Báo cáo Phân tích Chuyên sâu: Các Hình thức Tấn công Mạng Phổ biến và Xu hướng Bảo mật Mới nổi trong Môi trường Kỹ thuật số

I. Tổng quan về Tấn công mạng và Bối cảnh An ninh mạng

1.1. Tấn công mạng là gì và Mục đích của Tin tặc

Tấn công mạng là hành vi cố ý xâm nhập, phá hoại, hoặc chiếm đoạt hệ thống máy tính, mạng lưới, và dữ liệu với mục đích xấu. Các cuộc tấn công này có thể được phân loại thành hai hình thức chính dựa trên quy mô và mục tiêu. Thứ nhất là **tấn công dựa trên hàng hóa (commodity-based attack)**, trong đó tội phạm mạng sử dụng các công cụ tự động để tấn công một nhóm lớn người dùng. Một ví dụ điển hình là việc gửi một email lừa đảo hàng loạt tới hàng triệu địa chỉ email. Kiểu tấn công này thường không nhắm đến một tổ chức cụ thể và kẻ tấn công sẽ không tiếp tục theo đuổi nếu nỗ lực ban đầu thất bại.[1]

Ngược lại, **tấn công do con người điều khiển (human-operated attack)** là các cuộc tấn công có chủ đích, được thực hiện bởi một hoặc một nhóm tội phạm mạng chuyên nghiệp. Chúng có thể khởi đầu bằng các phương thức ban đầu giống như tấn công hàng loạt, chẳng hạn như lừa đảo, nhưng sau đó có sự can thiệp trực tiếp vào hệ thống để gây tổn hại nghiêm trọng hơn. Kiểu tấn công này thường nhắm mục tiêu cụ thể vào các doanh nghiệp, tổ chức hoặc chính phủ và sử dụng nhiều phương pháp tinh vi hơn để duy trì quyền truy cập và gây ra thiệt hại.[1]

Động cơ đằng sau các cuộc tấn công này rất đa dạng, không chỉ giới hạn ở việc trục lợi tài chính. Các mục đích chính có thể bao gồm: **lợi nhuận tài chính**, thông qua việc đánh cắp

thông tin cá nhân, tài chính, tống tiền doanh nghiệp, hoặc hiển thị quảng cáo trái phép.[2] Ngoài ra, còn có các động cơ liên quan đến

cạnh tranh không lành mạnh, khi một tổ chức tấn công đối thủ để giành lợi thế trên thị trường. Các thế lực thù địch cũng có thể tấn công vì **mục đích chính trị hoặc tội phạm**, nhằm gây rối loạn, phá hoại hệ thống, hoặc đánh cắp thông tin nhạy cảm của một quốc gia. Cuối cùng, một số cá nhân thực hiện tấn công chỉ để **thỏa mãn mục đích cá nhân** như trả thù, hoặc đơn giản là để **thử sức và tò mò**, khám phá các lỗ hổng bảo mật và thể hiện kỹ năng của mình.[2]

Sự dịch chuyển từ tấn công hàng loạt sang tấn công có chủ đích cho thấy một sự thay đổi chiến lược từ phía tội phạm mạng. Lý do là các cuộc tấn công do con người điều khiển, mặc dù đòi hỏi nhiều công sức và nguồn lực hơn, nhưng mang lại lợi nhuận cao hơn đáng kể và gây ra hậu quả nghiêm trọng hơn cho nạn nhân. Sự thành công của các vụ tấn công này phụ thuộc vào khả năng nghiên cứu, lập kế hoạch và kiên trì của kẻ tấn công, biến mối đe dọa không còn chỉ đến từ các "script kiddies" hay botnet đơn giản, mà từ các nhóm tội phạm chuyên nghiệp và các thế lực nhà nước. Điều này đòi hỏi các tổ chức phải chuyển từ phòng thủ bị động sang chiến lược phòng thủ chủ động và thông minh hơn.

1.2. Bối cảnh An ninh mạng hiện nay tại Việt Nam và Thế giới

Tình hình an ninh mạng trên toàn cầu và tại Việt Nam đang chứng kiến sự gia tăng cả về tần suất và mức độ tinh vi của các cuộc tấn công. Theo báo cáo về an ninh mạng khu vực APAC trong tháng 1/2025, các mối đe dọa phổ biến nhất bao gồm **đánh cắp tài khoản và danh tính** (chiếm 40%), **tấn công DDoS** (chiếm 22%), và đặc biệt là **tấn công mã độc tống tiền** (tăng 70% so với tháng trước).[4] Các xu hướng này phản ánh sự ưu tiên của tin tặc đối với các cuộc tấn công mang lại lợi nhuận tài chính trực tiếp và khả năng gây gián đoạn hoạt động quy mô lớn.

Tại Việt Nam, các cơ quan chức năng đã đưa ra cảnh báo về ba xu hướng tấn công mạng nổi bật trong năm 2025, bao gồm: **tấn công mã độc tống tiền (ransomware)**, **tấn công có chủ đích APT (Advanced Persistent Threat)**, và **tấn công giả mạo, lừa đảo trực tuyến (phishing)**.[5] Các số liệu thực tế đã củng cố cảnh báo này, cho thấy một sự gia tăng đáng kể của mã độc tống tiền, với gần 60.000 cuộc tấn công ransomware nhắm vào Việt Nam.[7] Ngoài ra, các mục tiêu của tin tặc đang mở rộng sang các lĩnh vực mới như dịch vụ điện toán đám mây, chuỗi cung ứng, hệ thống ngôn ngữ lớn (LLM), ứng dụng trí tuệ nhân tạo (AI), các hệ thống điều khiển công nghiệp, xe tự hành, và máy bay không người lái (drone).[5]

II. Phân tích Chuyên sâu các Hình thức Tấn công Mạng Phổ biến

2.1. Tấn công Giả mạo (Phishing Attack)

Tấn công giả mạo là một trong những hình thức tấn công mạng phổ biến và nguy hiểm nhất hiện nay. Phishing là một chiến thuật kỹ thuật xã hội, trong đó kẻ tấn công giả mạo một đối tượng đáng tin cậy như ngân hàng, nhà cung cấp dịch vụ, hoặc một người quen để lừa dối người dùng, khiến họ tự nguyện cung cấp các thông tin nhạy cảm như tên đăng nhập, mật khẩu, hoặc thông tin thẻ tín dụng.[8]

Cơ chế hoạt động của một cuộc tấn công phishing diễn ra theo ba bước cơ bản. Đầu tiên, kẻ tấn công thực hiện việc **giả mạo (spoofing)** bằng cách tạo ra một email, tin nhắn văn bản, hoặc trang web có giao diện giống hệt bản gốc. Chẳng hạn, một email được thiết kế để trông giống như được gửi từ PayPal, hoặc một trang đăng nhập được sao chép y hệt trang web ngân hàng chính thống.[8] Tiếp theo là bước

lừa dối (deception). Nội dung lừa đảo thường tạo ra một cảm giác khẩn cấp hoặc đưa ra các lời mời hấp dẫn để khuyến khích nạn nhân hành động nhanh chóng mà không kịp suy nghĩ, ví dụ như thông báo về một giao dịch bất thường hoặc một chương trình khuyến mãi độc quyền.[9] Cuối cùng, khi nạn nhân tin tưởng và nhập thông tin vào trang web hoặc trả lời email giả mạo, kẻ tấn công sẽ thực hiện bước

chiếm đoạt (exfiltration), thu thập được dữ liệu cá nhân có giá trị của họ.[11]

Các biến thể của tấn công phishing đã phát triển ngày càng tinh vi. **Spear Phishing** là một hình thức tấn công có tính cá nhân hóa cao, nhắm vào một cá nhân hoặc một nhóm nhỏ cụ thể. Kẻ tấn công sẽ tiến hành nghiên cứu chi tiết về nạn nhân trên mạng xã hội hoặc các trang web công cộng để tạo ra các email hoặc tin nhắn giả mạo có độ tin cậy cực cao.[10] Một dạng đặc biệt của spear phishing là

Whaling, nhắm trực tiếp vào các lãnh đạo cấp cao của doanh nghiệp như Giám đốc điều hành (CEO).[10] Tấn công cũng có thể được thực hiện qua tin nhắn văn bản, gọi là

Smishing, trong khi **Social Media Phish** tận dụng các nền tảng mạng xã hội để lừa đảo.[8] Kẻ tấn công cũng có thể tạo ra các bản sao của trang web chính thống với các lỗi chính tả tinh vi trong URL hoặc sử dụng các ký tự tương tự từ các bảng mã khác để đánh lừa người dùng.[11]

Một biến thể khác là

Malware-based Phishing, sử dụng email lừa đảo để dụ nạn nhân mở các tệp đính kèm chứa mã độc hoặc ransomware.[8]

Sự tiến hóa của phishing là một minh chứng rõ nét cho sự chuyển dịch của tội phạm mạng từ việc khai thác các lỗ hổng kỹ thuật sang việc lợi dụng điểm yếu về con người. Tội phạm mạng nhận ra rằng việc lừa một người dùng thiếu cảnh giác để tự cung cấp thông tin hoặc cài đặt phần mềm độc hại dễ dàng và hiệu quả hơn rất nhiều so với việc vượt qua các lớp bảo mật công nghệ. Do đó, tấn công phishing không còn là một cuộc tấn công độc lập mà thường là bước đầu tiên trong một chuỗi tấn công phức tạp hơn, nhằm thu thập thông tin đăng nhập ban đầu để sau đó thực hiện các cuộc tấn công nghiêm trọng hơn như mã độc tống tiền hoặc đánh cắp dữ liệu quy mô lớn.

2.2. Mã độc Tống tiền (Ransomware)

Mã độc tống tiền là một loại phần mềm độc hại nguy hiểm được thiết kế để mã hóa hoặc khóa các tệp tin của nạn nhân, sau đó yêu cầu một khoản tiền chuộc để cung cấp khóa giải mã.[8] Khác với các loại virus máy tính thông thường chỉ nhằm phá hoại âm thầm, mục đích cuối cùng của ransomware không phải là phá hủy dữ liệu, mà là biến chính dữ liệu đó thành công cụ để tống tiền.[17] Cơ chế mã hóa của ransomware vô cùng phức tạp và tinh vi, giúp nó vượt qua nhiều rào cản của phần mềm diệt virus thông thường.[18]

Mô hình tấn công ransomware đã tiến hóa đáng kể trong những năm gần đây. Ban đầu, các cuộc tấn công chỉ dừng lại ở việc mã hóa dữ liệu đơn thuần. Tuy nhiên, khi các tổ chức bắt đầu sử dụng các bản sao lưu dữ liệu để phục hồi mà không cần trả tiền chuộc, tội phạm mạng đã phát triển mô hình **tống tiền kép (double extortion)**. Trong mô hình này, kẻ tấn công không chỉ mã hóa dữ liệu mà còn đánh cắp dữ liệu nhạy cảm, đe dọa sẽ công khai thông tin đó nếu nạn nhân không trả tiền.[17] Gần đây hơn, mô hình

tống tiền ba lần (triple extortion) đã xuất hiện, bao gồm cả việc thực hiện các cuộc tấn công DDoS vào hệ thống của nạn nhân hoặc liên hệ trực tiếp với khách hàng và đối tác để gây thêm áp lực, nhằm tối đa hóa khả năng nhận được tiền chuộc.[17]

Sự xuất hiện của mô hình kinh doanh **Ransomware-as-a-Service (RaaS)** đã làm giảm đáng kể rào cản kỹ thuật cho các tội phạm mạng, giúp số vụ tấn công tăng đột biến. Trong mô hình này, kẻ phát triển ransomware sẽ bán hoặc cho thuê mã độc cho các "đối tác," để họ tự thực hiện tấn công và chia lợi nhuận. Điều này khiến các cuộc tấn công ransomware ngày càng trở nên phổ biến và khó lường.[17]

Một cuộc tấn công ransomware điển hình thường diễn ra theo ba bước.[16]

Bước 1 là lây nhiễm, thường thông qua các phương thức kỹ thuật xã hội như email phishing, hoặc khai thác các lỗ hổng bảo mật chưa được vá trong hệ thống của nạn nhân. **Bước 2 là mã hóa**, khi ransomware xâm nhập, nó sẽ tìm kiếm và mã hóa các tệp tin quan trọng trên thiết bị hoặc hệ thống, khiến chúng không thể truy cập được.[20] Cuối cùng,

bước 3 là yêu cầu tiền chuộc, nạn nhân nhận được một thông báo yêu cầu thanh toán bằng tiền ảo (như Bitcoin) để đổi lấy khóa giải mã.[16]

Các vụ tấn công ransomware nổi bật như vụ tấn công vào công ty đường ống Colonial Pipeline (thủ phạm là băng đảng DarkSide RaaS) đã gây thiệt hại 4,4 triệu USD, hoặc vụ tấn công vào nhà sản xuất thịt bò JBS USA (thủ phạm là Revil RaaS) với số tiền chuộc lên tới 11 triệu USD, đã minh họa rõ rệt hậu quả và quy mô của các cuộc tấn công này.[19]

Tấn công ransomware không chỉ là một phần mềm độc hại đơn lẻ mà là một chiến dịch tội phạm phức tạp. Tội phạm mạng đã tối ưu hóa chuỗi tấn công của chúng: sử dụng phishing để lây nhiễm ban đầu, sau đó khai thác các lỗ hổng để lây lan, và cuối cùng sử dụng mô hình tống tiền đa cấp để tối đa hóa lợi nhuận. Do đó, để phòng chống hiệu quả, các tổ chức không thể chỉ dựa vào một phần mềm diệt virus duy nhất. Họ cần một chiến lược phòng thủ đa lớp (Defense-in-Depth) bao gồm cả các biện pháp kỹ thuật, quy trình quản lý, và nâng cao nhận thức của con người.

2.3. Tấn công Từ chối dịch vụ Phân tán (DDoS)

Tấn công từ chối dịch vụ phân tán (DDoS) là một hành vi làm quá tải một máy chủ, dịch vụ, hoặc tài nguyên mạng, khiến chúng không thể phục vụ người dùng hợp pháp.[2] Khác với tấn công DoS (Denial of Service) chỉ sử dụng một hoặc một số ít máy tính để làm quá tải hệ thống, DDoS sử dụng một mạng lưới lớn các máy tính đã bị chiếm quyền điều khiển, được gọi là

botnet, để đồng loạt gửi một lượng truy cập khổng lồ đến mục tiêu.[22]

Cơ chế hoạt động của một cuộc tấn công DDoS dựa trên ba thành phần chính: **kẻ chủ mưu (hacker)**, **mạng lưới máy tính ma (botnet)**, và **nạn nhân**.[21] Kẻ tấn công sẽ sử dụng các công cụ độc hại để chiếm quyền kiểm soát hàng nghìn, thậm chí hàng triệu máy tính hoặc thiết bị IoT, biến chúng thành một mạng lưới botnet. Sau đó, kẻ tấn công sẽ điều khiển mạng lưới này từ xa để đồng loạt tấn công một mục tiêu cụ thể, làm cạn kiệt tài nguyên của hệ thống và khiến nó không thể hoạt động bình thường.[14]

Tấn công DDoS có thể được phân loại theo kỹ thuật tấn công, bao gồm:

- **Tấn công băng thông (Volumetric Attacks):** Nhằm mục đích làm quá tải băng thông của mạng.
- **Tấn công giao thức (Protocol Attacks):** Tận dụng các lỗ hổng trong các giao thức mạng. Một số ví dụ phổ biến là tấn công **TCP SYN flood**, **Teardrop**, và **Ping-of-death**.[14]
- **Tấn công ứng dụng (Application Attacks):** Nhắm vào các lỗ hổng ở tầng ứng dụng, chẳng hạn như HTTP.[24]

Một điểm quan trọng cần lưu ý là DDoS không chỉ là một cuộc tấn công đơn lẻ mà thường là một chiến thuật trong một chiến dịch phức tạp. Tấn công DDoS có thể được sử dụng để làm gián đoạn hệ thống phòng thủ của nạn nhân, khiến họ phải tập trung toàn bộ nguồn lực vào việc xử lý lưu lượng truy cập lớn trong khi kẻ tấn công âm thầm thực hiện một cuộc tấn công khác. Ví dụ, một cuộc tấn công DDoS có thể được khởi chạy để làm sập hệ thống và sau đó kẻ tấn công sẽ tiến hành chiếm quyền điều khiển (hijacking) hoặc cài đặt mã độc vào hệ thống đang hỗn loạn đó.[2] Điều này cho thấy rằng việc phòng chống DDoS hiệu quả đòi hỏi các giải pháp chuyên biệt có khả năng phân tích và lọc lưu lượng truy cập ở nhiều tầng mạng, đồng thời cần có một kế hoạch ứng phó sự cố để đối phó với các cuộc tấn công thứ cấp.

2.4. Tấn công Xen giữa (Man-in-the-Middle - MitM)

Tấn công xen giữa, hay còn gọi là tấn công MitM, là một hình thức tấn công mà kẻ tấn công bí mật xen vào giữa hai bên (ví dụ: người dùng và một trang web) để nghe lén, chặn, hoặc thay đổi giao tiếp của họ.[1] Một cuộc tấn công MitM điển hình diễn ra theo hai giai đoạn:

chặn (interception) và **giải mã (decryption)**.[27] Giai đoạn đầu tiên, kẻ tấn công sẽ chen vào giữa người dùng và máy chủ thông qua các kỹ thuật như tạo điểm truy cập Wi-Fi giả mạo hoặc lợi dụng các mạng công cộng không an toàn.[27] Sau khi chặn được dữ liệu, kẻ tấn công sẽ giải mã thông tin để truy cập vào tài nguyên của nạn nhân và thực hiện các hành vi trục lợi.[27]

Các hình thức tấn công MitM phổ biến bao gồm:

- **Nghe lén Wi-Fi (Wi-Fi eavesdropping):** Kẻ tấn công thiết lập một kết nối Wi-Fi giả mạo với tên gọi đáng tin cậy ở các địa điểm công cộng để dụ người dùng kết nối. Sau khi nạn nhân kết nối, kẻ tấn công có thể theo dõi toàn bộ hoạt động trực tuyến và thu thập thông tin đăng nhập hoặc thông tin thẻ tín dụng.[25]
- **Giả mạo IP, DNS, HTTPS (Spoofing):** Kẻ tấn công thay đổi địa chỉ IP nguồn của trang web để lừa người dùng, hoặc tạo ra một trang web DNS giả mạo để chuyển hướng người dùng từ trang web gốc sang trang web giả mạo của chúng.[25] Trong tấn công giả mạo HTTPS, kẻ tấn công đánh lừa trình duyệt của nạn nhân tin rằng một trang web không an toàn là trang web an toàn, từ đó theo dõi và đánh cắp thông tin.[25]
- **Chiếm đoạt phiên (Session Hijacking):** Kẻ tấn công đánh cắp các thông tin được lưu

trữ trong cookie của trình duyệt như mật khẩu đã lưu, để thực hiện các hành vi trục lợi.[14]
- **Đánh cắp email (Email Hijacking):** Kẻ tấn công giả mạo email để theo dõi các giao dịch và đưa ra các hướng dẫn sai lệch, thường nhắm vào các giao dịch tài chính để chiếm đoạt tiền.[25]

Tấn công MitM không chỉ gây rủi ro về việc đánh cắp thông tin mà còn làm hỏng tính toàn vẹn của dữ liệu và niềm tin của người dùng. Bằng cách kiểm soát kênh giao tiếp, kẻ tấn công có thể thay đổi các tin nhắn hoặc dữ liệu đang được trao đổi mà hai bên không hề hay biết, mở ra khả năng gian lận tài chính ở mức độ tinh vi hơn.[28] Do đó, các giao thức mã hóa như SSL/TLS và việc sử dụng các mạng riêng ảo (VPN) trở nên thiết yếu, đặc biệt khi người dùng truy cập mạng ở các địa điểm công cộng.

III. Các Hình thức Tấn công Nâng cao và Xu hướng Mới nổi

3.1. Tấn công có chủ đích Nâng cao (APT)

Tấn công có chủ đích Nâng cao, hay APT, là một tập hợp các quy trình tấn công bí mật và liên tục, thường được thực hiện bởi một nhóm có tổ chức (thường được chính phủ tài trợ) nhắm vào một thực thể cụ thể.[5] Thuật ngữ này có ba đặc điểm chính:

"Nâng cao" (Advanced) vì nó sử dụng các kỹ thuật tinh vi và phần mềm độc hại tùy chỉnh để khai thác lỗ hổng. **"Liên tục" (Persistent)** vì kẻ tấn công duy trì sự kiểm soát hệ thống mục tiêu trong thời gian dài để liên tục theo dõi và lấy cắp dữ liệu. Cuối cùng là **"Mối đe dọa" (Threat)** vì nó thể hiện sự tham gia của con người trong việc dàn xếp và điều khiển cuộc tấn công, thay vì chỉ là các kịch bản tự động.[30] Các cuộc tấn công APT thường nhắm vào các tổ chức tư nhân, nhà nước, hoặc cả hai vì các động cơ kinh doanh hoặc chính trị.[30] Một ví dụ điển hình là vụ tấn công SolarWinds năm 2020, nơi tin tặc đã xâm nhập vào phần mềm cập nhật để theo dõi các cơ quan chính phủ và tập đoàn lớn như Microsoft và Intel.[1]

3.2. Tấn công Chuỗi cung ứng (Supply Chain Attack)

Tấn công chuỗi cung ứng là một trong những mối đe dọa nguy hiểm nhất hiện nay, trong đó kẻ tấn công xâm nhập vào một tổ chức bằng cách khai thác các lỗ hổng trong hệ thống của các nhà cung cấp hoặc dịch vụ bên thứ ba.[2] Cơ chế hoạt động là kẻ tấn công sẽ xâm nhập vào một nhà cung cấp đáng tin cậy, chèn mã độc vào phần mềm hoặc phần cứng của họ. Khi sản phẩm hoặc bản cập nhật phần mềm được phân phối, mã độc sẽ tự động lây lan sang tất cả các khách hàng của nhà cung cấp đó.[32] Hình thức tấn công này phản ánh một lỗ hổng bảo mật mang tính hệ thống. Các tổ chức thường đặt niềm tin vào các nhà cung cấp của mình, nhưng nếu một mắt xích trong chuỗi cung ứng bị tổn thương, nó có thể trở thành một cổng vào để kẻ tấn công xâm nhập vào toàn bộ hệ sinh thái khách hàng. Do đó, các tổ chức không chỉ cần áp dụng các tiêu chuẩn bảo mật nghiêm ngặt cho nội bộ mà còn cho toàn bộ các đối tác trong chuỗi cung ứng.

3.3. Tấn công vào các hệ thống AI, IoT và OT

Sự hội tụ của Trí tuệ nhân tạo (AI) và Internet vạn vật (IoT) đã tạo ra một xu hướng công nghệ mới được gọi là AIoT, nơi các thiết bị IoT không chỉ thu thập dữ liệu mà còn có khả năng phân tích và ra quyết định thông minh nhờ tích hợp AI.[33] Tuy nhiên, sự phổ biến của AIoT và các hệ thống công nghệ vận hành (OT) đã tạo ra các bề mặt tấn công mới mà tin tặc đang nhắm đến. Các mục tiêu hấp dẫn mới bao gồm các hệ thống điều khiển công nghiệp, xe tự hành, và máy bay không người lái (drone).[5] Việc bảo vệ các hệ thống này là vô cùng khó khăn, và một nghiên cứu cho thấy chỉ có khoảng 6% người dùng AI và 10% chủ sở hữu IoT tin rằng công ty của họ được bảo vệ hoàn toàn trước các cuộc tấn công.[34] Sự hội tụ của công nghệ thông tin (IT) và công nghệ vận hành (OT) đòi hỏi một sự chuyển đổi trong tư duy bảo mật. Các hệ thống OT/IoT có những đặc thù riêng, chẳng hạn như yêu cầu độ tin cậy và thời gian thực cao, do đó các giải pháp bảo mật truyền thống có thể không hiệu quả. Các tổ chức phải phát triển các chiến lược bảo mật chuyên biệt cho từng loại hệ thống, đồng thời tăng cường khả năng phục hồi và phát hiện sớm các mối đe dọa.

IV. Đối tượng Nạn nhân và Hậu quả Đa chiều

4.1. Phân loại Nạn nhân

Các cuộc tấn công mạng nhắm đến nhiều đối tượng khác nhau, từ cá nhân, doanh nghiệp đến các tổ chức chính phủ, thậm chí cả một quốc gia.[3]

Cá nhân thường là nạn nhân của các cuộc tấn công hàng loạt như phishing và drive-by download, với mục đích chính là đánh cắp thông tin tài chính, chiếm đoạt tài khoản mạng xã hội hoặc lấy cắp dữ liệu cá nhân.[10]

Doanh nghiệp là mục tiêu phổ biến nhất của các cuộc tấn công, vì lợi nhuận là động cơ chính của tội phạm mạng. Chúng nhắm vào dữ liệu tài chính, tài sản trí tuệ, danh sách khách hàng và thông tin nhận dạng cá nhân (PII).[3]

Chính phủ là mục tiêu của các cuộc tấn công có chủ đích, đặc biệt là các vụ tấn công APT, với động cơ chính trị hoặc gián điệp.[1]

4.2. Hậu quả của Tấn công mạng

Tấn công mạng gây ra nhiều hậu quả nghiêm trọng, vượt xa tổn thất tài chính trực tiếp.

- **Tổn thất Tài chính:** Các khoản tiền chuộc khổng lồ, chi phí phục hồi hệ thống, và các khoản bồi thường pháp lý. Ví dụ, nhà sản xuất thịt bò JBS USA đã phải trả 11 triệu USD tiền chuộc bằng Bitcoin, trong khi công ty Kronos phải trả 6 triệu USD để giải quyết một vụ kiện tập thể.[19]
- **Gián đoạn Hoạt động:** Tấn công có thể làm sập hệ thống, gây gián đoạn hoạt động sản xuất kinh doanh. Một vụ tấn công ransomware có thể gây gián đoạn trung bình 24 ngày hoạt động của công ty.[17]
- **Mất mát Dữ liệu:** Đánh cắp hoặc xóa bỏ dữ liệu nhạy cảm có thể dẫn đến hậu quả pháp lý nghiêm trọng.
- **Tổn hại Danh tiếng và Niềm tin:** Tấn công mạng có thể làm mất niềm tin của khách hàng và đối tác. Theo một báo cáo, 53% doanh nghiệp bị tấn công báo cáo hình ảnh công ty bị ảnh hưởng xấu, đặc biệt nếu dữ liệu khách hàng bị rò rỉ.[17]

V. Chiến lược Phòng chống và Ứng phó Toàn diện

5.1. Nâng cao Nhận thức và Đào tạo cho Nhân viên

Trong bất kỳ chiến lược bảo mật nào, yếu tố con người luôn được xem là mắt xích yếu nhất nhưng đồng thời cũng là lớp phòng thủ đầu tiên. Nhiều cuộc tấn công thành công đều bắt nguồn từ lỗi của con người, chẳng hạn như nhấp vào các liên kết độc hại trong email hoặc mở các tệp đính kèm chứa mã độc.[17] Nếu thiếu đào tạo, nhân viên có thể giấu sự cố khi phát hiện máy tính bị nhiễm virus, tạo điều kiện cho mã độc lây lan ra toàn bộ hệ thống. Do đó, việc đào tạo nhận thức an ninh mạng thường xuyên cho nhân viên là một trong những chiến lược phòng chống hiệu quả nhất. Các tổ chức cần xây dựng văn hóa "an ninh là trách nhiệm chung", khuyến khích nhân viên báo cáo sự cố sớm để đội ngũ phản ứng có thể kịp thời cô lập máy bị nhiễm và ngăn chặn sự lây lan.[17]

5.2. Biện pháp Phòng thủ Kỹ thuật Đa lớp (Defense-in-Depth)

Không có một giải pháp đơn lẻ nào có thể đảm bảo an toàn tuyệt đối trước các cuộc tấn công mạng. Một chiến lược phòng thủ đa lớp, kết hợp nhiều công nghệ và biện pháp khác nhau, là điều cần thiết.

- **Sao lưu dữ liệu theo quy tắc 3-2-1:** Để giảm thiểu thiệt hại từ ransomware, các tổ chức nên tuân thủ quy tắc 3-2-1: luôn giữ **3 bản sao** của dữ liệu, lưu trên **2 loại thiết bị lưu trữ khác nhau**, và có ít nhất **1 bản sao ngoại tuyến** (off-site backup) được ngắt kết nối vật lý với mạng để ransomware không thể mã hóa hoặc xóa.[17]
- **Vá lỗi và cập nhật hệ thống kịp thời:** Thường xuyên cập nhật các bản vá bảo mật là biện pháp thiết yếu để ngăn chặn tấn công, đặc biệt là các dịch vụ phơi bày ra Internet như VPN và RDP. Nhiều cuộc tấn công xảy ra đơn giản vì kẻ tấn công khai thác những lỗ hổng đã biết mà nạn nhân chưa kịp vá.[17]
- **Kiểm soát truy cập và Xác thực Đa yếu tố (MFA):** Áp dụng nguyên tắc "quyền tối thiểu" (Least Privilege) để mỗi nhân viên chỉ có quyền truy cập những gì cần thiết cho công việc. Đồng thời, bật xác thực đa yếu tố cho tất cả các tài khoản và dịch vụ quan trọng để tăng cường bảo mật.[17]
- **Phân đoạn mạng:** Chia nhỏ mạng thành các vùng để hạn chế khả năng lây lan của mã độc, nếu một phần của mạng bị tấn công, phần còn lại vẫn được bảo vệ.[17]
- **Sử dụng các công cụ bảo mật chuyên dụng:** Các tổ chức nên sử dụng tường lửa (Firewall), hệ thống ngăn chặn xâm nhập (IPS), và các giải pháp bảo vệ điểm cuối (EDR/XDR) để phát hiện và ngăn chặn các hành vi bất thường.[13]
- **Cảnh giác với mạng công cộng và sử dụng VPN:** Hạn chế truy cập các điểm Wi-Fi công cộng không được bảo vệ bằng mật khẩu. Khi thực hiện các giao dịch quan trọng, nên sử dụng mạng riêng ảo (VPN) để mã hóa dữ liệu truyền đi, tránh rủi ro bị tấn công MitM.[20]
- **Sử dụng dịch vụ chống DDoS chuyên dụng:** Đối với các hệ thống thường xuyên bị tấn

công DDoS, việc sử dụng các dịch vụ chuyên dụng như Cloudflare hoặc tường lửa ứng dụng web (WAF) là cần thiết để lọc và giảm thiểu lưu lượng truy cập độc hại trước khi chúng đến máy chủ.[21]

Phụ Lục

Bảng I: Tổng quan các Loại Tấn công Phổ biến

Loại tấn công	Mục tiêu chính	Phương thức tấn công phổ biến	Động cơ của tin tặc	Hậu quả chính
Giả mạo (Phishing)	Thông tin cá nhân, tài khoản, tài chính	Email, tin nhắn (Smishing), trang web giả mạo	Trục lợi tài chính, thu thập thông tin để tấn công tiếp theo	Đánh cắp danh tính, lộ dữ liệu, mất tiền
Mã độc tống tiền (Ransomware)	Dữ liệu, hệ thống	Lây nhiễm qua email, lỗ hổng chưa vá; mã hóa tệp tin	Tống tiền tài chính, trục lợi trực tiếp	Mất quyền truy cập dữ liệu, gián đoạn hoạt động, thiệt hại tài chính
Từ chối dịch vụ (DDoS)	Tính sẵn sàng của dịch vụ, máy chủ	Sử dụng botnet làm quá tải lưu lượng truy cập	Gây gián đoạn hoạt động, cạnh tranh không lành mạnh, mục đích chính trị	Dịch vụ ngừng hoạt động, tổn thất doanh thu và danh tiếng
Xen giữa (MitM)	Dữ liệu, phiên giao tiếp	Giả mạo Wi-Fi, DNS/IP spoofing,	Đánh cắp thông tin, gian	Rò rỉ dữ liệu, mất tính toàn vẹn của dữ

		chiếm đoạt cookie	lận tài chính	liệu, gian lận tài chính
Tấn công có chủ đích Nâng cao (APT)	Thông tin mật, gián điệp	Tấn công kéo dài, bí mật, sử dụng mã độc tùy chỉnh	Gián điệp, chính trị, cạnh tranh chiến lược	Lộ bí mật nhà nước, đánh cắp tài sản trí tuệ
Chèn mã SQL (SQL Injection)	Cơ sở dữ liệu	Chèn câu lệnh SQL độc hại vào các trường input	Đánh cắp, thay đổi hoặc xóa dữ liệu nhạy cảm	Lộ dữ liệu khách hàng, kiểm soát máy chủ cơ sở dữ liệu, gián đoạn hệ thống
Chèn tập lệnh trên nhiều trang web (XSS)	Dữ liệu người dùng, phiên làm việc	Chèn đoạn mã độc hại vào trang web	Chiếm đoạt phiên người dùng, thu thập thông tin nhạy cảm	Đánh cắp thông tin đăng nhập, mạo danh người dùng

Bảng II: Các Vụ Tấn công Ransomware Tiêu biểu

Tên vụ tấn công	Thủ phạm/Loại Ransomware	Thời gian	Thiệt hại ước tính	Nạn nhân
Colonial Pipeline	DarkSide RaaS	7/5/2021	4.4 triệu USD	Công ty đường ống dẫn dầu lớn nhất nước Mỹ
JBS USA	Revil RaaS	30/5/2021	11 triệu USD	Nhà sản xuất thịt bò lớn nhất thế giới
Costa Rica	Conti	17/4/2022	30 triệu	Các tổ chức

			USD/ngày	chính phủ của Costa Rica
Impresa	Lapsus$	1/1/2022	Không báo cáo	Tập đoàn truyền thông lớn nhất Bồ Đào Nha
Swissport	BlackCat RaaS	3/2/2022	Gián đoạn dịch vụ	Công ty dịch vụ hàng không Thụy Sĩ

Nguồn trích dẫn

1. Tấn công qua mạng là gì? | Microsoft Security, truy cập vào tháng 9 10, 2025, https://www.microsoft.com/vi-vn/security/business/security-101/what-is-a-cyberattack
2. Tấn công mạng là gì? Các loại tấn công mạng, ví dụ và biện pháp phòng chống toàn diện, truy cập vào tháng 9 10, 2025, https://vietnix.vn/tan-cong-mang-la-gi/
3. Toàn bộ kiến thức về Tấn Công Mạng (Cyber-attack) - CyStack, truy cập vào tháng 9 10, 2025, https://cystack.net/vi/blog/tan-cong-mang-cyber-attack
4. Báo Cáo An Ninh Mạng APAC Tháng 1/2025: Xu Hướng & Giải Pháp Bảo Mật, truy cập vào tháng 9 10, 2025, https://techhorizonvn.com/bao-cao-an-ninh-mang-apac-thang-1-2025-xu-huong-giai-phap-bao-mat.html
5. 3 xu hướng tấn công mạng nổi bật năm 2025 - LSVN, truy cập vào tháng 9 10, 2025, https://lsvn.vn/3-xu-huong-tan-cong-mang-noi-bat-nam-2025-a153329.html
6. An ninh mạng 6 tháng đầu năm 2025: Mã độc tống tiền vẫn là thách thức lớn, truy cập vào tháng 9 10, 2025, https://kinhtedothi.vn/an-ninh-mang-6-thang-dau-nam-2025-ma-doc-tong-tien-van-la-thach-thuc-lon.741233.html
7. Gần 60.000 cuộc tấn công mã độc tống tiền ransomware nhắm vào Việt Nam - Báo Tuổi Trẻ, truy cập vào tháng 9 10, 2025, https://tuoitre.vn/gan-60-000-cuoc-tan-cong-ma-doc-tong-tien-ransomware-nham-vao-viet-nam-20240427111410281.htm
8. [2025] Phishing là gì? | 10 Loại tấn công Phishing Nguy Hiểm, truy cập vào tháng 9 10, 2025, https://vinahost.vn/phishing-la-gi/
9. Top 6 hình thức tấn công mạng phổ biến năm 2020 - SecurityBox, truy cập vào tháng 9 10, 2025, https://securitybox.vn/3126/top-6-kieu-tan-cong-mang-pho-bien-2020/
10. PHISHING LÀ GÌ ? 5 LOẠI TẤN CÔNG PHISHING PHỔ BIẾN - Athena, truy cập vào tháng 9 10, 2025, https://athena.edu.vn/tan-cong-phishing-la-gi/

11. Tấn công giả mạo (bài viết) | Khan Academy, truy cập vào tháng 9 10, 2025, https://vi.khanacademy.org/college-careers-more/an-toan-internet/x8182d33f1114b84c:an-toan-internet/x8182d33f1114b84c:tim-hieu-nhan-biet-va-phong-tranh-lua-dao-tren-khong-gian-mang/a/phishing-attacks
12. Phishing là gì? Cách phòng chống tấn công Phishing hiệu quả - CyStack, truy cập vào tháng 9 10, 2025, https://cystack.net/vi/blog/phishing-la-gi
13. Tấn công Phishing là gì? Giải pháp chống Phishing - SecurityBox, truy cập vào tháng 9 10, 2025, https://securitybox.vn/1797/tan-cong-phishing-la-gi-giai-phap-chong-phishing/
14. Các hình thức tấn công mạng phổ biến hiện nay - VNTT, truy cập vào tháng 9 10, 2025, https://vntt.com.vn/cac-hinh-thuc-tan-cong-mang/
15. Bảo vệ PC của bạn chống lại mã độc tống tiền - Microsoft Support, truy cập vào tháng 9 10, 2025, https://support.microsoft.com/vi-vn/windows/b%E1%BA%A3o-v%E1%BB%87-pc-c%E1%BB%A7a-b%E1%BA%A1n-ch%E1%BB%91ng-l%E1%BA%A1i-m%C3%A3-%C4%91%E1%BB%99c-t%E1%BB%91ng-ti%E1%BB%81n-08ed68a7-939f-726c-7e84-a72ba92c01c3
16. Điểm danh 03 hình thức tấn công Ransomware nguy hiểm nhất hiện nay - vncs.vn, truy cập vào tháng 9 10, 2025, https://vncs.vn/vi/tin-tuc/detail-diem-danh-03-hinh-thuc-tan-cong-ransomware-nguy-hiem-nhat-hien-nay-332
17. Ransomware là gì? 7 Chiến Lược Phòng Ngừa & Ứng Phó Hiệu ..., truy cập vào tháng 9 10, 2025, https://cyberjutsu.io/blog/ransomware-la-gi
18. Ransomware là gì? Mức độ nguy hiểm và cách ngăn chặn - Thegioididong.com, 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
19. 9 vụ tấn công ransomware lớn nhất lịch sử nhân loại - VietNamNet, truy cập vào tháng 9 10, 2025, https://vietnamnet.vn/9-vu-tan-cong-ransomware-lon-nhat-lich-su-nhan-loai-2265046.html
20. Virus máy tính Ransomware là gì và cách ngăn chặn - vhieu store, truy cập vào tháng 9 10, 2025, https://vhieu.com/virus-may-tinh-ransomware-la-gi-va-cach-ngan-chan.html
21. Tấn công DDoS là gì? 7 Cách phòng chống DDos hiệu quả - VinaHost, truy cập vào tháng 9 10, 2025, https://vinahost.vn/ddos-la-gi/
22. DDoS là gì? Cách nhận biết và phòng chống hiệu quả tấn công từ chối dịch vụ DDoS, truy cập vào tháng 9 10, 2025, https://fptshop.com.vn/tin-tuc/danh-gia/ddos-la-gi-156213
23. Tấn công DDoS là gì? Đặc điểm nhận biết và cách ngăn chặn hiệu quả - FPT Smart Cloud, truy cập vào tháng 9 10, 2025, https://microsoft.fptcloud.com/kien-thuc/tan-cong-ddos/
24. Tấn công DDos: các loại tấn công và cách phòng ngừa - Viblo, truy cập vào tháng 9 10, 2025, https://viblo.asia/p/tan-cong-ddos-cac-loai-tan-cong-va-cach-phong-ngua-naQ

ZRAPjKvx
25. Tấn công Man-in-middle là gì? Cần phòng tránh Man-in-middle như thế nào? - Locker Password Manager, truy cập vào tháng 9 10, 2025, https://locker.io/vi/blog/tan-cong-man-in-middle-la-gi-va-phong-tranh-nhu-the-nao
26. Tấn công xen giữa – Wikipedia tiếng Việt, truy cập vào tháng 9 10, 2025, https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_xen_gi%E1%BB%AFa
27. Man in the middle là gì? Các hình thức tấn công & Cách Phòng, truy cập vào tháng 9 10, 2025, https://lanit.com.vn/man-in-the-middle-mitm-la-gi.html
28. Tấn công xen giữa (man-in-the-middle attack) là gì? - FUNiX, truy cập vào tháng 9 10, 2025, https://funix.edu.vn/chia-se-kien-thuc/tan-cong-xen-giua-man-in-the-middle-attack-la-gi/
29. Tìm hiểu về tấn công Man In The Middle và Cách phòng tránh - NTT SuperCare365, truy cập vào tháng 9 10, 2025, https://ntt-supercare365.com/man-in-the-middle-attack/
30. Advanced persistent threat – Wikipedia tiếng Việt, truy cập vào tháng 9 10, 2025, https://vi.wikipedia.org/wiki/Advanced_persistent_threat
31. Tấn công mạng là gì? 5 cách doanh nghiệp cần làm để tự bảo vệ - VNTT, truy cập vào tháng 9 10, 2025, https://vntt.com.vn/tan-cong-mang-la-gi-5-cach-doanh-nghiep-can-lam-de-tu-bao-ve/
32. Supply chain attack: Phòng tránh tấn công chuỗi cung ứng - CyStack, truy cập vào tháng 9 10, 2025, https://cystack.net/vi/tutorial/supply-chain-attack
33. AIoT là gì? Sự kết hợp giữa AI và IoT tạo nên xu hướng công nghệ - Base, truy cập vào tháng 9 10, 2025, https://base.vn/blog/aiot-la-gi/
34. AI và IoT phổ biến khiến chúng dễ bị xâm nhập bởi các phương thức tấn công mạng mới, truy cập vào tháng 9 10, 2025, https://www.sggp.org.vn/ai-va-iot-pho-bien-khien-chung-de-bi-xam-nhap-boi-cac-phuong-thuc-tan-cong-mang-moi-post731738.html