Phân tích Toàn diện về Mã độc Tống tiền (Ransomware) và Chiến lược Ứng phó

Lời nói đầu

Mã độc tống tiền, hay Ransomware, là một loại phần mềm độc hại có chức năng mã hóa hoặc chặn truy cập vào dữ liệu cá nhân hay hệ thống máy tính của nạn nhân cho đến khi một khoản tiền chuộc được thanh toán.[1] Kẻ tấn công thường yêu cầu thanh toán bằng các loại tiền mã hóa khó truy vết như Bitcoin, gây khó khăn cho việc truy tìm và truy tố.[1]

Báo cáo này cung cấp một phân tích chuyên sâu về Ransomware, từ cơ chế hoạt động, lịch sử phát triển đến các xu hướng tấn công hiện đại. Phân tích cho thấy Ransomware đã phát triển từ một mối đe dọa ngẫu nhiên trở thành một mô hình tội phạm có tổ chức và thậm chí là một công cụ của chiến tranh mạng. Việc thiệt hại mà các nạn nhân của mã độc tống tiền phải gánh chịu dự kiến sẽ đạt 265 tỷ USD vào năm 2031.[3] Việc đối phó hiệu quả với mối đe dọa này đòi hỏi một chiến lược đa chiều, kết hợp giữa công nghệ, chính sách và yếu tố con người, không chỉ để khắc phục mà còn để phòng ngừa một cách chủ động.

Chương 1: Tổng quan về Mã độc Tống tiền (Ransomware)

1.1. Định nghĩa và Cơ chế Hoạt động

Ransomware là một loại phần mềm độc hại, sau khi lây nhiễm vào máy tính, sẽ mã hóa hoặc chặn truy cập dữ liệu trên đĩa, sau đó thông báo cho nạn nhân về khả năng khôi phục chúng, với điều kiện phải trả tiền chuộc.[4] Quá trình này thường bao gồm ba bước chính: xâm nhập, mã hóa và yêu cầu chuộc tiền.[5]

Có hai loại Ransomware chính được ghi nhận:

- **Locker Ransomware (Non-Encrypting Ransomware):** Loại này không mã hóa tệp tin mà thay vào đó khóa hoàn toàn quyền truy cập vào thiết bị.[7] Nạn nhân sẽ không thể thao tác được gì ngoài việc bật/tắt máy, và trên màn hình sẽ xuất hiện thông báo đòi tiền chuộc.[7]
- **Crypto Ransomware (Encrypting Ransomware):** Đây là loại phổ biến và nguy hiểm nhất. Chúng mã hóa các tệp tin dữ liệu quan trọng, đổi tên hoặc đuôi file, và đòi tiền chuộc để cung cấp khóa giải mã.[2] Các tệp gốc thường bị xóa sạch để ngăn nạn nhân tự khôi phục.[5]

Khi Ransomware xâm nhập, nó sẽ tự cài đặt trên thiết bị và lây lan đến các thiết bị mạng mà nó có thể truy cập.[4] Sau đó, mã độc sẽ bí mật kết nối với một máy chủ chỉ huy và kiểm soát (C&C server) do kẻ tấn công vận hành để tạo và nhận một khóa mã hóa.[2] Quá trình này đảm bảo rằng việc giải mã chỉ có thể thực hiện bằng khóa bí mật được lưu trữ trên máy chủ của tin tặc. Sau khi hoàn tất mã hóa, mã độc sẽ hiển thị một thông báo đòi tiền chuộc, thường kèm theo ID HOST và ID LOCK để nạn nhân có thể nhận diện và thực hiện thanh toán.[4]

1.2. Lịch sử Phát triển và các Chủng Ransomware Nổi bật

Lịch sử của Ransomware bắt đầu từ một cuộc tấn công tương đối thô sơ vào năm 1989, được biết đến là AIDS Trojan, lây nhiễm qua đĩa mềm và yêu cầu 189 USD tiền chuộc gửi qua đường bưu điện.[3] Sau hơn 30 năm, với sự phát triển của Internet và sự ra đời của tiền mã hóa, mã độc tống tiền đã trở nên tinh vi hơn rất nhiều, với quy mô và tác động tăng vọt, gây ra những thiệt hại kinh tế hàng tỷ đô la.[3]

Sự phát triển của Ransomware được thể hiện rõ qua các chủng mã độc nổi bật dưới đây, cho thấy sự thay đổi từ một mối đe dọa tài chính đơn thuần sang một công cụ hủy hoại với mục đích chính trị.

Chủng Ransomware	Năm xuất hiện	Véc-tơ lây nhiễm chính	Kỹ thuật nổi bật	Mục đích chính	Tác động
Petya	2016	Email giả mạo (phishing)	Mã hóa Master File Table (MFT)	Tài chính	Khóa toàn bộ ổ cứng.[10]

WannaCry	2017	Khai thác lỗ hổng EternalBlue	Lan truyền như một worm trong mạng nội bộ	Tài chính	Gây tê liệt hệ thống y tế và doanh nghiệp toàn cầu.[11]
NotPetya	2017	Khai thác lỗ hổng EternalBlue	Hủy hoại ổ cứng, xóa file gốc [2]	Hủy hoại (chính trị)	Gây gián đoạn chuỗi cung ứng toàn cầu, làm tê liệt các tập đoàn lớn.[12]

Phân tích NotPetya cho thấy một bước ngoặt đáng chú ý. NotPetya sử dụng cùng lỗ hổng EternalBlue như WannaCry để lan truyền tự động, nhưng Kaspersky đã đặt tên nó là "NotPetya" bởi vì nó có hành vi khác biệt so với Ransomware thông thường.[10] Mặc dù hiển thị thông báo đòi tiền chuộc, NotPetya dường như được thiết kế để hủy hoại dữ liệu hoàn toàn, với địa chỉ ví Bitcoin giả mạo khiến việc thanh toán là bất khả thi.[10] Việc một số quốc gia cáo buộc chính phủ Nga đứng sau cuộc tấn công này cho thấy mã độc tống tiền có thể được sử dụng với động cơ chính trị, vượt ra ngoài mục tiêu kiếm tiền thông thường.[10]

Chương 2: Phân tích Chuyên sâu về Kỹ thuật và Xu hướng Tấn công Hiện đại

2.1. Các Véc-tơ Lây nhiễm Phổ biến và Sự Nâng cấp của Tin tặc

Các cuộc tấn công Ransomware thành công thường không dựa vào kỹ thuật quá cao siêu mà lại tận dụng các điểm yếu đã được biết đến và sự thiếu cảnh giác của người dùng. Các phương thức lây nhiễm phổ biến nhất bao gồm:

- **Email lừa đảo (Phishing):** Đây là con đường lây nhiễm truyền thống và hiệu quả nhất.[4] Kẻ tấn công thường gửi email giả mạo với các tệp đính kèm độc hại, chẳng hạn như tài liệu Office có chứa macro hoặc các liên kết dẫn đến các trang web độc hại.[4]
- **Tấn công RDP (Remote Desktop Protocol):** Gần một phần ba các vụ tấn công Ransomware được phân phối thông qua các cuộc tấn công từ xa qua RDP.[4] Tin tặc

thường sử dụng các công cụ tự động để thực hiện tấn công vét cạn (brute-force), thử hàng triệu mật khẩu để chiếm quyền truy cập vào máy chủ.[4]

- **Khai thác lỗ hổng đã biết:** Đây là một phương thức lây nhiễm đặc biệt nguy hiểm. Các bản vá lỗ hổng thường được các nhà phát hành tung ra để khắc phục các điểm yếu bảo mật.[7] Tuy nhiên, nhiều tổ chức đã không cập nhật kịp thời, tạo ra "cánh cửa mở" cho tin tặc.[11] WannaCry là một ví dụ kinh điển về hậu quả của việc lơ là cập nhật bản vá. Mã độc này đã sử dụng lỗ hổng EternalBlue (CVE-2017-0144) trong giao thức SMBv1 của Windows để lây lan tự động trên toàn thế giới.[12] Mặc dù bản vá cho lỗ hổng này đã được Microsoft phát hành vài tháng trước đó, nhiều tổ chức vẫn chưa cài đặt, dẫn đến hơn 300,000 máy tính bị nhiễm.[10]

2.2. Kỹ thuật Mã hóa và Tạo Khóa

Sau khi xâm nhập, Ransomware sẽ bắt đầu mã hóa dữ liệu.[8] Hầu hết các chủng Ransomware hiện đại đều sử dụng một kỹ thuật phức tạp được gọi là mã hóa lai (hybrid encryption), kết hợp ưu điểm của cả hai thuật toán mã hóa đối xứng và bất đối xứng.

- **AES-128:** Đây là một thuật toán mã hóa đối xứng, được sử dụng để mã hóa các tệp tin quan trọng của nạn nhân. Thuật toán này có tốc độ xử lý rất cao, cho phép Ransomware mã hóa một lượng lớn dữ liệu trong thời gian ngắn.[14]
- **RSA-2048:** Đây là một thuật toán mã hóa bất đối xứng, sử dụng một cặp khóa công khai và khóa bí mật.[14] Ransomware sẽ sử dụng một khóa công khai để mã hóa khóa AES của mỗi nạn nhân. Khóa công khai này được chia sẻ rộng rãi, trong khi khóa bí mật tương ứng được lưu giữ an toàn trên máy chủ của kẻ tấn công.[14]

Quy trình này đảm bảo rằng việc khôi phục dữ liệu là bất khả thi nếu không có khóa bí mật duy nhất do kẻ tấn công nắm giữ.[14] Mặc dù trên lý thuyết, sau khi nạn nhân trả tiền chuộc, kẻ tấn công sẽ chuyển khóa giải mã, nhưng trên thực tế, không có sự đảm bảo nào, và nhiều tổ chức đã vĩnh viễn mất dữ liệu ngay cả khi đã thanh toán.[5]

2.3. Các Xu hướng Tấn công Mới và Đáng Chú ý

Thế giới tội phạm mạng đang không ngừng thay đổi và nâng cấp các chiến thuật tấn công.

- **Ransomware-as-a-Service (RaaS):** Đây là một mô hình kinh doanh cho phép các nhóm không chuyên về kỹ thuật cũng có thể thực hiện tấn công Ransomware.[6] Trong mô hình này, các nhà phát triển tạo ra mã độc và cung cấp nó cho các "đối tác," chia sẻ lợi nhuận

từ các khoản tiền chuộc. Các nhóm như LockBit và Medusa là những ví dụ điển hình hoạt động theo mô hình này.[6]

- **Tống tiền kép (Double Extortion) và Ba lớp (Triple Extortion):** Chiến thuật này vượt qua việc chỉ mã hóa dữ liệu.[18] Kẻ tấn công sẽ đánh cắp dữ liệu nhạy cảm trước khi mã hóa, sau đó đe dọa công khai thông tin này nếu nạn nhân không trả tiền chuộc.[19] Tấn công "tống tiền ba lớp" còn mở rộng áp lực sang các đối tác, khách hàng và chuỗi cung ứng, nhằm tạo ra những tác động lan rộng hơn.[19]
- **Vai trò của Trí tuệ Nhân tạo (AI):** AI đang được tội phạm mạng ứng dụng để tăng cường khả năng trinh sát, tự động hóa việc khai thác lỗ hổng và vượt qua các biện pháp phòng thủ truyền thống.[19] AI còn giúp kẻ tấn công tạo ra các chiến dịch lừa đảo được cá nhân hóa cao, thậm chí sử dụng công nghệ deepfake để giả mạo giọng nói của lãnh đạo nhằm đánh lừa nhân viên.[19]

Chương 3: Chiến lược Phòng ngừa và Bảo vệ Toàn diện

3.1. Tăng cường Nhận thức cho Người dùng

Các cuộc tấn công Ransomware thường thành công do khai thác lỗi con người.[6] Do đó, việc nâng cao nhận thức về an ninh mạng cho người dùng là tuyến phòng thủ quan trọng bậc nhất.[6] Các tổ chức cần tổ chức đào tạo định kỳ để nhân viên có thể nhận diện các email và liên kết đáng ngờ.[4] Các nguyên tắc cơ bản bao gồm: không mở email từ người gửi không quen biết, không nhấp vào các liên kết lạ và cẩn trọng với các tệp đính kèm yêu cầu bật macro.[4]

3.2. Các Biện pháp Phòng ngừa Kỹ thuật Chuyên sâu

Để xây dựng một hệ thống phòng thủ vững chắc, cần kết hợp nhiều biện pháp kỹ thuật khác nhau.

- **Sao lưu dữ liệu:** Đây được coi là tuyến phòng thủ cuối cùng và hiệu quả nhất khi đối mặt với Ransomware.[16] Các tổ chức nên tuân thủ
  Quy tắc sao lưu 3-2-1 [21]:
  - **3 bản sao:** Duy trì ba bản sao của dữ liệu quan trọng (một bản chính và hai bản sao lưu).[22]

    - **2 phương tiện lưu trữ khác nhau:** Lưu trữ các bản sao trên hai loại thiết bị khác nhau (ví dụ: ổ cứng ngoài và lưu trữ đám mây).[23]
    - **1 bản sao ngoại tuyến (offline/air-gapped):** Giữ ít nhất một bản sao lưu không kết nối với mạng.[23] Điều này là vô cùng quan trọng vì nhiều biến thể Ransomware hiện nay sẽ chủ động tìm và mã hóa luôn cả các bản sao lưu nối mạng.[21]

      Ngoài ra, việc định kỳ kiểm tra khả năng khôi phục từ bản sao lưu là bắt buộc, vì một bản sao lưu không được kiểm thử là "vô giá trị".21
- **Cập nhật hệ thống và vá lỗi:** Việc vá các lỗ hổng phần mềm ngay khi có bản cập nhật là một biện pháp thiết yếu để ngăn chặn Ransomware xâm nhập.[7] Việc chậm trễ cập nhật bản vá đã cho phép WannaCry lây lan trên quy mô lớn, gây ra hậu quả nghiêm trọng.[11]
- **Bảo mật truy cập và tài khoản:**
    - Thay đổi mật khẩu mặc định và sử dụng mật khẩu mạnh, độc đáo là điều kiện tiên quyết.[4]
    - Triển khai xác thực đa yếu tố (MFA) cho tất cả các dịch vụ quan trọng như email và VPN để thêm một lớp bảo mật quan trọng.[4]
    - Hạn chế việc sử dụng các dịch vụ truy cập từ xa như RDP.[11] Nếu cần thiết, hãy đặt RDP sau VPN và bật MFA cho các tài khoản quản trị.[21]
- **Bảo mật Mạng và Thiết bị:**
    - **Phân vùng mạng (network segmentation):** Chia mạng thành các khu vực riêng biệt để hạn chế sự lây lan của mã độc trong mạng nội bộ.[12]
    - **Sử dụng các giải pháp bảo mật hiện đại:** Đầu tư vào các giải pháp diệt virus thế hệ mới (Next-Generation Antivirus - NGAV) thay vì chỉ dựa vào các giải pháp truyền thống sử dụng signature đã lỗi thời.[25]
    - **Lọc email và web:** Sử dụng các bộ lọc email thông minh (chẳng hạn như Spam GUARD) và công nghệ lọc web để ngăn chặn các tệp tin độc hại xâm nhập vào hệ thống.[16]
    - **Áp dụng nguyên tắc đặc quyền tối thiểu (Least Privilege):** Cấp cho người dùng và hệ thống những đặc quyền tối thiểu cần thiết để thực hiện công việc của họ, từ đó giảm thiểu khả năng bị tấn công và hạn chế lây lan.[24]

Chương 4: Nhận biết và Phản ứng ban đầu

4.1. Các Dấu hiệu nhận biết Hệ thống bị Lây nhiễm

Các dấu hiệu nhận biết một cuộc tấn công Ransomware có thể rất tinh vi, nhưng thường có thể phát hiện qua một số bất thường sau:

- **Hiệu suất máy tính giảm sút bất thường:** Hệ thống phản ứng chậm, các chương trình khởi động lâu, và CPU sử dụng ở mức 100% dù không chạy nhiều ứng dụng nặng.[27]
- **Đèn LED ổ cứng nhấp nháy liên tục:** Đèn báo hiệu hoạt động của ổ cứng sáng lên bất thường hoặc nhấp nháy liên tục, cho thấy ổ cứng đang hoạt động quá mức để mã hóa dữ liệu.[27]
- **Tệp tin và đuôi file bị thay đổi:** Xuất hiện các tệp tin lạ hoặc các tệp tin quan trọng bị đổi tên hoặc đuôi file thành các ký tự lạ.[2]
- **Phần mềm diệt virus bị vô hiệu hóa:** Nhiều loại mã độc hiện đại có khả năng tắt hoặc vô hiệu hóa các phần mềm bảo mật để ngăn cản việc bị phát hiện và gỡ bỏ.[28]

4.2. Các Bước Sơ cứu Khẩn cấp (Incident Response)

Khi phát hiện một trong các dấu hiệu trên, tốc độ phản ứng là yếu tố quyết định để hạn chế thiệt hại.[29]

- **Bước 1: Cô lập thiết bị:** Ngay lập tức ngắt kết nối máy tính bị nhiễm khỏi mạng nội bộ (rút dây mạng, tắt Wi-Fi) để ngăn chặn mã độc lây lan sang các thiết bị khác hoặc các bản sao lưu nối mạng.[14]
- **Bước 2: Ủy quyền và thông báo:** Ủy quyền cho nhân viên IT hoặc an ninh thông tin thực hiện các biện pháp ngăn chặn khẩn cấp mà không cần tuân theo quy trình ủy quyền thông thường.[29] Sau đó, chủ động liên hệ với các chuyên gia bên ngoài, các đơn vị ứng cứu khẩn cấp về an ninh mạng và các cơ quan chức năng có thẩm quyền như Bộ Thông tin và Truyền thông, Bộ Công an để nhận được sự hỗ trợ.[29]
- **Bước 3: Đánh giá và ghi nhận:** Xác định loại Ransomware bằng cách sử dụng các công cụ trực tuyến như ID Ransomware [14] và đánh giá phạm vi thiệt hại của cuộc tấn công.[14]

4.3. Quan điểm về việc Trả Tiền Chuộc

Theo khuyến cáo của Cục An toàn thông tin (Bộ TT&TT Việt Nam) cũng như các cơ quan như FBI và CISA của Hoa Kỳ, các tổ chức và cá nhân **không nên trả tiền chuộc** cho hacker.[31] Có một số lý do quan trọng cho khuyến nghị này:

- **Không có sự đảm bảo:** Không có gì đảm bảo rằng sau khi thanh toán, kẻ tấn công sẽ cung cấp khóa giải mã hoặc dữ liệu sẽ được khôi phục.[5] Nhiều nạn nhân đã mất vĩnh viễn

quyền truy cập vào dữ liệu ngay cả sau khi trả tiền.[5]

- **Khuyến khích tội phạm:** Việc trả tiền chuộc khuyến khích tội phạm mạng tiếp tục thực hiện các cuộc tấn công tương tự, làm tăng thêm mức độ nghiêm trọng của vấn đề.[16]
- **Nguy cơ bị tấn công lại:** Khi một tổ chức trả tiền chuộc, nó sẽ bị đánh dấu là một mục tiêu "màu mỡ" và có nguy cơ cao bị tấn công lại trong tương lai.

Chương 5: Phục hồi Sau Tấn công và Khôi phục Dữ liệu

5.1. Khôi phục từ Bản sao lưu

Đây là phương pháp hiệu quả và an toàn nhất để khôi phục dữ liệu sau khi bị tấn công.[14] Các tổ chức cần sử dụng các bản sao lưu không bị ảnh hưởng, đặc biệt là các bản sao lưu ngoại tuyến (offline) để khôi phục hệ thống.[14] Trước khi tiến hành khôi phục, cần đảm bảo rằng các bản sao lưu đã được quét bằng phần mềm diệt malware để tránh việc nhiễm lại mã độc.[14]

5.2. Sử dụng Công cụ Giải mã Miễn phí

Trong một số trường hợp, các nhà nghiên cứu bảo mật có thể tìm ra lỗ hổng trong thuật toán của một chủng Ransomware cụ thể và phát triển các công cụ giải mã miễn phí.[14] Các công cụ này có thể giúp nạn nhân khôi phục dữ liệu mà không cần trả tiền chuộc. Một trong những nỗ lực hợp tác quốc tế lớn nhất trong lĩnh vực này là dự án

No More Ransom Project.[35] Dự án này là một sáng kiến phi lợi nhuận do các cơ quan thực thi pháp luật (như Europol) và các công ty an ninh mạng (như Kaspersky, McAfee) đồng sáng lập, cung cấp một kho lưu trữ 121 công cụ giải mã miễn phí, hỗ trợ hơn 151 họ Ransomware.[2]

Các công cụ này chỉ có hiệu quả đối với các chủng Ransomware đã được nghiên cứu và có công cụ giải mã sẵn.[32]

5.3. Các Phương pháp Khôi phục Dữ liệu Chuyên sâu

Trong trường hợp không có bản sao lưu ngoại tuyến và không có công cụ giải mã miễn phí, việc khôi phục dữ liệu sẽ cực kỳ phức tạp và tốn kém. Các phương pháp chuyên sâu thường yêu cầu sự can thiệp của các chuyên gia cứu dữ liệu và có thể bao gồm:

- **Sử dụng phần mềm khôi phục tệp tin:** Một số phần mềm khôi phục dữ liệu có thể tìm và khôi phục các tệp gốc đã bị Ransomware xóa, nhưng chưa bị ghi đè.[9]
- **Tái dựng cấu trúc hệ thống lưu trữ:** Đối với các hệ thống phức tạp như NAS/RAID, các chuyên gia có thể phải tiến hành imaging từng ổ cứng, tái dựng lại cấu trúc RAID một cách thủ công và phân tích dữ liệu thô để khôi phục các tệp tin quan trọng.[30] Quá trình này rất phức tạp và chỉ có thể thực hiện bởi các kỹ thuật viên có chuyên môn cao và công cụ chuyên dụng.[30]

Chương 6: Tổng kết và Khuyến nghị Chuyên sâu

Ransomware không còn là một mối đe dọa đơn lẻ mà đã trở thành một mô hình tội phạm có tổ chức và thậm chí là một công cụ của chiến tranh mạng. Phân tích này đã chỉ ra rằng các cuộc tấn công thường thành công không phải vì chúng quá tinh vi mà vì chúng lợi dụng sự thiếu cảnh giác của con người và sự lơ là trong việc cập nhật các biện pháp bảo mật cơ bản. Việc ứng phó hiệu quả đòi hỏi một chiến lược phòng thủ đa chiều, kết hợp chặt chẽ giữa công nghệ, chính sách và con người.

Dựa trên những phân tích trên, các khuyến nghị chiến lược được đưa ra như sau:

- **Đối với Cá nhân và Tổ chức nhỏ:**
  - **Thực hành an toàn trực tuyến:** Luôn cảnh giác với các email, liên kết và tệp đính kèm lạ.
  - **Sao lưu dữ liệu:** Thường xuyên sao lưu các tệp tin quan trọng và lưu trữ bản sao lưu ngoại tuyến hoặc trên đám mây an toàn.
  - **Cập nhật phần mềm:** Luôn cập nhật hệ điều hành, trình duyệt và các ứng dụng khác để vá các lỗ hổng bảo mật.
  - **Sử dụng MFA và mật khẩu mạnh:** Bật MFA cho tất cả các tài khoản quan trọng và sử dụng mật khẩu mạnh, độc đáo.
- **Đối với Tổ chức và Doanh nghiệp lớn:**
  - **Xây dựng văn hóa an ninh mạng:** Tổ chức các chương trình đào tạo nhận thức định kỳ cho toàn thể nhân viên, nhấn mạnh tầm quan trọng của việc tuân thủ các quy tắc an toàn thông tin.
  - **Triển khai chiến lược sao lưu 3-2-1:** Đây là tuyến phòng thủ tối thượng. Đảm bảo có ít nhất một bản sao lưu "air-gapped" không kết nối với mạng và kiểm thử định kỳ khả năng khôi phục từ bản sao lưu đó.

- **Quản lý bản vá lỗi nghiêm ngặt:** Thiết lập một quy trình tự động và chặt chẽ để rà quét và cập nhật các bản vá bảo mật cho tất cả các thiết bị và phần mềm trong hệ thống.
- **Nâng cao bảo mật hệ thống:** Áp dụng nguyên tắc đặc quyền tối thiểu, phân vùng mạng, sử dụng các giải pháp bảo mật thế hệ mới và giám sát liên tục để phát hiện sớm các hành vi xâm nhập.
- **Lập kế hoạch ứng phó sự cố:** Xây dựng một kế hoạch ứng phó chi tiết với các bước sơ cứu đã được ủy quyền trước, bao gồm việc cô lập ngay lập tức các thiết bị bị nhiễm và liên hệ với các chuyên gia hoặc cơ quan chức năng.

Nguồn trích dẫn

1. Ransomware, truy cập vào tháng 9 10, 2025, https://en.wikipedia.org/wiki/Ransomware
2. Ransomware là gì? Mức độ nguy hiểm và cách ngăn chặn, truy cập vào tháng 9 10, 2025, https://www.thegioididong.com/game-app/ransomware-la-gi-muc-do-nguy-hiem-va-cach-ngan-chan-1371507
3. 9 vụ tấn công ransomware lớn nhất lịch sử nhân loại - Trang chủ, truy cập vào tháng 9 10, 2025, https://daknong.gov.vn/chuyendoiso/9-vu-tan-cong-ransomware-lon-nhat-lich-su-nhan-loai-485071
4. Ransomware là gì? - Bitdefender Vietnam, truy cập vào tháng 9 10, 2025, https://www.bitdefender.vn/post/ransomware/
5. Mã độc tống tiền là gì? | Microsoft Security, truy cập vào tháng 9 10, 2025, https://www.microsoft.com/vi-vn/security/business/security-101/what-is-ransomware
6. Nhận thức là yếu tố quan trọng nhất trong phòng chống ransomware, truy cập vào tháng 9 10, 2025, https://ictvietnam.vn/nhan-thuc-la-yeu-to-quan-trong-nhat-trong-phong-chong-ransomware-64768.html
7. Gợi ý 3 cách phòng chống Ransomware hiệu quả mà người dùng không nên bỏ qua, truy cập vào tháng 9 10, 2025, https://viettelidc.com.vn/tin-tuc/goi-y-3-cach-phong-chong-ransomware-hieu-qua-ma-nguoi-dung-khong-nen-bo-qua-3014
8. Ransomware là gì? Những điều cần biết để phòng chống mã độc tống tiền, truy cập vào tháng 9 10, 2025, https://www.hpt.vn/tin-tuc/ransomware-la-gi-nhung-dieu-can-biet-de-phong-chong-ma-doc-tong-tien/9408
9. 3 cách cứu dữ liệu bị mã hóa bởi virus Ransomware - Bách khoa Data Recovery, truy cập vào tháng 9 10, 2025, https://recoverdata.com.vn/cuu-du-lieu/3-cach-cuu-du-lieu-bi-ma-hoa-boi-virus-ransomware/
10. What are Petya and NotPetya? | Ransomware attacks | Cloudflare, truy cập vào tháng 9 10, 2025,

https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/
11. 11 bước cần thực hiện để phòng chống ransomware, truy cập vào tháng 9 10, 2025, https://mst.gov.vn/11-buoc-can-thuc-hien-de-phong-chong-ransomware-197144312.htm
12. Ransomware Petya: Mã độc tống tiền nguy hiểm và cách bảo vệ doanh nghiệp - Viettel IDC, truy cập vào tháng 9 10, 2025, https://viettelidc.com.vn/tin-tuc/tu-bao-ve-may-tinh-truoc-ransomware-petya
13. EternalBlue Exploit Explained - AVG AntiVirus, truy cập vào tháng 9 10, 2025, https://www.avg.com/en/signal/eternal-blue
14. Phân tích cuộc tấn công mạng Ransomware trên cơ sở thuật toán mã hóa RSA và AES, truy cập vào tháng 9 10, 2025, https://baomoi.com/phan-tich-cuoc-tan-cong-mang-ransomware-tren-co-so-thuat-toan-ma-hoa-rsa-va-aes-c48964914.epi
15. Mã hóa RSA - Thuật toán mã hóa bất đối xứng mạnh mẽ - Viettel IDC, truy cập vào tháng 9 10, 2025, https://viettelidc.com.vn/tin-tuc/ma-hoa-rsa-thuat-toan-ma-hoa-bat-doi-xung
16. MỘT SỐ MẸO GIÚP PHÒNG CHỐNG RANSOMWARE KẾT LUẬN, truy cập vào tháng 9 10, 2025, https://www.unodc.org/roseap/uploads/documents/ransomaware/documents/30info_vietnamese.pdf
17. Xu hướng an ninh mạng 2025: Thách thức, mối đe dọa & giải pháp nổi bật - PACISOFT, truy cập vào tháng 9 10, 2025, https://www.pacisoft.vn/tin-san-pham/xu-huong-an-ninh-mang-2025-thach-thuc-moi-de-doa-giai-phap-noi-bat/
18. FBI cảnh báo nguy cơ tấn công mạng từ mã độc tống tiền Medusa, truy cập vào tháng 9 10, 2025, https://baomoi.com/fbi-canh-bao-nguy-co-tan-cong-mang-tu-ma-doc-tong-tien-medusa-c51726619.epi
19. Ransomware 2.0: AI đang thay đổi cách thức tấn công như thế nào?, truy cập vào tháng 9 10, 2025, https://ictvietnam.vn/ransomware-2-0-ai-dang-thay-doi-cach-thuc-tan-cong-nhu-the-nao-69370.html
20. 7 chiến lược chủ động chống các cuộc tấn công ransomware - vnetwork, truy cập vào tháng 9 10, 2025, https://www.vnetwork.vn/news/7-chien-luoc-chu-dong-chong-cac-cuoc-tan-cong-ransomware/
21. Ransomware là gì? 7 Chiến Lược Phòng Ngừa & Ứng Phó Hiệu Quả Bảo Vệ Doanh Nghiệp | CyberJutsu Academy, truy cập vào tháng 9 10, 2025, https://cyberjutsu.io/blog/ransomware-la-gi
22. Quy tắc sao lưu dữ liệu 3-2-1 là gì? Cách triển khai - Viettel IDC, truy cập vào tháng 9 10, 2025, https://viettelidc.com.vn/tin-tuc/quy-tac-sao-luu-du-lieu-3-2-1-la-gi
23. Quy tắc sao lưu dữ liệu 3-2-1: Chiến lược bảo vệ dữ liệu hiệu quả - Sunteco, truy

cập vào tháng 9 10, 2025, https://sunteco.vn/quy-tac-sao-luu-du-lieu-3-2-1/
24. 9 biện pháp cơ bản để phòng chống tấn công mã độc Ransomware - SafeGate, truy cập vào tháng 9 10, 2025, https://safegate.vn/vi/post/9-bien-phap-co-ban-de-phong-chong-tan-cong-ma-doc-ransomware-38.htm
25. Làm thế nào để bảo vệ tổ chức, doanh nghiệp trước các cuộc tấn công Ransomware?, truy cập vào tháng 9 10, 2025, https://vncs.vn/vi/tin-tuc/detail-lam-the-nao-de-bao-ve-to-chuc-doanh-nghiep-truoc-cac-cuoc-tan-cong-ransomware-334
26. Cách xử lý ransomware mã hóa dữ liệu qua hệ thống mail - vnetwork, truy cập vào tháng 9 10, 2025, https://www.vnetwork.vn/news/ransomware-ma-hoa-du-lieu-qua-he-thong-mail/
27. 5 dấu hiệu nhận biết máy tính Windows đang bị tấn công, truy cập vào tháng 9 10, 2025, https://www.hpt.vn/tin-tuc/5-dau-hieu-nhan-biet-may-tinh-windows-dang-bi-tan-cong/10541
28. Dấu hiệu cho thấy máy tính đang tải về malware - Viettel IDC, truy cập vào tháng 9 10, 2025, https://viettelidc.com.vn/tin-tuc/9-dau-hieu-cho-thay-may-tinh-dang-tai-ve-malware
29. Hướng dẫn biện pháp khắc phục sự cố khi bị tấn công ransomware - vnetwork, truy cập vào tháng 9 10, 2025, https://www.vnetwork.vn/news/huong-dan-bien-phap-khac-phuc-su-co-khi-bi-tan-cong-ransomware/
30. Khôi phục dữ liệu NAS bị ransomware, xóa LUN, mất Storage Pool – Có cứu được không?, truy cập vào tháng 9 10, 2025, https://cuudulieu24h.com/tin-tuc/khoi-phuc-du-lieu-nas-bi-ransomware-xoa-lun-storage-pool.html
31. Doanh nghiệp, tổ chức tài chính cần chủ động khắc phục sớm các cuộc tấn công mạng, truy cập vào tháng 9 10, 2025, https://thoibaotaichinhvietnam.vn/doanh-nghiep-to-chuc-tai-chinh-can-chu-dong-khac-phuc-som-cac-cuoc-tan-cong-mang-148488.html
32. Hướng dẫn khôi phục dữ liệu bị mã hóa bởi virus tống tiền - DVMS, truy cập vào tháng 9 10, 2025, https://dvms.com.vn/tin-tuc/tin-nganh/73728-huong-dan-khoi-phuc-du-lieu-bi-ma-hoa-boi-virus-tong-tien.html
33. CISA, FBI, and NSA Release Conti Ransomware Advisory to Help Organizations Reduce Risk of Attack, truy cập vào tháng 9 10, 2025, https://www.cisa.gov/news-events/news/cisa-fbi-and-nsa-release-conti-ransomware-advisory-help-organizations-reduce-risk-attack
34. No Ransom: Free ransomware file decryption tools by Kaspersky, truy cập vào tháng 9 10, 2025, https://noransom.kaspersky.com/
35. No More Ransom - The GFCE, truy cập vào tháng 9 10, 2025, https://thegfce.org/initiative/no-more-ransom/
36. No More Ransom - ECTEG, truy cập vào tháng 9 10, 2025,

https://www.ecteg.eu/nomoreransom/
37. Free Ransomware Decryption Tools | Unlock Your Files - AVG AntiVirus, truy cập vào tháng 9 10, 2025, https://www.avg.com/en-us/ransomware-decryption-tools