |
| Enable - CVE exploit scanning | Enabled - CVE exploits scanning |  |
| Real-Time Scan-Action Settings | Virus/Malware > Use a specific action for each virus/malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine | | Other Malware: Clean & Quarantine | | Used specific action for each Virus/Malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine & Quarantine | | Select - Other Malware: Clean & Quarantine | |  |
| Enable - Back up files before cleaning. | Enabled - Back up files before cleaning. |  |
| Enable - Run cleanup when probable virus/malware is detected | Enabled - Run cleanup when probable virus/malware is detected. |  |
| Enable - Spyware/Grayware > Clean: Apex One terminates processes. | Enabled - Spyware/Grayware > Clean: Apex One terminates processes. |  |
| Schedule Scan Policy Settings | Enable - Virus/Malware Scan | Enabled - Virus/Malware Scan |  |
| Enable - Spyware/Grayware scan | Enabled - Spyware/Grayware scan |  |
| Configure Schedule Scan to run at least once a week. | Weekly Every Monday - Start time: 00:00 |  |
| Files to Scan > All Scannable files | All Scannable files |  |
| Select - Scan compressed files. > Maximum layers: 2 | Selected - Scan compressed files. > Maximum layers: 2 |  |
| Selected - Scan compressed files. > Maximum layers:3 | Selected - Scan OLE objects. > Maximum layers: 3 |  |
| Enable - Detect exploit code in the OLE files. | Enabled - Detect exploit code in the OLE files. |  |
| Virus/Malware Scan Settings Only > Scan boot area | Enabled Scan boot area |  |
| CPU Usage > Medium | Medium |  |
| Schedule Scan-Action Settings | Virus/Malware > Use a specific action for each virus/malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine | | Other Malware: Clean & Quarantine | | Used specific action for each Virus/Malware type:   |  | | --- | | Select - Joke: Quarantine | | Select - Trojans: Quarantine | | Select - Virus: Clean & Quarantine | | Select - Test Virus: Quarantine | | Select - Packer: Quarantine | | Select - Probable Malware: Quarantine & Quarantine | | Select - Other Malware: Clean & Quarantine | |  |
| Select - Back up files before cleaning. | Enabled - Back up files before cleaning. |  |
| Enable - Damage Cleanup Services with Advanced Clean up | Enabled - Damage Clean up Services with Advanced clean-up. |  |
| Enable - Run cleanup when probable virus/malware is detected | Enabled - Run cleanup when probable virus/malware is detected. |  |
| Enable - Spyware/Grayware > Clean: Apex One terminates processes. | Enabled - Spyware/Grayware > Clean: Apex One terminates processes. |  |
| Behavior Monitoring | Enable Malware Behavior Blocking Known and potential threats | Enabled |  |
| Ransomware Protection Protect documents against unauthorized encryption or modification | Enabled |  |
| Protect documents against unauthorized encryption or modification -> Automatically backup and restore files changed by suspicious programs | Enabled |  |
| Enable program inspection to detect and block compromised executable files | Enabled |  |
| Anti-exploit Protection Terminate programs that. exhibit abnormal Behavior. associated with exploit attacks | Enabled |  |
| Newly Encountered Programs Monitor newly encountered programs downloaded through web or email application channels -> Prompt User | Enabled |  |
| Exceptions (specify exception if any) | No exceptions added to the Approved Program list |  |
| Predictive Machine Learning | Enable | Enabled |  |
| Action  File: quarantine  Process: Terminate | Action Set  File: Quarantine  Process: Terminate |  |
| Exception (specify exception if any) | No Exceptions added |  |
| Suspicious Connection | Enable with Block option | Enabled with Block option |  |
| Web Reputation | Enable for Internal and External agents with Security Level Medium | Enabled with Security Level Medium |  |
| Vulnerability Protection | Enable | Enabled with Inline Mode |  |
| Device Control | Enable | Enabled |  |
| Application Control | Enable | Enabled |  |
| Firewall | Enable (Optional) | Enabled |  |
| Agent Self-Protection | Enable Self-Protection with a password. | Enabled |  |
| Additional Service | Configure respective services | Enabled Unauthorized Change Prevention Service for Windows desktops and Enabled Windows Server platforms with full mode.  Enabled Firewall Service for Windows desktops and Enabled for Windows Server platforms.  Enabled Suspicious Connection Service for Windows desktops and Enabled Windows Server platforms.  Enabled Data Protection Service for Windows desktops and Enabled Windows Server platforms.  Enabled Advanced Protection Service for Windows desktops and Enabled Windows Server platforms. |  |

## 4.3 Apex Central Configuration Overview

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Trend Recommended | Deployed | Status |
| **Configuration Health - Overview** | |  |  |
| License | Within Term | Invalid date |  |
| Version | Build | Build |  |
| Active Directory Sync | Configure | Configured |  |
| Log Retention | Configure | Configured |  |
| Reports | Configure | Scheduled |  |
| Event Notifications | Enable | Enabled |  |
| Syslog | Configure | Configured |  |
| Report Maintenance | Configure | Configured |  |
| Product Registration | Register all Trend Micro products with Apex Central | Apex One Server is Registered |  |

## 4.4 Identified Gaps and Recommendations

(input) Agents have outdated Program versions out of (input) agents keep all agent program versions updated. Minimum OS Version requirement for the latest Apex One SaaS agent version: <https://success.trendmicro.com/dcx/s/solution/000291904?language=en_US>

(input) endpoints are required to restart for the update. Apex One Agents may need to reboot for engine updates. Recommend restarting those endpoints.

(input) endpoints (input) are required to restart for cleanup.

(input) agents are installed on the Windows 7 (Legacy OS) platform, recommended to upgrade it to the latest OS. For the Windows 7 & 8.1 machines End-of-Support <https://success.trendmicro.com/dcx/s/solution/000291687?language=en_US&sfdcIFrameOrigin=null>

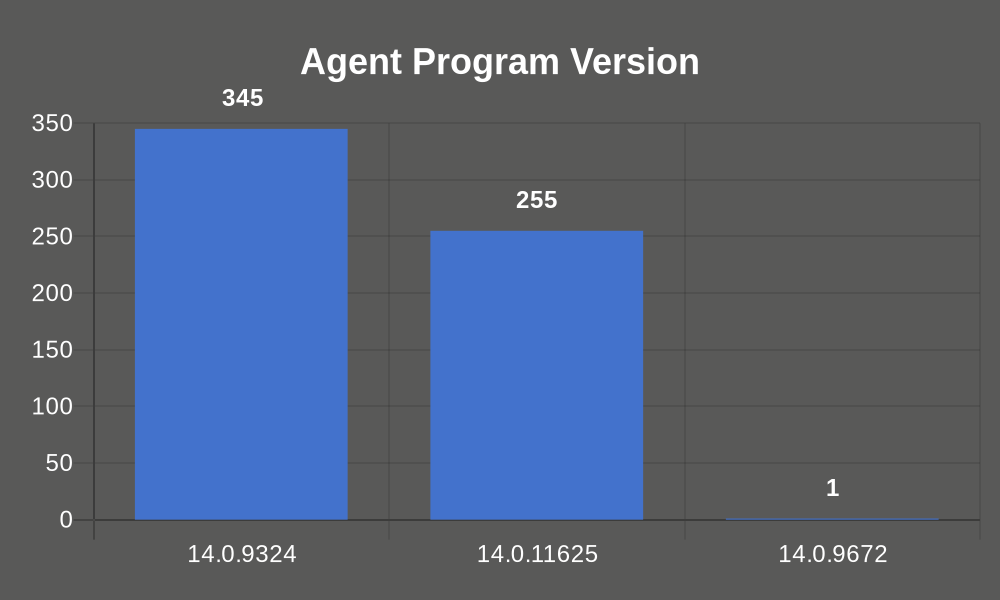
(input) agents (input) are using the Windows servers platform. recommended to use Cloud One Workload Security for better protection of the server.

(input) Endpoints are without policy, recommended to apply policy to all endpoints on priority for better protection.

# 5 Apex One Product Efficacy

## 5.1 Agent Distribution

|  |  |
| --- | --- |
| **Agent Platform** | **Count** |
| Windows 10 10.0.19045 | 366 |
| Windows 11 10.0.22621 | 161 |
| Windows 11 10.0.22000 | 34 |
| Windows Server 2019 10.0.17763 | 18 |
| Windows Server 2012 R2 6.3.9600 | 7 |
| Windows 10 10.0.19044 | 5 |
| Windows Server 2016 10.0.14393 | 5 |
| Windows 10 10.0.19042 | 2 |
| Windows 10 10.0.19043 | 1 |
| Windows 10 10.0.17134 | 1 |
| Windows Server 2012 6.2.9200 | 1 |
| **Total** | **601** |



14.0.9324 is the latest agent Program version recommended to upgrade all the older agents to the latest version.

(INPUT) endpoints (NAMES-OF-ENDPOINTS) are required restart for cleanup.

(INPUT) Agents have outdated Program versions out of (INPUT) agents.

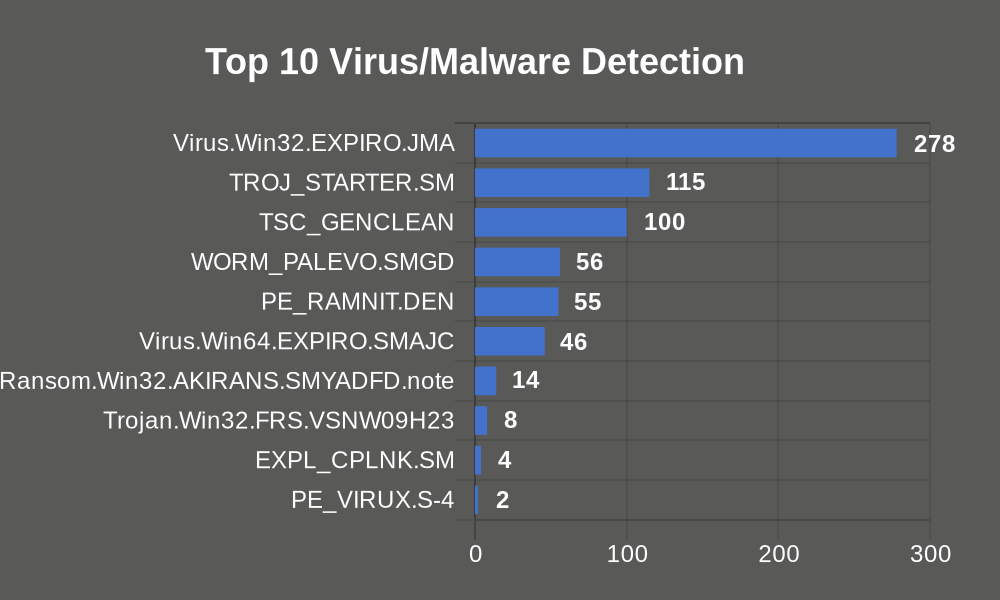
(INPUT) agents have outdated patterns older than 7 days out of (INPUT) agents.

(INPUT) agents (NAMES-OF-AGENTS) are using the Windows servers platform.

(INPUT) agents are installed on the Windows 7 (Legacy OS) platform.

## 5.2 Virus/Malware

We generated a Virus/Malware Event of the last 30 Days on 4th Mar 2024 from Apex Central/Apex One. There was a total of 690 detections.

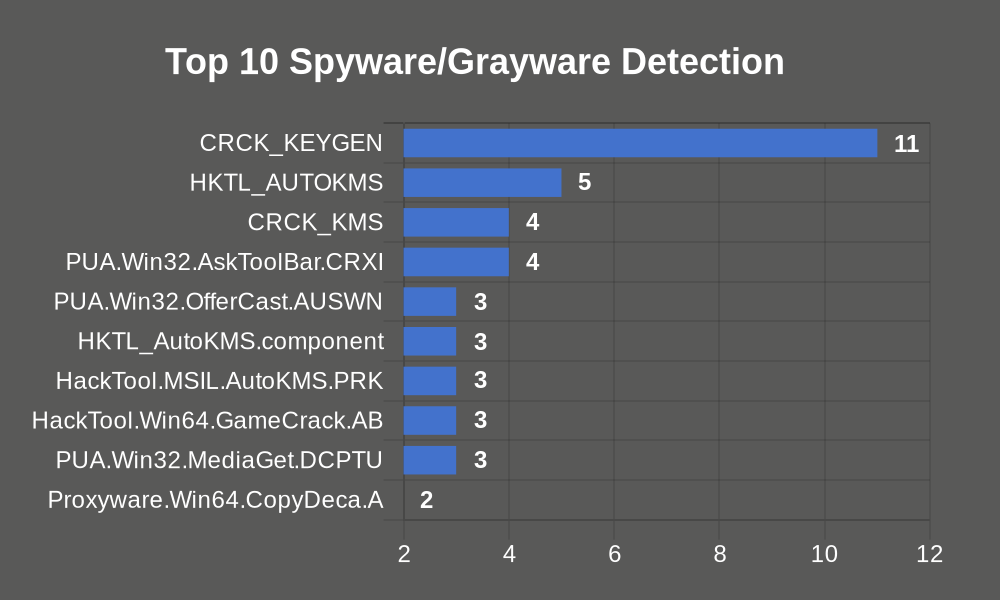


Virus.Win32.EXPIRO.JMA Virus/Malware was detected 278 times on the IDPCSBY080 endpoint, and the files were successfully No action by Apex One.

TROJ\_STARTER.SM Virus/Malware was detected 115 times on the IDPCSBY077 endpoint, and the files were successfully cleaned by Apex One.

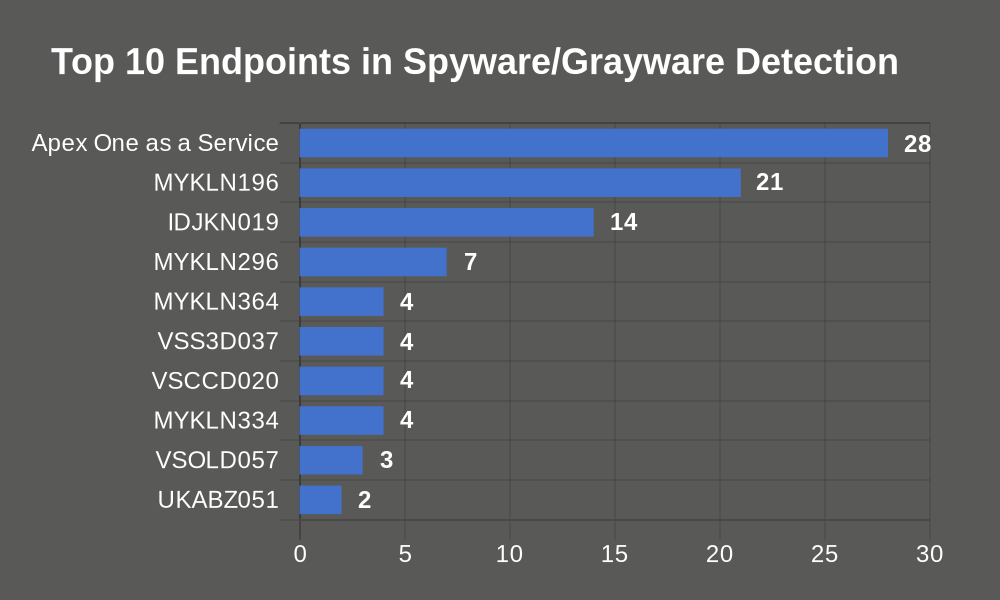
## 5.3 Spyware/ Grayware

We generated a Spyware/Grayware Event of the last 90 Days on 27th Sep 2023 from Apex Central/Apex One. There was a total of 113 detections.



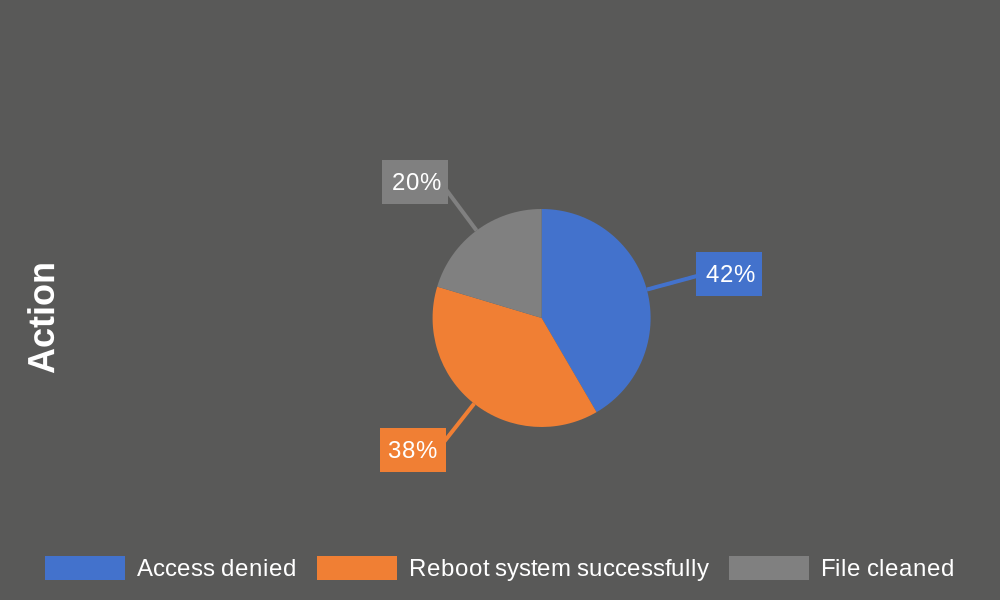
CRCK\_KEYGEN Spyware/Grayware was detected 11 times on MYKLN196, IDJKN019, VSS3D037, Apex One as a Service, and MYKLN334 endpoints, and the files were successfully Reboot system successfully and access denied by Apex One.

HKTL\_AUTOKMS Spyware/Grayware was detected 5 times on MYKLN196 and MYKLN296 endpoints, and the files were successfully Reboot system successfully and access denied by Apex One.



28 times Spyware/Grayware was detected on the Apex One as a Service endpoint, and the files were successfully cleaned, Reboot system successfully, and access denied by Apex One.

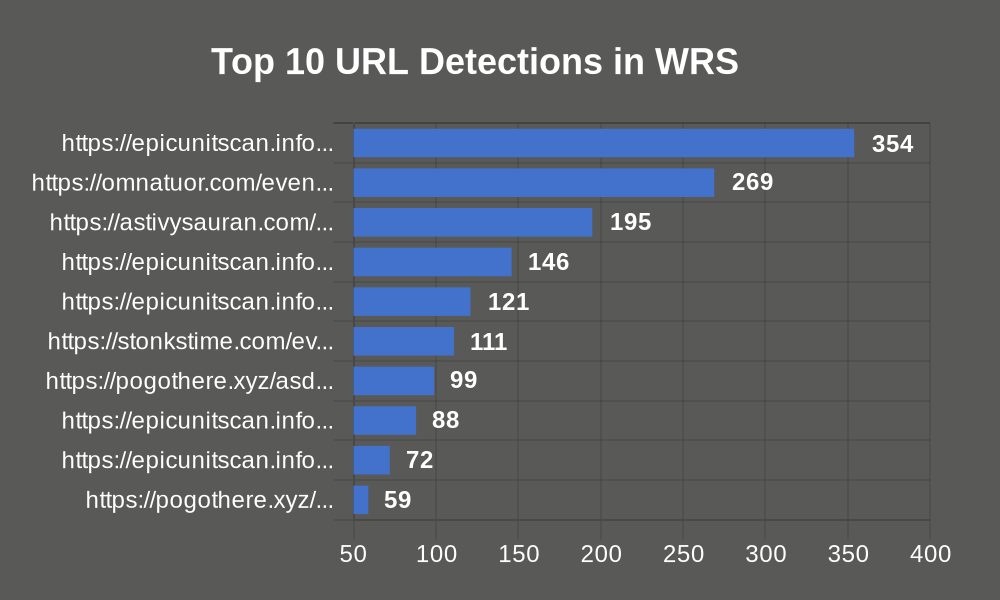
21 times Spyware/Grayware was detected on the MYKLN196 endpoint, and the files were successfully access denied and Reboot system successfully by Apex One.



Files were access denied, Reboot system successfully, and cleaned by Apex One.

## 5.4 Web Reputation

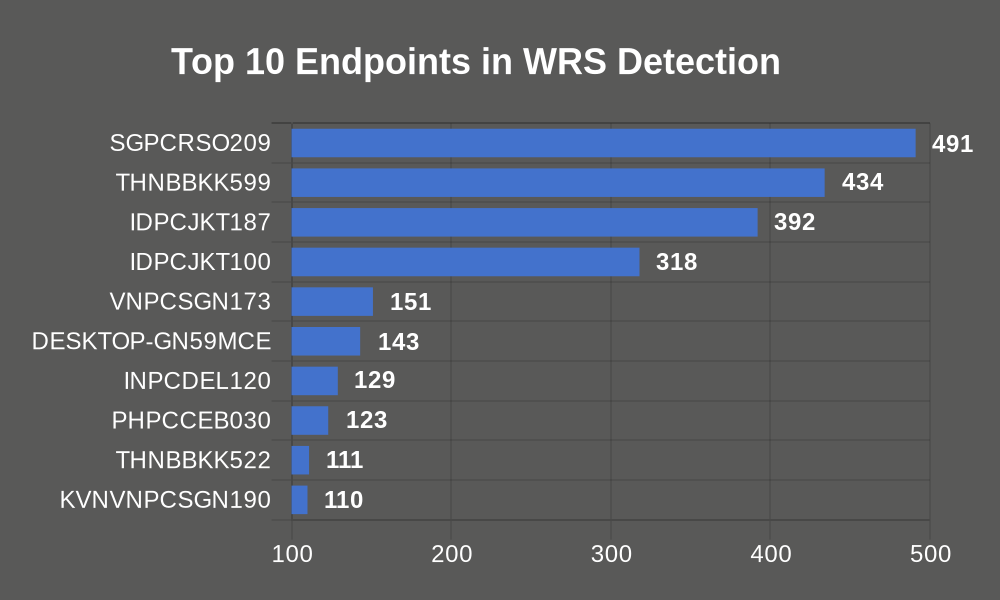
We generated a Web Reputation Detections Event of the last 30 Days on 4th Mar 2024 from Apex Central/Apex One. There was a total of 3346 detections.



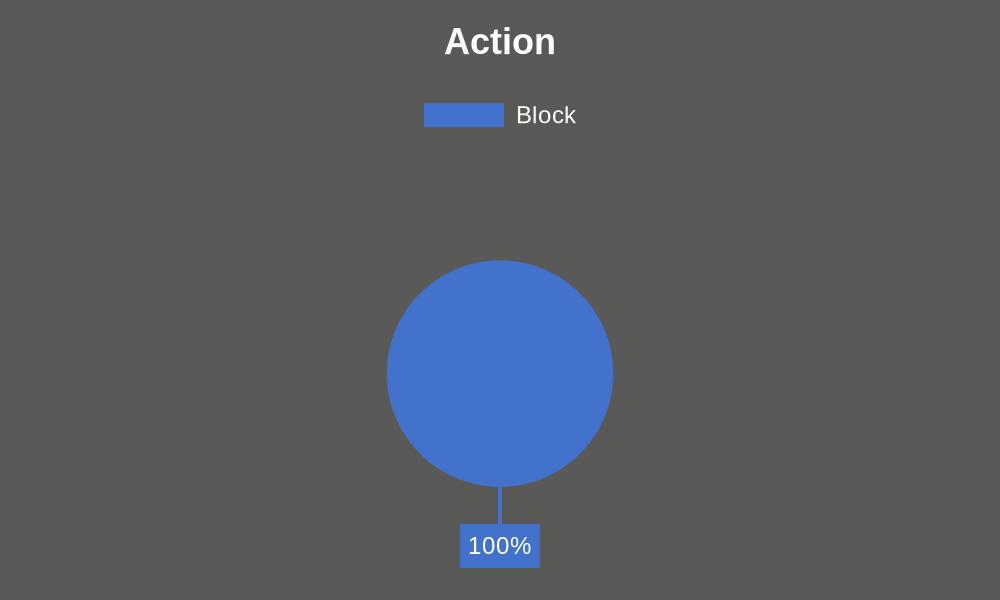
61 times HTTP sites are detected in WRS detection, and the files were successfully blocked by Apex One.. Check whether it's secure or not if it's secure then add it to the approved list otherwise block it.

https://epicunitscan.info/00service/update2/crx?os=win&arch=x64&os\_arch=x86\_64&nacl\_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=115.0.5790.110&lang=en-US&acceptformat=crx3,puff&x=id%3Dnckgahadagoaajjgafhacjanaoiihapd%26v%3D0.0.0.0%26installsource%3Dnotfromwebstore%26installedby%3Dinternal%26uc This site is detected 354 times on the SGPCRSO209 endpoint, and the files were successfully blocked by Apex One.

https://omnatuor.com/event This site is detected 269 times on the IDPCJKT187 endpoint, and the files were successfully blocked by Apex One.

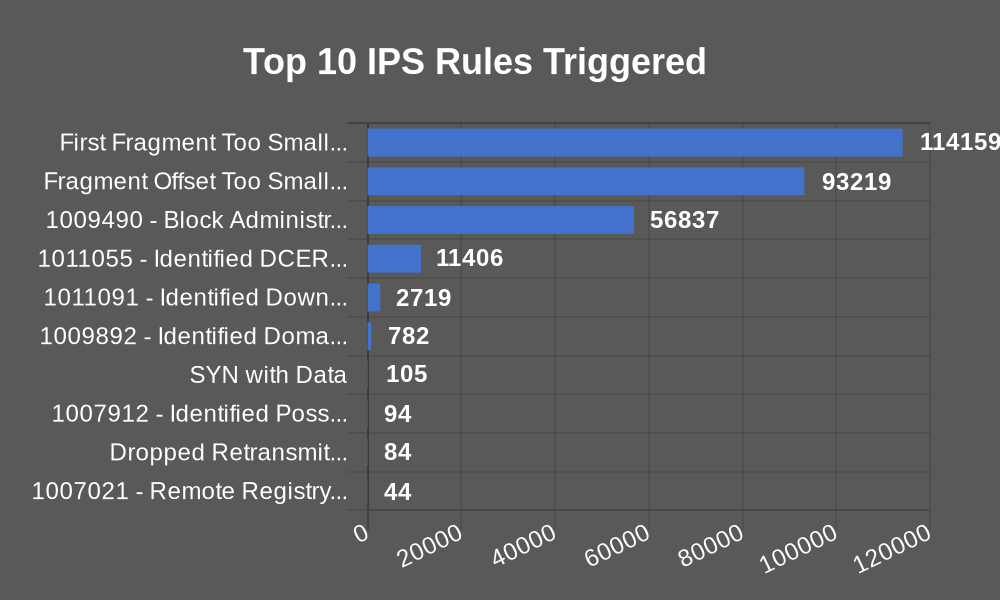


All the web violation events were successfully blocked by Apex One.



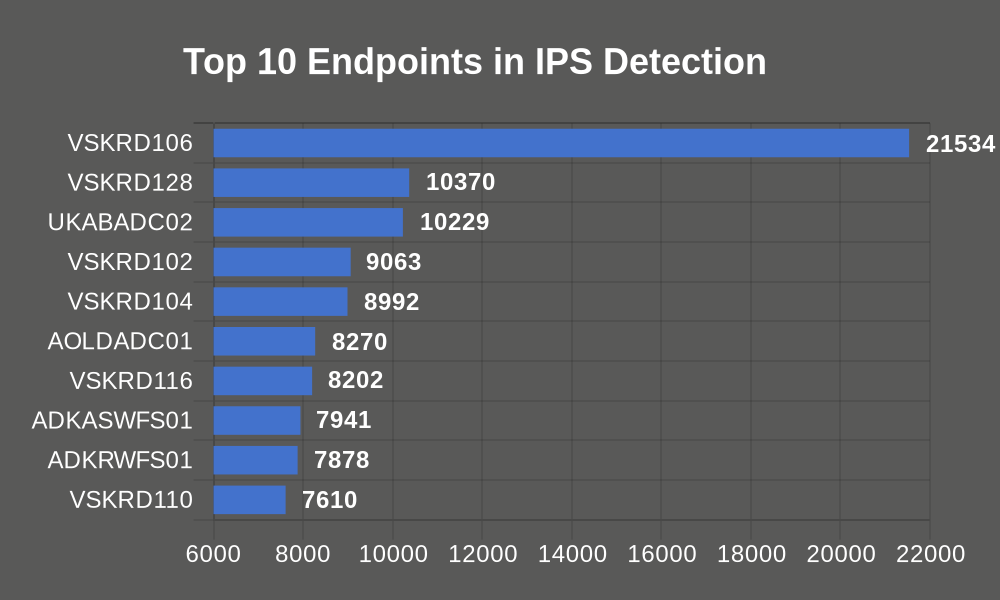
## 5.5 Intrusion Prevention

We generated an Intrusion Prevention Event of the last 90 Days on 27th Sep 2023 from Apex Central/Apex One. There was a total of 279557 detections.



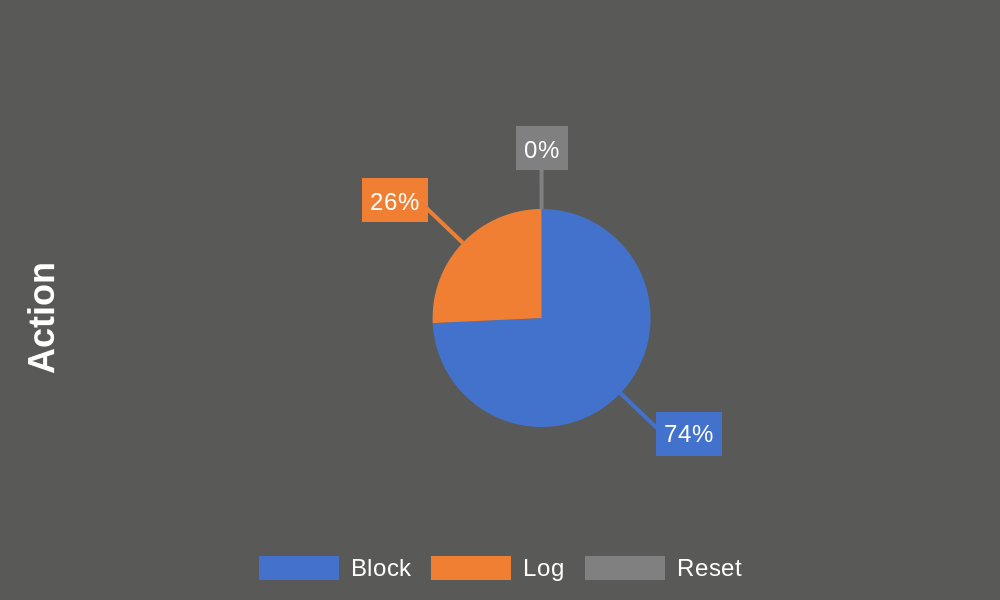
First Fragment Too Small triggered 114159 times with Critical severity, and it is in Prevent mode and the files were successfully blocked by Apex One.

Fragment Offset Too Small triggered 93219 times with Critical severity, and it is in Prevent mode and the files were successfully blocked by Apex One.



Intrusion Prevention was detected 21534 times on the VSKRD106 endpoint, and the files were successfully blocked and logged by Apex One.

Intrusion Prevention was detected 10370 times on the VSKRD128 endpoint, and the files were successfully blocked and logged by Apex One.

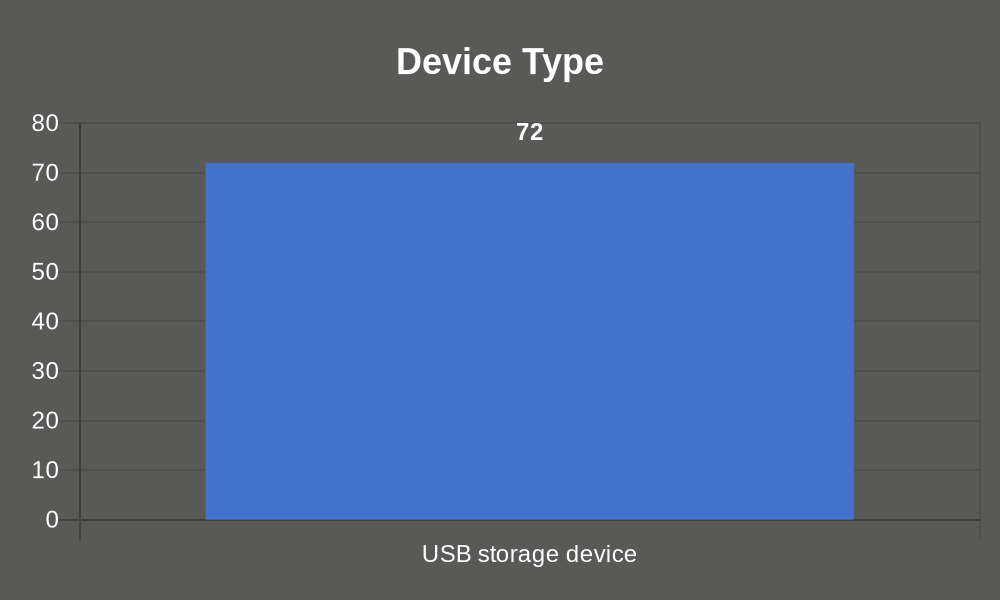


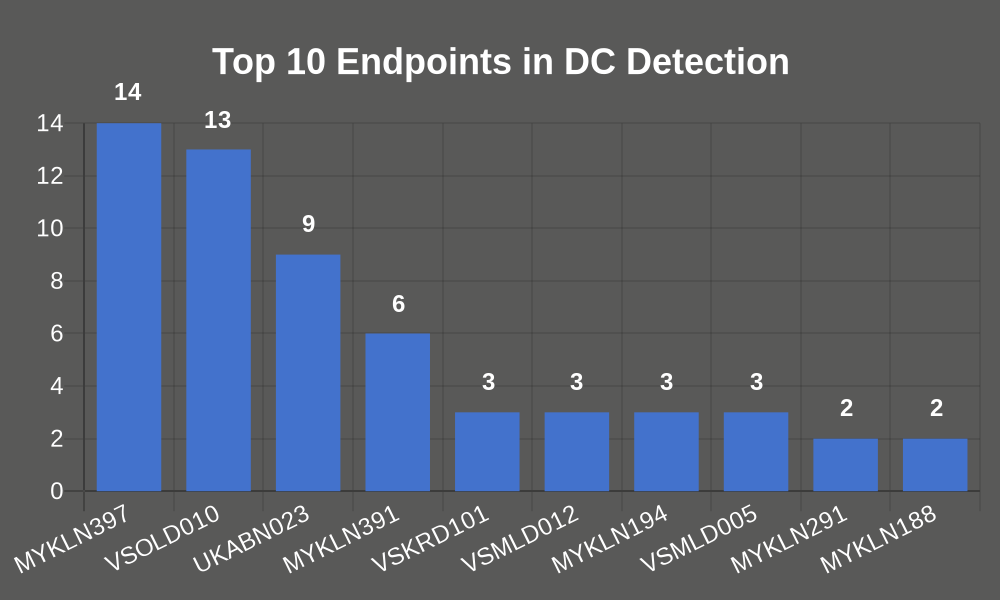
All the events that were triggered have been blocked, logged, and reset successfully.

|  |  |  |  |
| --- | --- | --- | --- |
| **IPS DETECTION & SEVERITY** | **ACTION** | | |
| **Block** | **Log** | **Reset** |
| **First Fragment Too Small** | **114159** |  |  |
| Critical |  |  |  |
| **1011055 - Identified DCERPC OpenPrinterEx Call Over SMB Protocol** |  | **11406** |  |
| Critical |  |  |  |
| **1009490 - Block Administrative Share - 1 (ATT&CK T1021.002)** |  | **56837** |  |
| Medium |  |  |  |
| **Fragment Offset Too Small** | **93219** |  |  |
| Critical |  |  |  |
| **1009892 - Identified Domain-Level Information Dumping Over DCERPC (ATT&CK T1003.006, T1018)** |  | **782** |  |
| Critical |  |  |  |
| **1011091 - Identified Download Of Executable File Over HTTP (ATT&CK T1105)** |  | **2719** |  |
| Low |  |  |  |
| **1011593 - Identified Executable File Upload On Network Share (ATT&CK T1570)** |  | **4** |  |
| Low |  |  |  |
| **1007021 - Remote Registry Access Through SMBv2 Protocol Detected (ATT&CK T1012)** |  | **44** |  |
| Low |  |  |  |
| **Dropped Retransmit** | **84** |  |  |
| Critical |  |  |  |
| **1007065 - Executable File Uploaded On Network Share (ATT&CK T1570)** |  |  | **15** |
| Low |  |  |  |
| **SYN with Data** | **105** |  |  |
| Critical |  |  |  |
| **Invalid Flags** | **27** |  |  |
| Critical |  |  |  |
| **1009478 - Identified Remote Service Creation Over DCE/RPC Protocol (ATT&CK T1543.003)** |  | **1** |  |
| Critical |  |  |  |
| **1007912 - Identified Possible Ransomware File Rename Activity Over Network Share - Client** |  | **94** |  |
| Critical |  |  |  |
| **1010164 - Identified Possible Ransomware File Extension Create Activity Over Network Share (ATT&CK T1486, T1080)** |  | **9** |  |
| Critical |  |  |  |
| **Invalid Traversal** |  |  | **8** |
| Critical |  |  |  |
| **Packet on Closed Connection** | **15** |  |  |
| Critical |  |  |  |
| **1010585 - Identified Possible Ransomware File Extension Create Activity Over Network Share - Client (ATT&CK T1486, T1080)** |  | **9** |  |
| Critical |  |  |  |
| **Invalid TCP Header Length** | **1** |  |  |
| Critical |  |  |  |
| **1007456 - DNS Malformed Response Detected** |  | **1** |  |
| Medium |  |  |  |
| **1009562 - Identified Remote Desktop Protocol (RDP) Brute Force Attempt (ATT&CK T1110)** |  | **1** |  |
| Critical |  |  |  |
| **1005448 - SMB Null Session Detected - 1** |  | **14** |  |
| High |  |  |  |
| **Insufficient Memory** |  | **1** | **2** |
| Critical |  |  |  |
| **Total** | **207610** | **71922** | **25** |

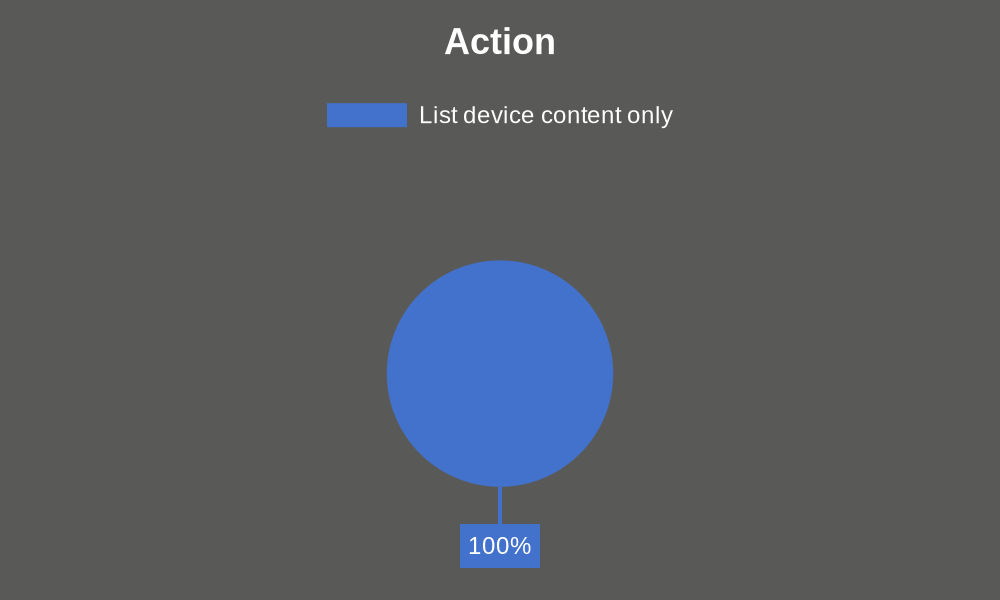
## 5.6 Device Control Detection

We generated a Device control Detection Event of the last 90 Days on 27th Sep 2023 from Apex Central/Apex One. There was a total of 72 detections.



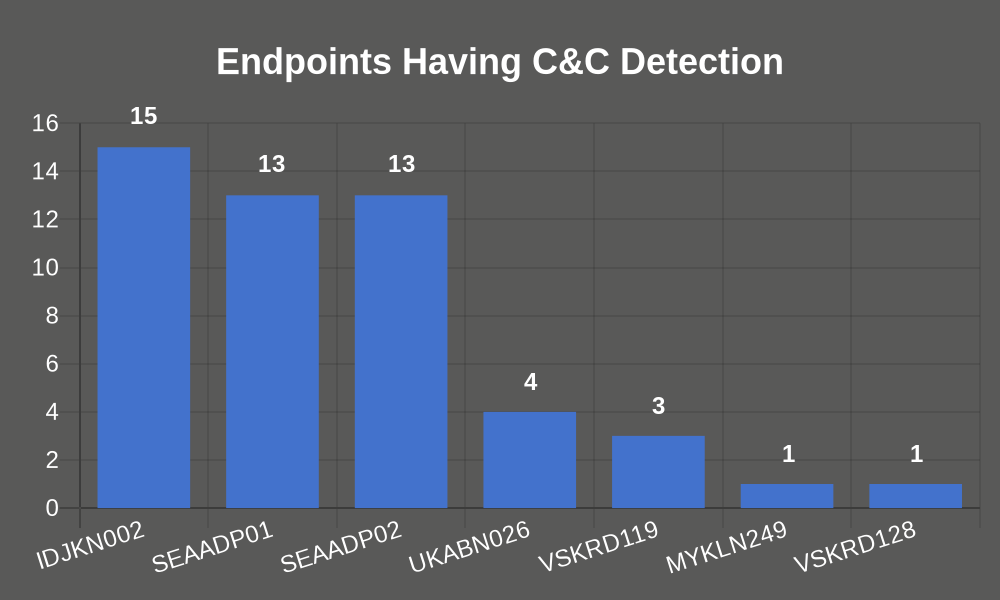


MYKLN397 was the endpoint that was triggered the most having Device control detection and was list device content only successfully.



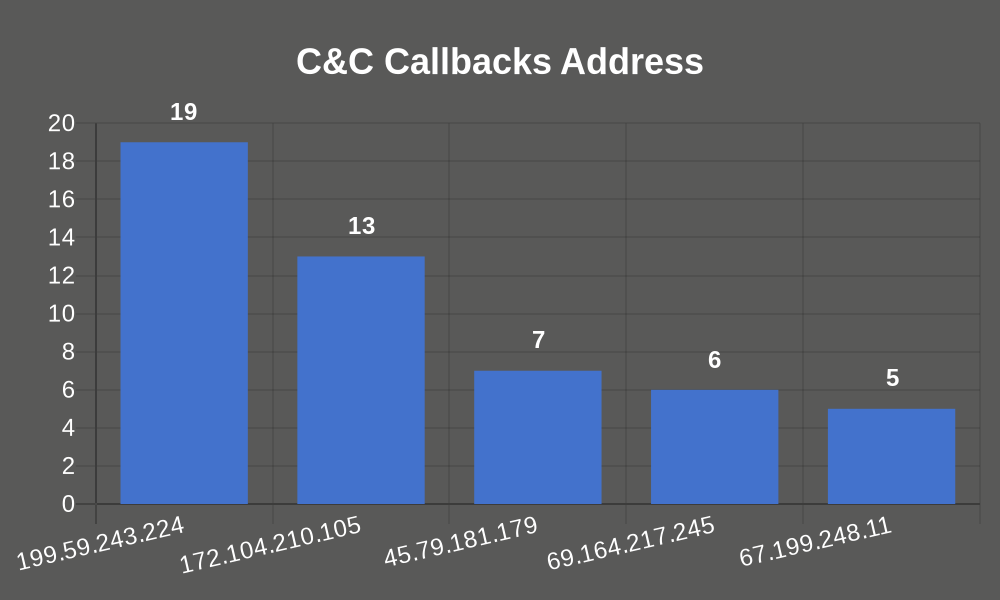
## 5.7 C&C Callback

We generated a C&C Callbacks Event of the last 30 Days on 27th Sep 2023 from Apex Central/Apex One. There was a total of 50 detections.



15 times C&C Callbacks were detected on the IDJKN002 endpoint.

13 times C&C Callbacks were detected on the SEAADP01 endpoint.



199.59.243.224 callback address detected 19 times, check this IP Address to if it's a secure connection then add it to the suspicious approve list otherwise block this IP address.

172.104.210.105 callback address detected 13 times, check this IP Address to if it's a secure connection then add it to the suspicious approve list otherwise block this IP address.

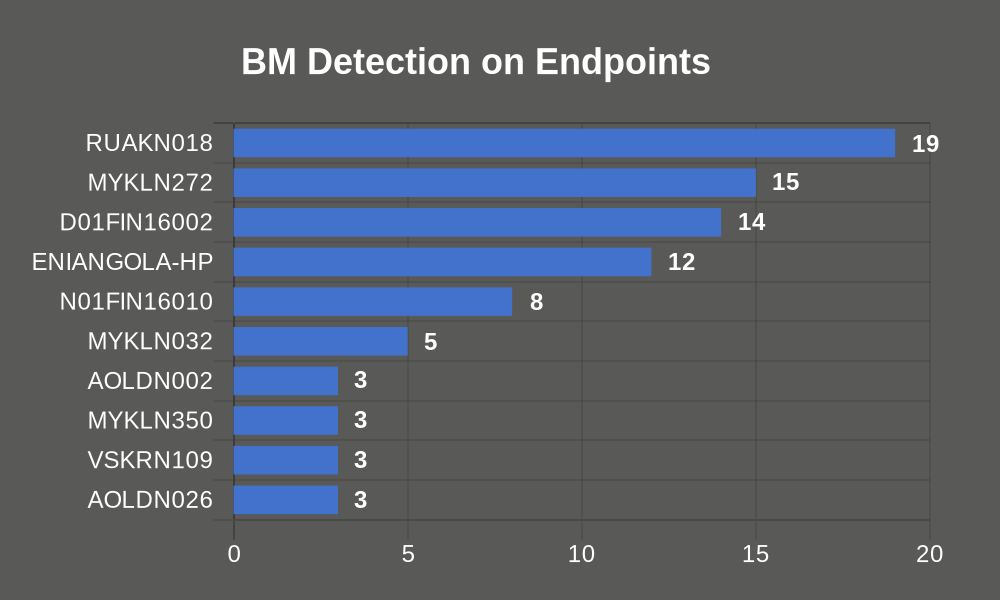
Check below KB in case of Command and Control (C&C) callback detection.

* + <https://success.trendmicro.com/solution/1121033>
  + <https://global.sitesafety.trendmicro.com/result.ph>

Recommended to check the Callback address that is triggered and whitelist the internal IP.

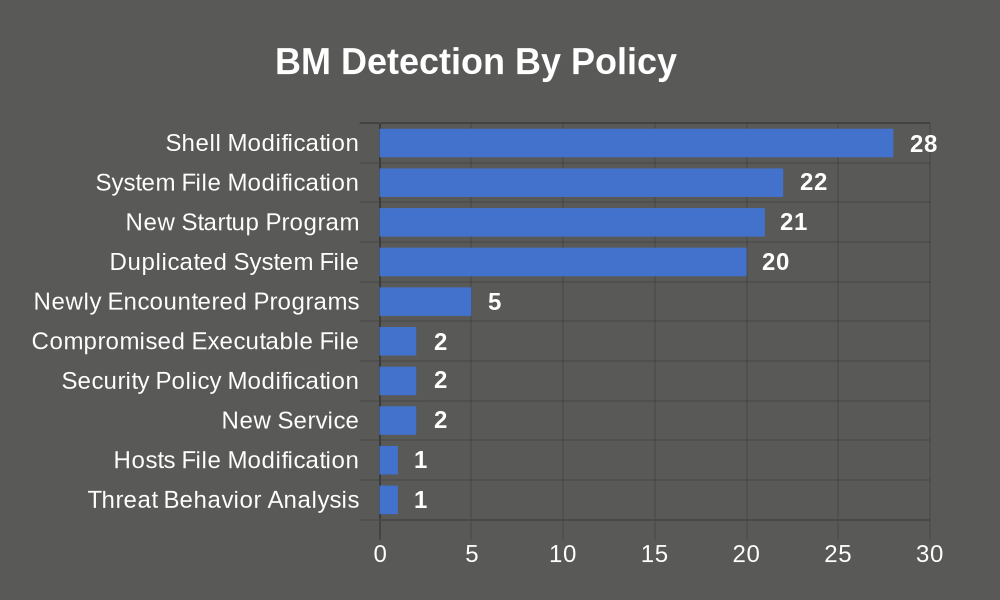
## 5.8 Behavior Monitoring

We generated a Behavior Monitoring Event of the last 90 Days on 27th Sep 2023 from Apex Central/Apex One. There was a total of 104 detections.



On the endpoint, RUAKN018 Behavior Monitoring was triggered 19 times with High Severity. Processes were denied and assessed by Apex One.

On the endpoint, MYKLN272 Behavior Monitoring was triggered 15 times with Low Severity. Processes were assessed by Apex One.



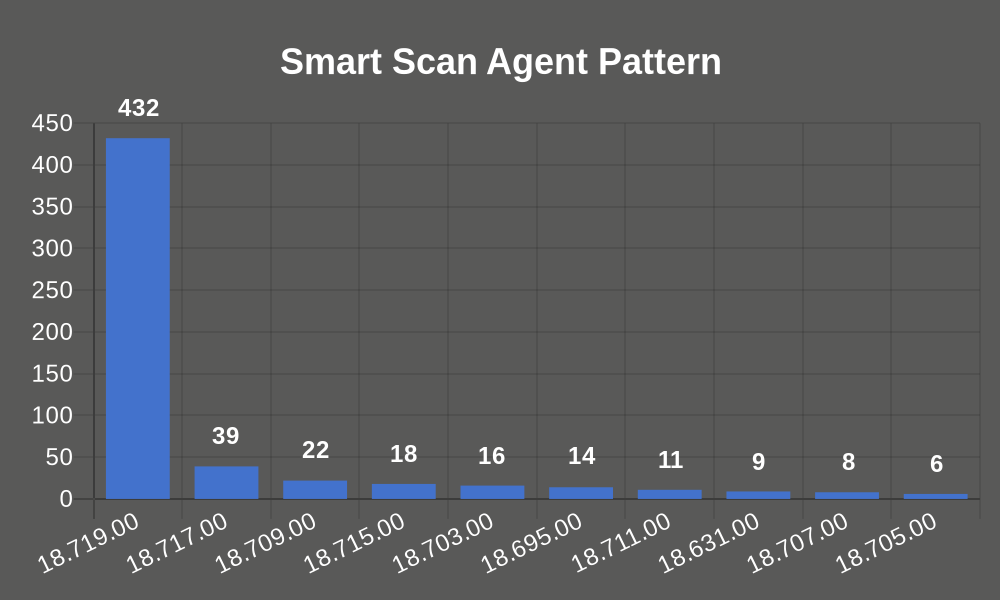
28 times Shell Modification was triggered on D01FIN16002, MYKLN032, N01FIN16010, and ENIANGOLA-HP endpoints, and it was denied and assessed by Apex One.

22 times System File Modification was triggered on RUAKN018 and MYKLN350 endpoints, and it was denied and assessed by Apex One.

|  |  |  |  |
| --- | --- | --- | --- |
| **BM BY POLICY & RISK LEVEL** | **ACTION** | | |
| **Deny** | **Assess** | **Terminate** |
| **Shell Modification** | **8** | **20** |  |
| Low |  |  |  |
| **System File Modification** | **1** | **21** |  |
| High |  |  |  |
| **New Startup Program** |  | **21** |  |
| Low |  |  |  |
| **Duplicated System File** | **3** | **17** |  |
| Low |  |  |  |
| **Newly Encountered Programs** | **5** |  |  |
| Low |  |  |  |
| **Compromised Executable File** |  |  | **2** |
| High |  |  |  |
| **Security Policy Modification** | **2** |  |  |
| High |  |  |  |
| **New Service** |  | **2** |  |
| Low |  |  |  |
| **Hosts File Modification** | **1** |  |  |
| High |  |  |  |
| **Threat Behavior Analysis** |  |  | **1** |
| High |  |  |  |
| **Total** | **20** | **81** | **3** |

## 5.9 Smart Scan Agent Pattern Coverage Details

|  |  |
| --- | --- |
| Last 3 days Pattern updated agents | 489 |
| Older than 3 Days Pattern updated agents | 112 |
| Total Agents | 601 |



# 6 Apex One & Apex Central Further Information

[Apex One Administrator Guide](https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p3_ag.pdf)

[Apex One Installation and Upgrade Guide](https://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne_2019_iug.pdf)

# 7 End of Life for Trend Micro Products information

<https://success.trendmicro.com/solution/1105726>

# 8 Other documentation

[Apex One Best Practice Guide](https://powerbox-na-file.trend.org/SFDC/DownloadFile_iv.php?jsonInfo=%7B%22Query%22%3A%22E6%2FaBX7NRLgNhlFV9prpuOiZ%2BfBD3GRI5g3EWcXN2wO0yrcs72AtOr%2Bd7jbTo0Fnj%2F%2F%2F76wXivkV6IVgYXc%2BQzbD%2B%2FKfkbOyItLyPfpSIJoT0HV%2B3GhPZU02OB6BmcIuhU7IZ3Ki%2B2ZNf3oZi%2FxcX%2BaDQ3AXLm1NlrYHrKAmBWl808Gv8mFeN0MeOaCoZ5%2FOZJhpJ4W6NboPVDxDNrHY%2BZWIfRvXkGVzX0vnfp%2B%2Fc34HfH%2B4SyIIL7cbRn1vJCEsxqanrr7sqZePi1K2jesmdb4l7KQ5HiOampFamEGT698%3D%22%2C%22iv%22%3A%224ce282318ea4758451af77c290c71f25%22%7D)