Sổ tay Ứng phó Sự cố Ransomware

Dự án: **Australian Government Cyber Security Training Development Program for Vietnam - Chương trình Phát triển Năng lực An toàn thông tin Việt Nam của Chính phủ Úc**

Tháng 1/2025

Nội dung

Danh sách các Bảng

Danh sách các Hình

1 Giới thiệu

1.1 Mục đích và mục tiêu

Sổ tay Ứng phó Phần mềm tống tiền Ransomware (Ransomware Playbook, gọi tắt là Sổ tay Ứng phó Sự cố Ransomware) này hỗ trợ cho các tổ chức thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia (gọi tắt là Mạng lưới UCSC) xây dựng Kế hoạch Ứng phó đối với sự cố tấn công tống tiền.

Tài liệu này khuyến nghị các hành động nên thực hiện khi phát hiện Ransomware. Danh sách các hành động này có thể không đầy đủ, và các giai đoạn có thể được thực hiện đồng thời. Các tổ chức có thể bổ sung thêm các hành động ngoài các hướng dẫn trong Sổ tay này cũng như có thể giảm bớt các hành động được nêu trong Sổ tay nếu không phù hợp với quá trình ứng phó sự cố thực tế.

Sổ tay này không nêu chi tiết việc xem xét cho các sự cố loại khủng hoảng, cũng như chi tiết cho hoạt động truyền thông cần thiết. Đội ứng cứu sự cố nên tham khảo thêm Kế hoạch ứng phó sự cố an toàn thông tin.

Sổ tay Ransomware này không bao gồm các hướng dẫn kỹ thuật cụ thể cho việc ứng phó.

Trong trường hợp xảy ra sự cố an toàn thông tin mạng nghiêm trọng, khuyến nghị các đơn vị tham khảo quy định tại Quyết định 05/2017/QĐ-TTg và báo cho cơ quan điều phối quốc gia hỗ trợ.

1.2 Đối tượng

Sổ tay Ransomware này dành cho:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC).
- Thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia.
- Các tổ chức, doanh nghiệp trong nước có nhu cầu tham khảo, áp dụng.

1.3 Các tiêu chuẩn và khung tham chiếu

Sổ tay này đã xem xét và sử dụng các tiêu chuẩn và tham chiếu sau:

- Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ NIST: Computer Security Incident Handling Guide – Hướng dẫn xử lý sự cố bảo mật máy tính, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Trung tâm An toàn mạng Úc: Cyber Incident response Plan Guidance and Template - Hướng dẫn và Mẫu Kế hoạch ứng phó sự cố mạng, https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/incident-response/cyber-security-incident-response-planning-practitioner-guidance

Ngoài ra, trong Sổ tay Ransomware này, có tham khảo thông tin kỹ thuật của các cơ quan an toàn thông tin mạng quốc gia và các công ty an toàn mạng hàng đầu trong ngành:

- Trung tâm An toàn mạng Úc ACSC (https://www.cyber.gov.au)
- Trung tâm An toàn mạng Vương quốc Anh NCSC-UK (https://www.ncsc.gov.uk/)
- Cơ quan An toàn mạng và An toàn Cơ sở hạ tầng Hoa Kỳ CISA (https://www.cisa.gov/)
- Viện Công nghệ SANS (https://www.sans.org)
- Công ty CyberCX - Úc (https://cybercx.com.au/
- Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ NIST (https://www.nist.gov/)

1.4 Ưu tiên ứng phó sự cố

Các tổ chức Thành viên Mạng lưới UCSC sẽ ưu tiên tiến hành ứng phó các sự cố an toàn thông tin mạng theo trình tự sau:

1) **Bảo vệ tính mạng và an toàn con người**: nếu một sự cố an toàn thông tin mạng có thể gây thương tích hoặc tử vong cho con người, ưu tiên hàng đầu trong việc ứng phó với sự cố đó là bảo vệ an toàn của con người.
2) **Duy trì/khôi phục hoạt động của các hệ thống trọng yếu quốc gia**: nếu một sự cố an toàn thông tin mạng đang ảnh hưởng đến một hệ thống trọng yếu cung cấp dịch vụ cho công dân Việt Nam, thì việc duy trì hoặc khôi phục hoạt động của hệ thống đó là ưu tiên.
3) **Thu thập bằng chứng kỹ thuật số**: nếu không xung đột với hai ưu tiên trên, việc thu thập bằng chứng thích hợp để hỗ trợ điều tra kỹ lưỡng về sự cố an toàn thông tin mạng và có thể đưa ra bằng chứng tại toà án là một ưu tiên.
4) **Phục hồi kịp thời sau sự cố**: nếu không xung đột với ba ưu tiên trên, ưu tiên sẽ là đảm bảo phục hồi nhanh chóng sau sự cố an toàn thông tin mạng và đưa hoạt động trở lại bình thường.

1.5 Thẩm quyền và Xem xét

[Giám đốc/Người được uỷ quyền của Tổ chức] có thẩm quyền phê duyệt tài liệu này để áp dụng trong toàn tổ chức.

Hàng năm, tài liệu này phải được *[Giám đốc/Người được uỷ quyền của Tổ chức]* xem xét để đảm bảo tài liệu luôn được cập nhật. Sử dụng Bảng 1 và Bảng 2 để ghi lại tất cả các cập nhật và phê duyệt đối với Sổ tay này.

Kiểm soát Tài liệu	
Tác giả	CyberCX – VNCERT/CC
Chủ sở hữu	Tổ chức …
Ngày tạo	
Tên người/đơn vị xem xét lần cuối	
Ngày xem xét lần cuối	
Tên người/đơn vị phê duyệt lần cuối và ngày	
Ngày xem xét tiếp theo	

Bảng 1: Kiểm soát và Xem xét Tài liệu

Phiên bản	Ngày phê duyệt	Được phê duyệt bởi	Mô tả thay đổi
1.0	…/…/2024	Cục An toàn thông tin	Bản hướng dẫn gửi thành viên Mạng lưới UCSC
1.1	…/….2024		bản sửa đổi cho phù hợp với …

Bảng 2: Kiểm soát Phiên bản

2 Giới thiệu

Ransomware là một loại phần mềm độc hại khóa và mã hóa các tệp của nạn nhân để họ không thể truy cập được nữa. 'Tiền chuộc' là khoản tiền để đổi lấy việc khôi phục quyền truy cập vào các tệp, hệ thống và/hoặc mạng, thường ở dạng tiền điện tử. Tội phạm ransomware có thể yêu cầu tiền chuộc để ngăn chặn những dữ liệu và tài sản trí tuệ bị rò rỉ hoặc bán trực tuyến.

Cũng như các phần mềm độc hại khác, ransomware có thể được kích hoạt sau khi nạn nhân truy cập các trang web không an toàn hoặc đáng ngờ, mở email hoặc tệp từ các nguồn không xác định hoặc nhấp vào các liên kết độc hại trong email hoặc trên mạng xã hội. Khi ransomware thành công, các dấu hiệu phổ biến thường là bật lên các thông báo yêu cầu thanh toán để mở khóa tệp, không thể truy cập thiết bị hoặc đăng nhập, yêu cầu mật khẩu hoặc mã để mở hoặc truy cập tệp, thông báo các tệp đã di chuyển khỏi thư mục hoặc vị trí thông thường của chúng, và/hoặc các tệp có phần mở rộng hoặc tên tệp bất thường.

3 Cách sử dụng Sổ tay

Sổ tay này trình bày chi tiết cách đội ứng cứu sự cố sẽ phản ứng hiệu quả với các sự cố ransomware.

Mục của tài liệu	Mô tả
Giới thiệu và Tổng quan	
Mục 1-2	Trước khi đi vào quy trình ứng phó sự cố ransomware, Sổ tay cung cấp phần giới thiệu về mục đích, đối tượng, các tiêu chuẩn và khuôn khổ liên quan, các ưu tiên và bối cảnh. **Hướng dẫn sử dụng**: Đọc các mục theo thứ tự từ 1 đến 2 để hiểu rõ ngữ cảnh của Sổ tay Ứng phó Ransomware.
Điều tra	
Mục 4	Giai đoạn điều tra cung cấp cho đội ứng cứu sự cố các nhiệm vụ cần thực hiện khi ứng phó với các cuộc tấn công ransomware. **Hướng dẫn sử dụng**: Đọc và làm theo các bước từ B0.01 đến B1.15 (đồng thời tham khảo các Phụ lục và Hình ảnh liên quan). Các bước 'Quyết định' được sử dụng để tạo một khoảng dừng trong quy trình để đưa ra quyết định trước khi quy trình có thể tiếp tục.
Ngăn chặn	
Mục 5	Giai đoạn ngăn chặn nhằm mục đích hạn chế mức độ ảnh hưởng của sự cố và sử dụng thông tin thu thập được từ giai đoạn điều tra để bảo vệ khỏi bị tấn công và hạn chế sự di chuyển ngang (lateral movement) của ransomware. **Hướng dẫn sử dụng**: Đọc và làm theo các bước từ B2.01 đến B2.06 (đồng thời tham khảo các Phụ lục liên quan). Các bước 'Quyết định' được sử dụng để tạo một khoảng dừng trong quy trình để đưa ra quyết định trước khi thực hiện tiếp quy trình.

Loại bỏ	
Mục 6	Giai đoạn loại bỏ nhằm đảm bảo rằng sự cố đã được khắc phục. **Hướng dẫn sử dụng**: Đọc và làm theo các bước từ B3.01 đến B3.03 (đồng thời tham khảo các Phụ lục liên quan). Các bước 'Quyết định' được sử dụng để tạo một khoảng dừng trong quy trình để đưa ra quyết định trước khi thực hiện tiếp quy trình.
Phục hồi	
Mục 7	Giai đoạn phục hồi nhằm mục đích xác định nguyên nhân của sự cố, từ đó đưa ra các cải tiến trong tương lai hoặc triển khai các công nghệ kỹ thuật, cũng như xác nhận các bước khắc phục đã thực hiện trước đó và khôi phục bất kỳ chức năng nào bị hạn chế. **Hướng dẫn sử dụng:** Đọc và làm theo các bước từ B4.01 đến B4.03 (đồng thời tham khảo các Phụ lục liên quan).

4 Điều tra

Điều tra ransomware gồm nghiên cứu và phân tích về kẻ tấn công đang nghi ngờ hoặc đã biết, và/hoặc biến thể ransomware. Nghiên cứu này có thể hỗ trợ Đội ứng cứu sự cố trong việc xác định phản ứng phù hợp nhất đối với cuộc tấn công ransomware cụ thể.

Trước khi thực hiện các bước điều tra từ B0.01 đến B1.14, đội ứng cứu sự cố sẽ làm việc với đơn vị bị ảnh hưởng để thực hiện các biện pháp ngăn chặn ngay lập tức nhằm hạn chế tác động của sự cố đang diễn ra.

Hành động		**Mô tả**
Cô lập ransomware ngay lập tức		Đội ứng cứu sự cố sẽ ngay lập tức cô lập ransomware.
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
B1.01	Ngay lập tức cô lập ransomware	*[Nhập vị trí công việc liên quan cụ thể …]*
Mô tả hành động		
Sau khi xác định máy chủ/mạng bị ảnh hưởng, đội ứng cứu sự cố sẽ thực hiện ngay lập tức các biện pháp để cô lập ransomware. Cân nhắc các bước cô lập dưới đây, tùy theo hoàn cảnh sự cố ransomware cụ thể: 1. Khoá các kết nối của hệ thống, sử dụng các kỹ thuật như ngăn chặn qua EDR, triển khai tường lửa cục bộ, tắt giao diện mạng hoặc vô hiệu hóa cổng chuyển mạch của bộ định tuyến. 2. Sau khi chặn kết nối, các hệ thống bị ảnh hưởng phải được cách ly để ngăn chặn sự di chuyển ngang của ransomware. Phương pháp tốt nhất cho việc này sẽ được xác định bởi các hệ thống được đề cập và công cụ có sẵn. Trong một số trường hợp, điều này có thể yêu cầu ngắt kết nối vật lý các hệ thống hoặc máy chủ khỏi mạng, vô hiệu hóa giao diện mạng hoặc cấu hình lại các thiết bị mạng. 3. Nếu không thể tạm ngừng mạng bị ảnh hưởng, đội ứng cứu sự cố sẽ:		

- Ngắt kết mọi kết nối với các Thiết bị Lưu trữ Mạng như máy chủ, máy tính, điện thoại và máy tính bảng.
- Nếu có thể, rút cáp ethernet của các thiết bị bị nhiễm.
- Ngắt kết nối Wi-Fi (nếu có) của các thiết bị bị ảnh hưởng.
- Nếu thiết bị bị ảnh hưởng không thể gỡ khỏi mạng, tắt nguồn của thiết bị (sau khi đã trích xuất toàn bộ bộ nhớ để điều tra).

Cần lưu ý rằng các bước trên sẽ bị ảnh hưởng nhiều vào các hoàn cảnh cụ thể của sự cố ransomware và đội ứng cứu sự cố. Quy trình cô lập sẽ được điều chỉnh cho từng trường hợp cụ thể.

Việc trích xuất dữ liệu của ransomware thường bao gồm trích xuất thông tin đăng nhập hàng loạt. Nếu nghi ngờ một sự cố như vậy, bắt buộc phải bảo vệ mạng và các nguồn thông tin khác khỏi khả năng truy cập trái phép dựa trên thông tin xác thực. Nếu phù hợp, Đội ứng cứu sự cố cần vô hiệu:

- Mạng riêng ảo VPN.
- Máy chủ truy cập từ xa
- Tài nguyên đăng nhập một lần SSO

Sau khi hoàn thành, hãy chuyển sang giai đoạn Điều tra.

Bảng 3: Quy trình Cô lập ngay lập tức

Xem chi tiết các tiến trình điều tra trong bảng bên dưới.

Hành động		**Mô tả**
Điều tra sự cố		Đội ứng cứu sự cố điều tra sự cố ransomware.
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
B1.02	Loại bỏ các thông báo ransomware	*[Nhập vị trí công việc liên quan cụ thể …]*
Mô tả hành động		

Ransomware là một dạng phần mềm độc hại có thể lây lan qua các trang web độc hại, tệp đính kèm hoặc liên kết trong email, bài đăng trên mạng xã hội và các ứng dụng hoặc tệp có thể tải xuống. Một khi đã thực thi thành công, ransomware có thể lây lan qua các máy tính, máy chủ, mã hóa các thiết bị và có thể đánh cắp dữ liệu.
 	
Tuy nhiên, một số tội phạm dùng nỗi lo sợ về ransomware trong chiêu lừa nhằm đòi tiền chuộc. Một số khác kém tinh vi hơn có thể gửi hàng loạt email lừa đảo cho các cá nhân và tuyên bố đã lây nhiễm máy tính, máy chủ trong khi họ chưa làm.
 	
Khi nhận được báo cáo sự cố, đội ứng cứu sự cố nên yêu cầu thông tin sau từ người hoặc bên báo cáo:
• Nạn nhân biết hoặc nhận được thông báo về một khả năng sự cố ransomware khi nào?
• Nếu đã nhận được tin nhắn, có kèm theo bất kỳ mối đe dọa, yêu cầu và bằng chứng nào về sự xâm nhập không?
  ○ Những mối đe dọa chứa các tuyên bố đó có dễ bác bỏ không?
  ○ Tin nhắn có không đề cập đến tên cá nhân hoặc bất kỳ tham chiếu nào đến tổ chức hay không?
• Đã có bất kỳ thiết bị nào bị mã hóa chưa?
 	
Đội ứng cứu sự cố sẽ xem xét các cân nhắc trên và quyết định xem sự cố có phải là lừa đảo hay không. Nếu sự cố là một trò lừa đảo chứ không phải ransomwares, sẽ hướng dẫn nạn nhân/tổ chức		

xóa và chặn email. Nếu đã trả tiền cho các kẻ lừa đảo, thì cá nhân/tổ chức cần gửi báo cáo đến các cơ quan thực thi pháp luật.

Sau khi hoàn thành, hãy tiếp tục đến Bước B1.03.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.03	Xác định phạm vi ảnh hưởng	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Đội ứng cứu sự cố sẽ xác định phạm vi ảnh hưởng gần đúng trên các hệ thống/dịch vụ của tổ chức và các tác động tiềm ẩn có thể xảy ra.

Đội ứng cứu sự cố sẽ xem xét các câu hỏi dưới đây:

1. Các dịch vụ và/hoặc hệ thống của tổ chức đã bị ảnh hưởng đến mức độ nào?
   - Những hệ thống nào được biết là bị ảnh hưởng?
   - Bản chất của các hệ thống bị ảnh hưởng là gì? (Hệ điều hành, hệ thống tệp, kết nối mạng, loại cơ sở hạ tầng)
   - (Nếu có thể áp dụng) Phiên bản của hạt nhân (kernel), thông tin gói dịch vụ, cơ sở dữ liệu bị ảnh hưởng, ổ đĩa chia sẻ, SAN và trạng thái sao lưu cho các hệ thống bị ảnh hưởng là gì?
   - Các vectơ nào có thể đã phát tán ransomware từ các hệ thống này sang các hệ thống khác?
   - Những hệ thống nào có thể bị ảnh hưởng nhưng cần phải điều tra thêm?
   - Đã không thể truy cập được trong bao lâu?
   - Điều này có tác động gì đến hoạt động của tổ chức?
   - Nếu tổ chức thuộc cơ quan trọng yếu, liệu cuộc tấn công có cản trở khả năng thực hiện các dịch vụ quan trọng của tổ chức không?
2. Những thành phần phụ thuộc nào có thể dẫn đến lỗi liên hoàn?
   - Những lỗi liên hoàn đó có ảnh hưởng đến các tổ chức và bên liên quan khác không?
3. Tình trạng sao lưu của tổ chức đối với các hệ thống và dịch vụ bị ảnh hưởng là gì?
   - (Nếu có thể) Thời gian khôi phục ước tính là bao lâu?
   - (Nếu có thể) Các bản sao lưu có đầy đủ không hay có dữ liệu nào bị thiếu? Sẽ tác động gì đến hoạt động của tổ chức?
   - Có lịch tắt sao lưu cho đến khi xác thực tính toàn vẹn của tài liệu không?
   - Có ngắt kết nối mạng giữa các hệ thống có khả năng bị ảnh hưởng và hệ thống sao lưu không?
   - Có tạo bản sao trên máy của hệ thống sao lưu không?
   - Có tắt nguồn hệ thống sao lưu trên máy không?
   - Nếu không có bản sao lưu nào có thể dùng được:
     - Tổ chức có bất kỳ tùy chọn dự phòng nào khác không?
     - Điều này ảnh hưởng như thế nào đến thời gian khôi phục cho các dịch vụ bị ảnh hưởng?
4. Có cần xem xét những tác động rộng hơn bên ngoài hệ thống CNTT không?

Đội ứng cứu sự cố sẽ xem xét và cân nhắc các câu hỏi trên, làm chi tiết các câu trả lời có sẵn cho mỗi câu hỏi và thực hiện phân tích thêm để khám phá các khu vực chưa rõ.

Trong trường hợp bước điều tra này tiết lộ các tổ chức và bên liên quan khác có thể bị ảnh hưởng, Đội ứng cứu sự cố cần thông báo cho các tổ chức và hoặc bên liên quan đó.

Sau khi hoàn thành, hãy tiếp tục đến Bước B1.04.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.04	Rà soát các tài sản các cơ quan trọng yếu	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Đội ứng cứu sự cố sẽ rà soát các tài sản của các cơ quan trọng yếu bị ảnh hưởng, dựa trên phân loại cơ sở hạ tầng trọng yếu đã được quy định trong quyết định 632/QĐ-TTg Ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia khi áp dụng cho danh sách hệ thống thông tin của họ. Nếu có bất kỳ tài sản quan trọng nào của quốc gia bị ảnh hưởng, cần liên hệ chủ sở hữu tài sản có liên quan ngay lập tức.

Sau khi hoàn thành, hãy tiếp tục đến bước B1.05.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.05	Xác định và ngăn chặn kiểu xâm nhập	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Đội ứng cứu sự cố sẽ điều tra sự cần thiết phải thực hiện các biện pháp ngăn chặn ngay lập tức trong trường hợp xâm phạm của ransomware có khả năng lây lan sang các nơi khác.

Đội ứng cứu sự cố sẽ phải xác định nguyên nhân gốc rễ của sự cố để giúp thông báo các việc cần làm nhằm ngăn chặn kiểu xâm phạm. Các kiểu phổ biến là:

- Lừa đảo qua email phishing
- Lừa đảo qua giọng nói
- Dẫn dụ tải về
- Các lỗ hổng như: Thực thi mã từ xa, SSRF, Injection (chèn), Dịch vụ từ xa, dùng mật khẩu mặc định hoặc yếu, khai thác CVE.
- Mất thiết bị
- Lỗi của con người

Nếu xác định có khả năng là một cuộc tấn công khai thác CVE, đội nên chuyển sang ngăn chặn do tính chất có thể phức tạp của các cuộc tấn công khai thác CVE và việc cần thiết phải ngăn chặn kiểu xâm phạm đó ngay. B1.12. sẽ phác thảo các bước để điều tra sâu về khai thác CVE.

Đội ứng cứu sự cố sẽ làm việc với nạn nhân để tìm hiểu xem liệu có nguy cơ xâm phạm thêm đối với các nạn nhân khác hay không do phần mềm độc hại nằm trong email, trang web, ứng dụng, tệp và/hoặc tin nhắn mạng xã hội độc hại mà người khác có thể tương tác.

Nếu có thể, đội ứng cứu sự cố sẽ xác định vị trí của email, trang web, ứng dụng, tệp và/hoặc tin nhắn mạng xã hội độc hại mà người dùng khác có thể tương tác. Sau đó, nếu thích hợp hoặc tuỳ trường hợp cụ thể mà đội sẽ thực hiện các hoạt động để từ chối truy cập, ngăn chặn sự xâm nhập thêm.

Ví dụ: đội ứng cứu sự cố có thể:

- Xóa hoặc chặn truy cập vào email độc hại.
- Chặn truy cập vào liên kết URL độc hại.
- Từ chối ứng dụng hoặc tệp sử dụng whitelist (danh sách trắng).
- Chặn hoặc xóa tin nhắn mạng xã hội.

Ngoài ra, hoặc kết hợp với các hành động trên, nên truyền đạt cảnh báo cho toàn tổ chức bị ảnh hưởng.

Sau khi hoàn thành, hãy tiếp tục đến bước B1.06.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.06	Điều tra mức độ xâm phạm	*[Nhập vị trí công việc liên quan cụ thể …]*
Mô tả hành động		
Đội ứng cứu sự cố sẽ điều tra mức độ xâm phạm của ransomware. Tham khảo Phụ lục A hướng dẫn về cách điều tra mức độ xâm phạm. Sau khi hoàn thành, tiếp tục như bên dưới.		
Quyết định: Cuộc tấn công ransomware có bao gồm thông báo hoặc tin nhắn đòi tiền chuộc không?		• Nếu có – Tiếp tục đến bước B1.07 • Nếu không – Tiếp tục đến bước B1.08.
#	**Nhiệm vụ**	**Người chịu trách nhiệm:**
B1.07	Điều tra và xác định tác nhân đe doạ	*[Nhập vị trí công việc liên quan cụ thể …]*
Mô tả hành động		

Các kẻ tấn công thường để lại các thông báo hoặc tin nhắn đòi tiền chuộc sau khi lây nhiễm thành công vào hệ thống của tổ chức và yêu cầu thanh toán. Các thông báo, đôi khi được hiển thị trên màn hình của các thiết bị đã bị mã hóa hoặc được lưu vào màn hình nền (thường có tiêu đề là "readme.txt"), cung cấp các thông tin sau:

- Thông tin về cuộc tấn công
- Các yêu cầu
- Thời gian phải tuân thủ
- Chi tiết liên hệ
- (Nếu có) Liên kết TOR có liên quan đến trang web rò rỉ ransomware
- Loại biến thể ransomware

Những tin nhắn đó cần phải được phân tích và lưu lại vì các chi tiết trong đó sẽ cung cấp thông tin cho các bước điều tra tiếp theo.

Tham khảo Phụ lục B để xem các ví dụ về thông báo đòi tiền chuộc.

Nhóm có thể xác định kẻ tấn công dựa trên cuộc tấn công. Việc xác định kẻ tấn công sẽ giúp hiểu các TTP mà họ thường dùng. Các thông tin thường dùng để xác định kẻ tấn công là:

- Thông báo đòi tiền chuộc
- Payload phần mềm độc hại
- Phần mở rộng tệp bị mã hóa
- Email / Cổng thông tin web
- Địa chỉ Bitcoin

Tùy thuộc vào mức độ tinh vi của kẻ tấn công, biến thể ransomware đã dùng có thể lỗi thời, có sẵn các bước dễ dàng giải mã.

Đội ứng cứu sự cố sẽ thực hiện nghiên cứu về nhóm tấn công ransomware, sử dụng thông tin thu thập được trong các bước trên để khám phá thêm các yếu tố dưới đây:

- Danh tiếng và lịch sử của tác nhân đe dọa ransomware là gì?

- Họ có danh tiếng về việc tôn trọng các khoản thanh toán không?
- Họ có được biết đến với việc bán dữ liệu công khai trên darkweb không?
- Họ có đang bị điều tra từ bất kỳ CERT quốc tế nào mà có thể hỗ trợ không?
- Nhóm có tinh vi không?
- Nhóm có liên kết với một quốc gia nào không?
- Họ có một trang web công bố các rò rỉ có thể truy cập công khai không?
- Nhóm có sử dụng một loại biến thể ransomware cụ thể không?
- Biến thể này có nổi tiếng với việc đánh cắp dữ liệu hàng loạt không?

Tham khảo Phụ lục C để biết các tài nguyên có thể được tận dụng để nghiên cứu các biến thể ransomware và tác nhân đe dọa.

Sau khi hoàn thành, hãy tiếp tục đến bước B1.08.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.08	Tham gia với các CERT quốc tế	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Ransomware là một thách thức đáng kể đối với các chính phủ và tổ chức trên toàn cầu. Do đó, các cơ quan an toàn thông tin mạng quốc tế (đôi khi được gọi là CERT) sẽ hợp tác với nhau để giảm tác động của ransomware và hỗ trợ lẫn nhau trong việc ứng phó với các sự cố, thông qua:

- Giảm thiểu các biến thể ransomware
- Sách trắng về các nhóm ransomware
- Hỗ trợ kỹ thuật

Nếu bước B1.07 không tiết lộ bất kỳ tư vấn công khai nào liên quan đến các nhóm và/hoặc biến thể ransomware cụ thể, Đội ứng cứu sự cố nên cân nhắc liên hệ với các CERT quốc tế.

Đội ứng cứu sự cố sẽ xem xét Hình 8, trong đó có nêu các CERT quốc gia nổi bật nhất có thể được liên hệ để yêu cầu hỗ trợ và/hoặc cung cấp thông tin về biến thể ransomware cụ thể có liên quan đến sự cố Ransomware.

Sau khi hoàn thành, hãy tiếp tục bước B1.09.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.09	Đánh giá tác động của các hệ thống và/hoặc mạng bị khóa	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Đội ứng phó sự cố sẽ điều tra mở rộng tác động của các hệ thống và/hoặc mạng bị khóa.

Đội ứng phó sự cố sẽ tận dụng bất kỳ công cụ kỹ thuật nào có sẵn có thể hỗ trợ xác định các hệ thống được thuê ngoài.

Sau khi hoàn thành, hãy tiếp tục bước B1.10.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.10	Đánh giá tác động của sự cố	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Đội ứng cứu sự cố sẽ đánh giá tác động của các hệ thống và/hoặc dữ liệu đã bị mã hóa và xem xét những thông tin có khả năng bị trích xuất.

Đội ứng cứu sự cố sẽ đánh giá tác động này dựa trên tác động đã biết của các mối đe dọa phổ biến và cụ thể của công ty. Các tác động có thể bao gồm:

- Đánh cắp thông tin đăng nhập
- Phát tán phần mềm độc hại
- Hoạt động tội phạm
- Tống tiền/Ransomware
- Tổn thất tài chính
- Mất hợp đồng
- Hợp đồng không được gia hạn
- Giảm giá thầu cho khách hàng của mình
- Tiền phạt
- Quy định

Thiết lập danh sách các điểm cuối bị ảnh hưởng, các tài khoản/máy chủ bị xâm nhập và xác định mức độ ưu tiên mà các tài sản bị ảnh hưởng cần phải được khôi phục.

Trên các thiết bị bị ảnh hưởng, (nếu có thể) chạy bất kỳ phần mềm chống vi-rút/chống mã độc nào có sẵn để hỗ trợ xác định tác động trên toàn mạng. Nếu việc nhiễm mã độc được xác nhận, hãy sử dụng Sổ tay Mã độc để ứng phó.

Đội ứng cứu sự cố sẽ điều tra các câu hỏi về đánh cắp dữ liệu cụ thể của ransomware như bên dưới:

- Loại dữ liệu nào đã bị đánh cắp?
    - Phân loại dữ liệu (bí mật, nhạy cảm, v.v.).
    - Tính quan trọng của dữ liệu đối với hoạt động, kinh doanh.
- Có bao nhiêu dữ liệu đã bị đánh cắp?
- Từ những hệ thống nào bị nghi ngờ có dữ liệu bị đánh cắp?
- Các cân nhắc về uy tín, tổ chức, pháp lý và đạo đức nào cần cho việc xem xét hậu quả của việc mã hóa và trích xuất dữ liệu dữ liệu?
- Những ai hoặc tổ chức nào có thể cần liên hệ do đánh cắp dữ liệu? Chẳng hạn như:
    - Cơ quan thực thi pháp luật.
    - Bộ phận An toàn An ninh Quốc gia.
    - Công chúng và/hoặc Ngành.

- Quốc hội.
- Bộ trưởng.
- Công chúng.
- Truyền thông.

Nếu có sẵn và có thể áp dụng, hãy cân nhắc sử dụng Sổ tay Ứng phó Mất Dữ liệu để thông báo các hành động tiếp theo sau khi hoàn thành các câu hỏi trên.

Đội ứng cứu sự cố cũng sẽ cần xem xét rủi ro liên quan đến việc công bố dữ liệu bị đánh cắp:

- Dữ liệu đã được công bố trực tuyến chưa?
- Dữ liệu có thể truy cập miễn phí hoặc đang được bán trực tuyến hay không?
    - Nếu có, chi phí và lợi ích của việc công khai thừa nhận rằng đơn vị đã gặp sự cố an toàn thông tin mạng là gì?
    - Thông tin nào, nếu được công khai, có thể làm suy yếu vị thế của đơn vị trong việc đàm phán với tác nhân đe dọa?

Sau khi hoàn thành, hãy tiếp tục bước B1.11.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.11	Điều tra động cơ và bản chất của cuộc tấn công từ tác nhân đe dọa.	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Hiểu động cơ của tác nhân đe dọa là một bước quan trọng để hướng dẫn hướng ứng phó. Khi thực hiện điều tra, đội ứng cứu sự cố sẽ xem xét động cơ đằng sau cuộc tấn công, có thể bao gồm:

- Lợi ích tài chính.
- Lợi ích chính trị.
- Lợi ích quân sự.
- Theo chủ nghĩa hack - Hacktivism (sử dụng tấn công mạng để thúc đẩy chương trình chính trị hoặc xã hội).

Hiểu động cơ, hoặc ít nhất là xác định các động cơ tiềm ẩn đằng sau các cuộc tấn công ransomware có thể hỗ trợ Đội ứng cứu sự cố trong việc xác định các rủi ro liên quan và quyết định các bước tiếp theo.

Tương tự như vậy, việc xác định bản chất của cuộc tấn công là rất quan trọng để khắc phục. Khi phân loại loại tấn công, Đội ứng cứu sự cố sẽ đặt câu hỏi liệu mã độc ransomware có tinh vi hay không và liệu nó có nhắm mục tiêu vào một tổ chức hoặc cá nhân cụ thể hay không.

Ngoài ra, phải xác định xem tác nhân đe dọa có được phê chuẩn hay hỗ trợ của một quốc gia nào hay không nếu có thể. Nếu xác định được rằng tác nhân đe dọa là một tổ chức có hậu thuẫn của nhà nước, Đội ứng cứu sự cố sẽ nêu vấn đề này với *[Nhập vị trí công việc liên quan cụ thể …]*.

Sau khi hoàn thành, hãy tiếp tục bước B1.12.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.12	Điều tra các CVE (Lỗ hổng Bảo mật Phổ biến) được sử dụng trong cuộc tấn công.	*[Nhập vị trí công việc liên quan cụ thể ...]*

Mô tả hành động

Nếu có thể, Đội ứng cứu sự cố sẽ xem xét tất cả thông tin thu thập được trong giai đoạn điều tra và xác định xem liệu CVE mới hay CVE hiện có đã bị sử dụng trong cuộc tấn công ransomware hay không.

Xem bảng dưới đây để biết các tài nguyên CVE được đề xuất:

Tài nguyên CVE đáng tin cậy	URL
NIST	NVD - Home (nist.gov) https://nvd.nist.gov/
MITRE	CVE - CVE (mitre.org) https://cve.mitre.org/
NCSC	Reports & advisories - NCSC.GOV.UK https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories

Table 4: Tài nguyên CVE

Tài nguyên Bổ sung	URL
Offensive Security	Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers (exploit-db.com) https://www.exploit-db.com/
Trung tâm An toàn thông tin Úc ACSC	View all advisories https://www.cyber.gov.au/acsc/view-all-content/advisories
VulDB	Vulnerability Database https://vuldb.com/
Công cụ CVE ưa thích của Đội ứng cứu sự cố	[Nhập công cụ CVE ưa thích của Đội ứng cứu sự cố]

Bảng 5: Tài nguyên Bổ sung

Sau khi hoàn thành, hãy tiếp tục bước B1.13.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.13	Thuê Nhà cung cấp Bảo hiểm	*[Nhập vị trí công việc liên quan cụ thể ...]*

Mô tả hành động

Nếu có thể, Đội ứng cứu sự cố sẽ làm việc với đơn vị bị ảnh hưởng để liên hệ với nhà cung cấp bảo hiểm có liên quan nhằm thảo luận về các lựa chọn bảo hiểm.

Đội ứng cứu sự cố và đơn vị bị ảnh hưởng sẽ điều tra:

1. Chính sách bảo hiểm an toàn mạng bao gồm những gì?
2. Chính sách bảo hiểm an toàn mạng có chi trả chi phí phục hồi sau sự cố mạng hay không?
3. Có bị trường hợp loại trừ nào có thể áp dụng cho sự cố ransomware không?

Sau khi hoàn thành, hãy tiếp tục bước B1.14.

#	Nhiệm vụ	Người chịu trách nhiệm:
B1.14	Cập nhật Thẻ (ticket) Sự cố	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Cập nhật thẻ sự cố với tất cả thông tin thu thập được trong suốt giai đoạn điều tra này, sử dụng [nhập công cụ quản lý /thẻ dịch vụ và các hướng dẫn cách truy cập công cụ/thẻ].

Thẻ sự cố nên được phổ biến cho các bên liên quan, bao gồm:

- [Nhập thông tin liên hệ của các bên liên quan bao gồm nhóm bảo mật nội bộ, khách hàng bị ảnh hưởng, các nhóm nội bộ để khắc phục/tư vấn]

Sau khi hoàn thành, hãy tiếp tục đến phần Ngăn chặn và Loại bỏ.

Bảng 6: Quy trình Điều tra

5 Ngăn chặn

Mục tiêu chính của giai đoạn ngăn chặn là hạn chế mở rộng tác động của sự cố và thiệt hại hoặc mất mát tiềm tàng do sự cố gây ra, cũng như cung cấp thời gian để loại bỏ và khôi phục. Các hoạt động ngăn chặn được tiếp theo sau đánh giá tác động của sự cố từ giai đoạn điều tra.

Ngăn chặn chủ yếu tập trung vào việc bảo vệ các điểm bị tấn công để chúng không bị kẻ tấn công lợi dụng để xâm phạm thêm. Việc quan trọng là giai đoạn này cũng gồm việc thông báo cho các bên liên quan trong tổ chức về sự cố để nâng cao nhận thức và ngăn chặn sự xâm nhập thêm.

Xem chi tiết về giai đoạn ngăn chặn trong bảng dưới đây.

<table>
<tr><th colspan="2">Hành động</th><th>Mô tả</th></tr>
<tr><td colspan="2">Ngăn chặn Sự cố</td><td>Đội ứng cứu sự cố ngăn chặn sự cố ransomware.</td></tr>
<tr><td>#</td><td>Nhiệm vụ</td><td>Người chịu trách nhiệm:</td></tr>
<tr><td>B2.01</td><td>Xác nhận việc cô lập</td><td>[Nhập vị trí công việc liên quan cụ thể …]</td></tr>
<tr><td colspan="3">Mô tả hành động</td></tr>
<tr><td colspan="3">Đội ứng cứu sự cố sẽ tham khảo Bảng 3: Quy trình Cô lập Ngay lập tức và xác nhận sự cô lập sự cố ransomware. Đội ứng cứu sự cố sẽ sử dụng thông tin thu thập được trong quá trình điều tra để xác định nhu cầu đối với các biện pháp ngăn chặn thêm.

Nếu không thành công, Đội ứng cứu sự cố sẽ tham khảo B3.01.

Sau khi hoàn thành, hãy tiếp tục bước B2.02.</td></tr>
<tr><td>#</td><td>Nhiệm vụ</td><td>Người chịu trách nhiệm:</td></tr>
<tr><td>B2.02</td><td>Thiết đặt lại truy cập</td><td>[Nhập vị trí công việc liên quan cụ thể …]</td></tr>
<tr><td colspan="3">Mô tả hành động</td></tr>
<tr><td colspan="3">Để ngăn chặn tác động của các xâm phạm tài khoản, Đội ứng cứu sự cố sẽ bắt đầu bằng cách đặt lại (các) tài khoản bị xâm phạm bằng thông tin đăng nhập mới. Quá trình này cũng có thể bao gồm xem xét các quyền quản trị.

Trong suốt quá trình này, nạn nhân sẽ giả định rằng các tài khoản dưới đây đã bị xâm nhập:
• Các thông tin đăng nhập thiết bị máy chủ.
• Các tài khoản lưu trữ trên đám mây.
• Các tài khoản email.
• Các tài khoản ngân hàng.
• Các tài khoản doanh nghiệp.

Điều quan trọng là quá trình này cũng sẽ liên quan đến việc đăng xuất khỏi tất cả các phiên trên tất cả các thiết bị có liên quan, để hỗ trợ từ chối quyền truy cập đang có của tác nhân đe dọa.

Đội ứng cứu sự cố sẽ làm việc với (các) nạn nhân để điều tra them các xâm phạm tiềm tàng, do thông tin đăng nhập có thể đã bị đánh cắp, bao gồm nhưng không giới hạn ở:
• Các tài khoản làm việc và tài khoản cá nhân.
• Các thông tin đăng nhập khác được lưu trong môi trường bị xâm phạm.
• Thông tin Nhận dạng Cá nhân có sẵn có thể bị lợi dụng để xâm phạm thêm.</td></tr>
</table>

Nếu chưa có, nên kích hoạch xác thực đa yếu tố. Sau đó, Đội ứng cứu sự cố sẽ:

- Thiết đặt lại mật khẩu KRBTGT hai lần. (KRBTGT là tài khoản mặt định từ Microsoft Active Directory)
- Đặt lại tất cả các tài khoản đặc quyền.
- Nếu Tài khoản Quản trị tên Miền bị xâm phạm: khôi phục Active Directory từ bản sao lưu có trước khi bị xâm phạm.
    - Nếu bản sao lưu này chưa có, hãy cân nhắc xây dựng lại AD từ đầu
- Nếu có liên quan đến kiến trúc của khách hang: thu hồi và cấp lại tất cả các chứng chỉ.
- Nếu có liên quan: loại bỏ mọi tác vụ độc hại nào đã lên lịch.
- Xây dựng lại danh sách liên hệ, tư cách thành viên nhóm và quyền truy cập vào các tệp, nhóm hoặc hộp thư quan trọng.

Sau khi hoàn thành, hãy tiếp tục bước B2.03.

#	Nhiệm vụ	Người chịu trách nhiệm:
B2.03	Cân nhắc chuyển sang liên lạc dùng kênh riêng	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Đội ứng cứu sự cố sẽ xem xét chuyển sang kênh liên lạc riêng, là liên lạc khác với kênh chính thức.

Liên lạc kênh riêng có thể cần thiếtcần dự đoán rằng tác nhân đe dọa đã có quyền truy cập vào các kênh liên lạc của đơn vị. Liên lạc kênh triêngriêng sẽ cung cấp một phương thức liên lạc an toàn trong khi diễn ra quá trình ngăn chặn, điều tra, loại bỏ và khôi phục.

Hãy xem xét những điều sau đây khi quyết định xem có cần liên lạc kênh riêng hay không:

- Có nghi ngờ rằng tác nhân đe dọa đã xâm nhập hoặc truy cập các kênh liên lạc hay không?
- Có xác nhận được cách thức xâm nhập hay không?
    - Nếu được xác nhận, cách thức xâm nhập đó có được kết nối với bất kỳ kênh liên lạc nào không?

Xem bảng dưới đây để quyết định xem có cần liên lạc kênh riêng hay không.

Cân nhắc khi nào nên liên lạc ngoài kênh riêng	Considerations for when out-of-band communication is not recommended/ Cân nhắc khi nào không nên liên lạc kênh riêng
Một hoặc nhiều thiết bị/hệ thống bị ảnh hưởng đã kết nối và/hoặc liên quan đến các thiết bị bị ảnh hưởng.	Các cá nhân đã kết nối và/hoặc liên quan đến thiết bị bị ảnh hưởng.
Cách thức xâm nhập không rõ.	Đã biết cách thức xâm phạm không kết nối với các kênh liên lạc.

Có bằng chứng về trích xuất dữ liệu.	Không có bằng chứng về di chuyển ngang (lateral movement) sang các hệ thống và/hoặc mạng.

Bảng 7: Cân nhắc về liên lạc kênh riêng

Sau khi hoàn thành, hãy tiếp tục bước B2.04.

#	Nhiệm vụ	Người chịu trách nhiệm:
B2.04	Liên hệ với các bên liên quan	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Nếu có thể, Đội ứng cứu sự cố sẽ thông báo cho nhân viên có liên quan của đơn vị về gián đoạn dự kiến và các hướng dẫn cho họ.

Đội ứng cứu sự cố cũng phải thông báo cho tất cả các đơn vị/cơ quan có liên quan trong nước theo yêu cầu của Luật An toàn thông tin mạng.

Xem Phụ lục D để có thể áp dụng theo mẫu thông báo đó. Sau khi hoàn thành, hãy tiếp tục bước B2.05.

#	Nhiệm vụ	Người chịu trách nhiệm:
B2.05	Xây dựng và triển khai chiến lược ngăn chặn	*[Nhập vị trí công việc liên quan cụ thể …]*

Mô tả hành động

Đội ứng cứu sự cố sẽ xây dựng một chiến lược ngăn chặn, xem xét các bước bên dưới (nếu phù hợp):

- Quy tắc tường lửa để chặn lưu lượng truy cập, ngăn chặn dựa trên các hàm băm của mã độc và làm vô hiệu các tài khoản liên quan. Xem xét các nội dung bên dưới:
  - Sự cần thiết bảo quản bằng chứng;
  - Tính khả dụng của dịch vụ (ví dụ: kết nối mạng, các dịch vụ được cung cấp cho các bên bên ngoài)
  - Thời gian và tài nguyên cần thiết để triển khai chiến lược;
  - Hiệu quả của chiến lược (ví dụ: ngăn chặn một phần, ngăn chặn toàn bộ);
  - Thời gian của giải pháp (ví dụ: yêu cầu ứng cứu sự cố trong vòng 48 giờ, giải pháp vĩnh viễn);
  - Kế hoạch phê duyệt các biện pháp ngăn chặn có thể gây gián đoạn để giảm thiểu thiệt hại.
  - Rủi ro gia tăng thêm nếu sự cố không được ngăn chặn ngay lập tức.

Dựa trên chiến lược ngăn chặn, Đội ứng cứu sự cố sẽ hoàn thiện việc ngăn chặn sự cố.

Sau khi hoàn thành, hãy tiếp tục bước B2.06.

#	Nhiệm vụ	Người chịu trách nhiệm:

B2.06	Bắt đầu tiến trình ra quyết định về tiền chuộc	*[Nhập vị trí công việc liên quan cụ thể …]*
Mô tả hành động		
Đội ứng cứu sự cố sẽ bắt đầu tiến trình xem xét thanh toán tiền chuộc ransomware. Tham khảo Phụ lục E hướng dẫn xem xét thanh toán tiền chuộc ransomware. Các cơ quan quản lý nhà nước không khuyến khích thanh toán tiền chuộc cho những kẻ tấn công ransomware và các quyết định cần phù hợp với từng hoàn cảnh.		

Table 8: Quy trình Ngăn chặn

6 Loại bỏ

Giai đoạn loại bỏ thực hiện sau khi một sự cố ransomware đã được điều tra và ngăn chặn (các) mối đe dọa. Mục tiêu chính của giai đoạn này là đảm bảo rằng sự cố đã được khắc phục, không còn tác nhân đe dọa nào có quyền truy cập, sự cố không lan rộng và các cách tấn công vào đã bị chặn.

Việc loại bỏ này cũng phải được xác thực để đảm bảo rằng nó đã thành công, thường là thông qua việc giám sát liên tục người dùng hoặc hệ thống bị ảnh hưởng để đảm bảo bất kỳ hoạt động bất thường/đáng ngờ nào đều được phát hiện và điều tra nhanh chóng.

Xem chi tiết về giai đoạn loại bỏ trong bảng dưới đây.

<table>
<tr><th colspan="2">Hành động</th><th>Mô tả</th></tr>
<tr><td colspan="2">Loại bỏ Sự cố</td><td>Đội ứng cứu sự cố loại bỏ sự cố ransomware.</td></tr>
<tr><th>#</th><th>Nhiệm vụ</th><th>Người chịu trách nhiệm:</th></tr>
<tr><td>B3.01</td><td>Xem xét việc bên thứ ba tham gia hỗ trợ</td><td>[Nhập vị trí công việc liên quan cụ thể …]</td></tr>
<tr><th colspan="3">Mô tả hành động</th></tr>
<tr><td colspan="3">Nếu nhà cung cấp bên thứ ba chưa được sử dụng, hãy xem xét lại yêu cầu hỗ trợ từ bên thứ ba dựa trên thông tin thu thập được trong giai đoạn điều tra và ngăn chặn.

Tham khảo Quy trình Ứng cứu sự cố an toàn thông tin mạng (CSIRP) trong dự án này để xác định xem Đội ứng cứu sự cố có khả năng loại bỏ và khôi phục hay không. Nếu chọn 'cách thức bên ngoài', tham khảo CSIRP khi xem xét về bên thứ ba.

Sau khi hoàn thành, hãy tiếp tục B3.02.</td></tr>
<tr><th>#</th><th>Nhiệm vụ</th><th>Người chịu trách nhiệm:</th></tr>
<tr><td>B3.02</td><td>Xây dựng và triển khai kế hoạch loại bỏ</td><td>[Nhập vị trí công việc liên quan cụ thể …]</td></tr>
<tr><th colspan="3">Mô tả hành động</th></tr>
<tr><td colspan="3">Đội ứng cứu sự cố sẽ xây dựng kế hoạch loại bỏ dựa trên thông tin thu thập được và ưu tiên các tài sản đã thiết lập trong các giai đoạn trước đó.

Đội ứng cứu sự cố sẽ kết hợp các kế hoạch để xác thực các hoạt động loại bỏ vào chiến lược, nhất là qua việc giám sát liên tục người dùng bị ảnh hưởng.

Sau khi hoàn thành, hãy tiếp tục B3.03.</td></tr>
<tr><th>#</th><th>Nhiệm vụ</th><th>Người chịu trách nhiệm:</th></tr>
<tr><td>B3.03</td><td>Cố bỏ qua màn hình khóa</td><td>[Nhập vị trí công việc liên quan cụ thể …]</td></tr>
<tr><th colspan="3">Mô tả hành động</th></tr>
</table>

Nếu (các) thiết bị máy tính/máy chủ bị khóa màn hình, Đội ứng cứu sự cố sẽ xem xét các phương pháp thay thế:

- Khởi động máy trong chế độ Safe Mode, sao cho máy vẫn có thể chạy phần mềm chống vi-rút (hoặc chạy thêm phần mềm chống vi-rút).
- Ngoài ra, hãy xem lại hướng dẫn dành riêng cho thiết bị từ nhà sản xuất để biết các cách thiết lập lại.

Sau khi hoàn thành, hãy tiếp tục đến phần Phục hồi.

Bảng 9: Quy trình Loại bỏ

7 Phục hồi

Giai đoạn phục hồi nhằm phục hồi và khôi phục từ sự cố, đồng thời xác định các nguyên nhân để cải tiến trong tương lai.

Xem bảng dưới đây để biết chi tiết về các bước liên quan đến phục hồi.

<table>
<tr><th colspan="2">Hành động</th><th>Mô tả</th></tr>
<tr><td colspan="2">Phục hồi Sự cố</td><td>Đội ứng cứu sự cố khôi phục sau sự cố ransomware.</td></tr>
<tr><th>#</th><th>Nhiệm vụ</th><th>Người chịu trách nhiệm:</th></tr>
<tr><td>B4.01</td><td>Khôi phục từ các bản sao lưu</td><td>[Nhập vị trí công việc liên quan cụ thể …]</td></tr>
<tr><td colspan="3">Mô tả hành động</td></tr>
<tr><td colspan="3">Đội ứng cứu sự cố sẽ làm việc với bộ phận bị hại để xác định khả năng khôi phục dữ liệu từ các bản sao lưu, gồm điều tra và xem xét những việc sau:
Bộ phận bị ảnh hưởng có các bản sao lưu để có thể khôi phục hay không?
Tần suất sao lưu và sự hoàn chỉnh của các bản sao như thế nào?
Các bản sao lưu này đã được xác minh chưa?
Các bản sao lưu này có được tách biệt khỏi mạng trong sự cố không?
Ngoài ra, Đội ứng cứu sự cố sẽ xem xét khoảng thời gian xảy ra ransomware nếu sự cố này xảy ra từ nhiều tháng trước, có khả năng các bản sao lưu có thể đã vô tình sao lưu các tệp được mã hóa. Nếu vậy, cần phải điều tra các bản sao lưu trước khi khôi phục.
Nếu có thể, Đội ứng cứu sự cố sẽ hỗ trợ đơn vị trong việc khôi phục từ bản sao lưu.
Sau khi hoàn thành, hãy tiếp tục bước B4.02.</td></tr>
<tr><th>#</th><th>Nhiệm vụ</th><th>Người chịu trách nhiệm:</th></tr>
<tr><td>B4.02</td><td>Tiến trình xem xét thanh toán tiền chuộc ransomware</td><td>[Nhập vị trí công việc liên quan cụ thể …]</td></tr>
<tr><td colspan="3">Mô tả hành động</td></tr>
<tr><td colspan="3">Nếu các giai đoạn Ngăn chặn, Loại bỏ và Phục hồi trong Sổ tay này không thể tiến hành khôi phục thành công và các bên thứ ba cũng không thể hỗ trợ, Đội ứng cứu sự cố sẽ xem xét việc thanh toán tiền chuộc ransomware.
Tham khảo Phụ lục E hướng dẫn xem xét thanh toán tiền chuộc ransomware.
Các cơ quan quản lý nhà nước không khuyến khích thanh toán tiền chuộc cho những kẻ tấn công ransomware, việc đưa ra quyết định tuỳ theo hoàn cảnh thực tế.
Sau khi hoàn thành, hãy tiếp tục bước B4.03.</td></tr>
</table>

#	Nhiệm vụ	Người chịu trách nhiệm:
B4.03	Khôi phục	*[Nhập vị trí công việc liên quan cụ thể …]*
Mô tả hành động		
Sau giai đoạn loại bỏ, Đội ứng cứu sự cố sẽ tiếp tục phần Phục hồi trong Kế hoạch ứng cứu sự cố CSIRP. Đội ứng cứu sự cố nên xác định những hành động phục hồi nào cần được thực hiện: • Bỏ ngăn chặn • Cập nhật Proxy • Cập nhật quy tắc Tường lửa • Kết nối lại các ổ đĩa dùng chung • Bật lại các liên kết sao lưu • Cho phép các kết nối mạng • Cập nhật EDR/AV • Xác thực các chính sách và định nghĩa Ngoài ra, Đội ứng cứu sự cố cũng sẽ tham khảo Cập nhật dành cho cấp Điều hành và xem xét Bài học Kinh nghiệm của Kế hoạch ứng cứu sự cố CSIRP.		

Bảng 10: Quy trình Khôi phục

Phụ lục A Điều tra Ransomware

Đội ứng cứu sự cố sẽ xem xét tổ chức có hay không các hệ thống phát hiện hoặc ngăn chặn. Nếu có sẵn, đội sẽ xem xét:

- Dữ liệu chống vi-rút.
- Thông tin Phát hiện và Ứng phó trên Endpoint.
- Thông tin Hệ thống Ngăn chặn Xâm nhập.
- Nhật ký hệ thống.

Các bước trên có thể cho phép đội ứng cứu sự cố khám phá các hệ thống khác đã bị nhiễm ransomware.

Đội ứng cứu sự cố sau đó sẽ điều tra:

- Những tệp nào đã bị mã hóa.
- Phần mở rộng tệp của các tệp bị mã hóa.
- Có bao nhiêu người dùng sẽ/đã bị ảnh hưởng.
- Bao nhiêu máy chủ đã bị ảnh hưởng.
- Mức độ nghiêm trọng của các hệ thống bị ảnh hưởng.

Sau đó, Đội ứng cứu sự cố sẽ tiến hành chụp ảnh hệ thống và bộ nhớ của các thiết bị bị nhiễm, tập trung vào kiểu xâm nhập đã biết và các máy chủ bị nhiễm ban đầu (nếu biết), tiếp theo là các máy chủ/mạng bị ảnh hưởng khác. Nếu có thể, quá trình này sẽ xem từ các tài sản và/hoặc hệ thống quan trọng nhất đến ít quan trọng nhất.

Thực hiện thu thập các thông tin cho điều tra forensic sau:

- Mọi nhật ký liên quan trước sự cố, bao gồm nhưng không giới hạn:
    - Nhật ký tường lửa.
    - Hành vi người dùng.
    - Bất kỳ nhật ký mạng nào khác.
- Nhật ký và dữ liệu Bảo mật Windows.
- Tệp ban đầu của mã độc.
- Các chỉ báo xâm phạm (IoC - Indicators of compromise).
- (Nếu có thể) (các) tệp thực thi đã khôi phục.
- Các mẫu tệp được mã hóa.
- Tập lệnh PowerShell.
- Bộ nhớ trực tiếp.
- Mọi tài khoản người dùng nào được tạo ra trong active directory.
- Địa chỉ email/số điện thoại/hồ sơ mạng xã hội được những kẻ tấn công sử dụng để phát động cuộc tấn công.

Trong suốt tất cả các bước trên, Đội ứng cứu sự cố cần cẩn thận bảo quản bằng chứng của tất cả các bước và các tiến trình để nó có thể đủ điều kiện tham gia vào các thủ tục pháp lý.

Phụ lục B Ví dụ các Thông báo tống tiền

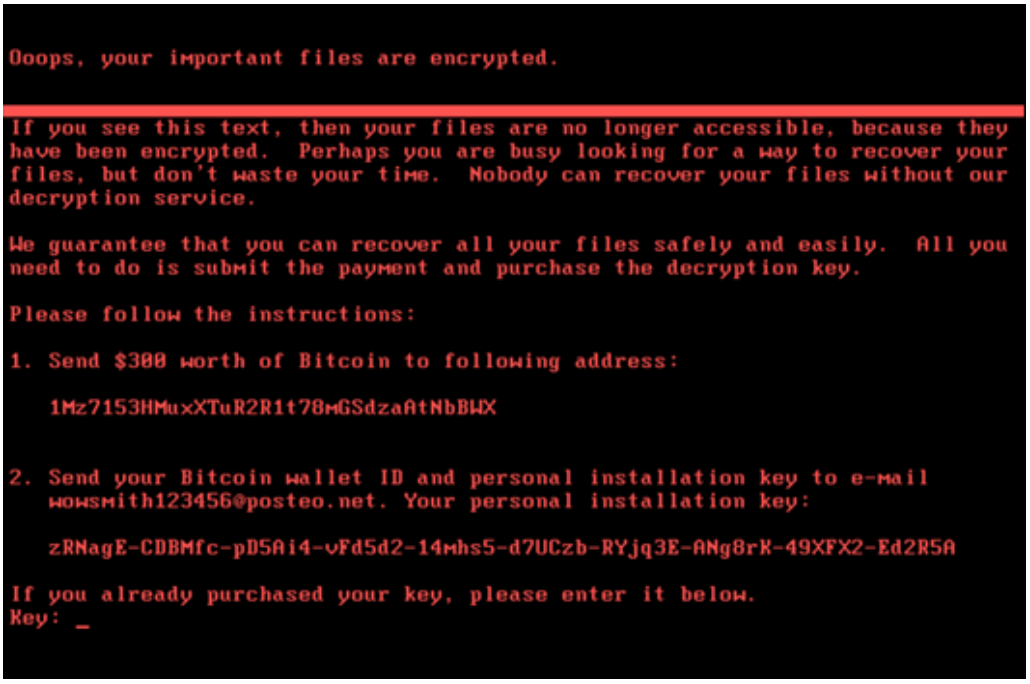
Xem các ví dụ dưới đây về thông báo tống tiền và các trang web cung cấp thông tin bị rò rỉ trên darkweb. Đội ứng cứu sự cố sẽ xem xét và so sánh các ví dụ dưới đây với sự cố ransomware, để xác định thông tin quan trọng về sự cố để điều tra thêm.

1: Thông báo tống tiền của Conti

```
All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.

To make sure that we REALLY CAN recover data - we offer you to decrypt samples.

You can contact us for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://[redacted].onion

HTTPS VERSION :
https://contirecovery.info

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready
 to publish it on out news website if you do not respond. So it will be better
 for both sides if you contact us ASAP.

---BEGIN ID---
7c85vpfYlRYHIA03SjFhX3oDfk2uTNlCQ8IROOMM33gL1FASiKPeodbG1K5YULtD
---END ID---
```

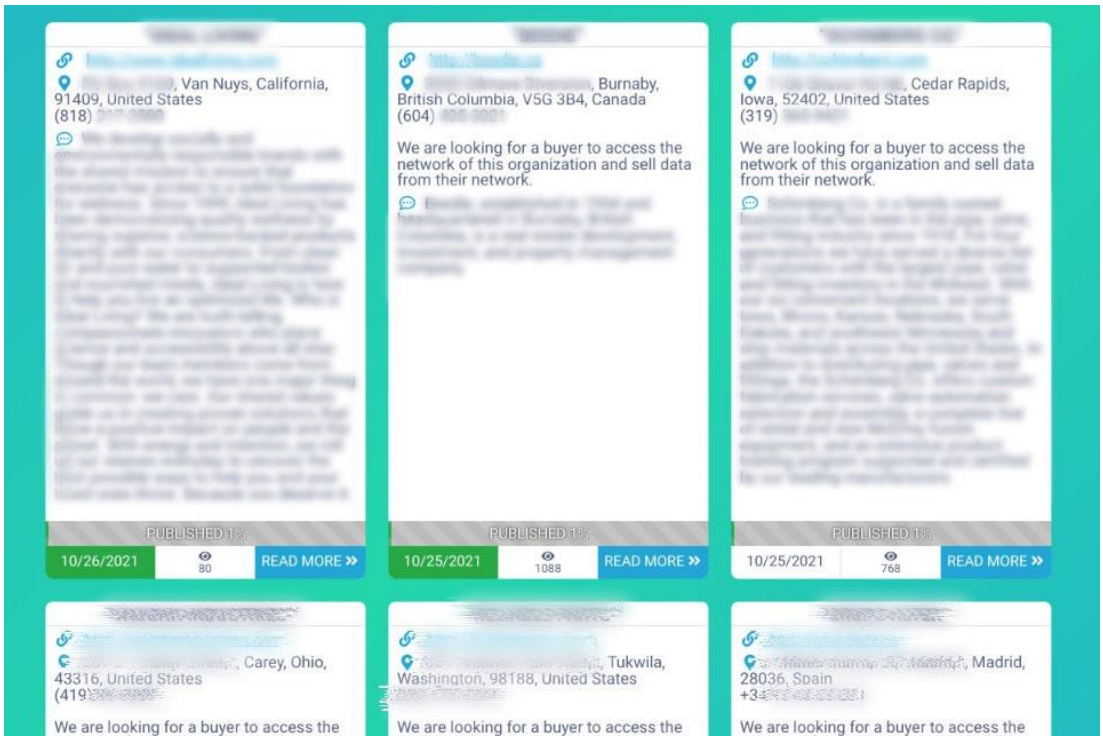
Hình 1: Thông báo của ransomware Conti

2: Thông báo Tống tiền của Peyta



Hình 2: Thông báo của ransomware Peyta

3: Trang web thông tin rò rỉ của Ransomware Conti



Hình 3: Trang web thông tin Rò rỉ của Ransomware Conti

4: Trang web rò rỉ thông tin của Ransomware Conti

Hình 4: Trang web Rò rỉ của Ransomware Conti

Phụ lục C Nghiên cứu các biến thể và tác nhân đe dọa ransomware

Đội ứng cứu sự cố sẽ điều tra biến thể ransomware thông qua nguồn giải mã dưới đây để xác định xem có tài nguyên hỗ trợ nào khả dụng hay không.

Nguồn giải mã	Mô tả
No More Ransom https://www.nomoreransom.org/en/index.html	No More Ransom là một trang web lưu trữ các công cụ giải mã đã biết cho các biến thể ransomware phổ biến. Dự án này là sáng kiến do Đơn vị Chống tội phạm công nghệ cao của Cảnh sát Hà Lan, Trung tâm tội phạm mạng châu Âu của Europol (Cảnh sát Châu Âu), Kaspersky và McAfee thành lập.

Bảng 11: Các nguồn giải mã

Ngoài ra, có thể các CERT quốc tế đã công bố tư vấn liên quan đến những biến thể ransomware cụ thể hoặc các nhóm ransomware. Đội ứng cứu sự cố có thể tham khảo các nguồn được liệt kê dưới đây.

Các nguồn từ các CERT/cơ quan an toàn thông tin quốc gia	Mô tả
Cơ quan an toàn thông tin và an toàn hạ tầng Hoa Kỳ CISA (Cybersecurity and Infrastructure Security Agency): https://www.cisa.gov/stopransomware/resources Trung tâm An toàn thông tin Úc ACSC (Australian Cyber Security Centre): https://www.cyber.gov.au/ransomware Trung tâm An toàn thông tin Vương quốc Anh NCSC UK (National Cyber Security Centre - UK): https://www.ncsc.gov.uk/ Trung tâm An toàn thông tin mạng Canada (Canadian Centre for Cyber Security): https://cyber.gc.ca/en Cục An toàn thông tin | Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam: https://ais.gov.vn/ | https://vncert.vn	Các cơ quan an toàn mạng của các quốc gia thường xuyên đăng các tư vấn và ấn phẩm chi tiết về các tác nhân đe doạ ransomware, có thể hỗ trợ trong việc ứng phó với tấn công ransomware.

Bảng 12: Nguồn Quốc tế

Phụ lục D Mẫu thông báo cho nhân viên

Bên dưới là một ví dụ về mẫu thông báo cho nhân viên, dùng song ngữ nếu cần thông báo cho các nhân viên người nước ngoài.

Staff notification template/ Mẫu thông báo cho nhân viên
From/Từ: *[Entity/Tên tổ chức]* To/Gửi đến: *[Insert relevant stakeholders/ Nhập tên các bên liên quan]* Subject/Tiêu đề: URGENT/KHẨN: *[Insert relevant subject line /Nhập đòng tiêu đề liên quan]* *Good morning/afternoon/evening,* *[Entity/Tổ chức] is contacting you to notify you of a cyber security (ransomware) incident / đang liên lạc với bạn để thông báo về một sự cố an toàn mạng loại ransomware.* *We were notified of the incident on / Chúng tôi đã được thông báo sự cố vào ngày [insert date/nhập ngày] at/lúc [insert time/nhập thời gian] by/bởi [if applicable, insert reporting source/nếu có thể, nhập nguồn báo cáo].* The declared incident is */ Sự cố được báo là [insert incident summary/nhập tóm tắt sự cố].* *The Incident response team is / Đội ứng cứu sự cố đang [insert current activities /nhập các hành động hiện tại].* *If any individuals or organisations associated attempt to make contact with you regarding ransom demands, do not engage with them and please notify [enter contact details] immediately. / Nếu bất kỳ cá nhân hoặc tổ chức nào liên quan cố gắng liên hệ với bạn yêu cầu đòi tiền chuộc, đừng tương tác với họ và vui lòng thông báo cho [nhập chi tiết liên hệ] ngay lập tức.* *[Include any instructions regarding engaging with media, how to continue with work and any other considerations / Bao gồm các hướng dẫn liên quan đến việc tương tác với giới truyền thông, cách tiếp tục công việc và các xem xét khác]* *We appreciate your cooperation / Chúng tôi cảm ơn sự hợp tác của bạn.* *Kind regards / Trân trọng,* *[Insert position title or name / Nhập chức danh hoặc tên người phát hành]*

Hình 3: Mẫu thông báo cho nhân viên

Phụ lục E Đàm phán Ransomware

Mặc dù quan điểm chung của các cơ quan quản lý nhà nước là không trả tiền chuộc liên quan đến đạo đức và pháp lý, nhưng vẫn có thể có những trường hợp cần thiết để tương tác với kẻ tấn công. Phụ lục này cung cấp một số cân nhắc trong việc tiến hành đàm phán với kẻ tấn công.

Đội ứng cứu sự cố sẽ làm việc với đơn vị bị ảnh hưởng để xem xét các lựa chọn dưới đây:

Lựa chọn	Ưu điểm	Nhược điểm
Không tương tác với kẻ tấn công	• Tiếp tục tuân thủ các yêu cầu pháp lý và quy định. • Giảm thiểu sự công khai về tiêu cực và tạo cơ hội để làm chủ diễn tiến. • Có thể giảm nguy cơ tăng chi phí bảo hiểm trong tương lai.	• Giảm cơ hội thu thập thêm thông tin về cuộc tấn công và kẻ tấn công. • Kẻ tấn công có thể tiết lộ thông tin hoặc thực hiện các hành động gây hại khác để tăng áp lực. • Tiếp tục gián đoạn hoạt động/kinh doanh.
Tương tác với kẻ tấn công nhưng không thanh toán	Cơ hội để: • Thu thập thông tin về các cách tấn công, tác động của tấn công và kẻ tấn công. • Tạm dừng bất kỳ hoạt động độc hại khác. • Đàm phán gia hạn thời hạn thanh toán. • Đàm phán giảm tiền chuộc.	• Đàm phán không thành công có nguy cơ làm khó chịu những kẻ tấn công. Điều này có thể hạn chế các lựa chọn đàm phán trong tương lai hoặc làm tăng khả năng hoạt động độc hại (bao gồm cả việc phát hành hoặc bán dữ liệu bị đánh cắp) của kẻ tấn công.
Tương tác với kẻ tấn công và xem xét đàm phán thanh toán	• Có thể tạo điều kiện cho việc nối lại các quy trình hoạt động / kinh doanh sớm hơn.	• Các cuộc đàm phán có thể không diễn ra nhanh chóng như mong đợi hoặc mong muốn. • Các công ty bảo hiểm có thể không chi trả tiền chuộc, khiếu nại, có thể ảnh hưởng đến chi

		phí trong tương lai hoặc khả năng đảm bảo bảo hiểm. • Không có gì đảm bảo rằng việc trả tiền chuộc sẽ dẫn đến kết quả mong muốn. Tiềm năng cho: • Công khai tiêu cực và tác động đến danh tiếng. • Khuyến khích các cuộc tấn công trong tương lai từ cùng một hoặc kẻ tấn công khác. • Thừa nhận pháp lý và đạo đức. • Sự can thiệp/kiểm toán theo quy định từ cơ quan quản lý.

Bảng 13: Ưu và nhược điểm của các lựa chọn tương tác với tác nhân Ransomware

Đội ứng cứu sự cố sẽ xem xét những việc sau:

Xem xét các Trụ cột	Cân nhắc các Câu hỏi
Đạo đức	• Xét đến hoàn cảnh cụ thể của sự cố ransomware thì liệu việc tương tác với nhóm ransomware có đạo đức hay không? • Sức khỏe, sự an toàn của nhân viên/khách hàng/công chúng có bị ảnh hưởng bởi sự cố ransomware không?
Kinh doanh và Kỹ thuật	• Dự kiến mất bao lâu để phục hồi? • Tổ chức có thể khôi phục hệ thống trong một khung thời gian hợp lý để hạn chế tối thiểu rủi ro đối với sức khỏe và an toàn, và sự gián đoạn hoạt động có thể chấp nhận được không? • Việc khôi phục dịch vụ có hiệu quả về chi phí và khả thi không?
Thông tin tình báo về Mối đe dọa	• Dựa trên những gì chúng ta biết về kẻ tấn công thông qua thông tin tình báo nội bộ và bên ngoài, liệu việc tương tác với kẻ tấn công và/hoặc thanh toán tiền chuộc có khả năng mang lại kết quả có ý nghĩa cho tổ chức không? • Dựa trên những gì chúng ta biết về (các) kẻ tấn công, khả năng (các) kẻ tấn công sẽ tôn trọng các thỏa thuận là gì? • Đặc biệt, kẻ tấn công có tiền sử rò rỉ dữ liệu sau khi thanh toán không?
Riêng tư và Dữ liệu	• Bản chất của dữ liệu bị xâm hại có thực sự cần phải tương tác với kẻ tấn công không?
Quy định và Danh tiếng	• Các tác động đến quy định từ cuộc tấn công ransomware đã được xem xét chưa? • Các tác động đến danh tiếng từ cuộc tấn công ransomware đã được lên kế hoạch chưa?

Pháp lý và Bảo hiểm	Công ty bảo hiểm của tổ chức có chi trả không? ○ Việc yêu cầu bồi thường có ngăn cản các yêu cầu trong tương lai không? ○ Công ty bảo hiểm có chấp thuận việc thanh toán không? ○ Công ty bảo hiểm có chi trả thiệt hại nếu tiền chuộc được trả và dữ liệu không được khôi phục không?

Bảng 14: Các cân nhắc khi Thanh toán Tiền chuộc Ransomware

Đội ứng cứu sự cố sẽ xem xét những điều sau đây trước khi bắt đầu liên lạc với (các) kẻ tấn công:

1. Đội ứng cứu sự cố có chuyên môn về đàm phán tiền chuộc không?
    - Nếu không, đã được tư vấn của chuyên gia đàm phán bên thứ ba chưa?
2. Thông tin nào nên được tìm kiếm từ (các) kẻ tấn công ransomware để xác định xem việc thanh toán tiền chuộc có phải là một lựa chọn phù hợp không?
    - Liệu kẻ tấn công ransomware có xem xét giảm số tiền không?
    - Liệu kẻ tấn công có chứng minh được rằng chúng có thể giải mã không?
    - Liệu kẻ tấn công có cung cấp bằng chứng về việc xóa dữ liệu không?
3. Thực hiện các bước điều tra sau đây đối với kẻ tấn công:
    - Liệu kẻ tấn công có đáng tin trong việc tôn trọng các thỏa thuận đòi tiền chuộc không?
    - Trước đó, kẻ tấn công đã bao giờ công bố dữ liệu sau khi nhận thanh toán chưa?
    - Việc thuê hoặc trả tiền cho kẻ tấn công có vi phạm bất kỳ nghĩa vụ pháp lý hoặc quy định nào không?
    - Kẻ tấn công có phải là tổ chức khủng bố không?

Đội ứng cứu sự cố sẽ làm việc với tổ chức để xem xét tất cả các cân nhắc trên và quyết định xem có nên tiếp tục hay không.

Nếu quyết định giao tiếp với kẻ tấn công, tổ chức nên thuê một nhóm đàm phán ransomware chuyên nghiệp của bên thứ ba.

Nếu quyết định không giao tiếp với kẻ tấn công, tổ chức nên thuê một bên thứ ba khi cần thiết để xây dựng lại và phục hồi.