TẤN CÔNG APT VÀ GIẢI PHÁP PHÒNG CHỐNG TRONG GIÁO DỤC AN NINH MẠNG HIỆN NAY

Trịnh Thị Vân
Thạc sỹ, Khoa Công nghệ Thông tin, Trường Đại học Hạ Long

Tóm tắt: *Trong bối cảnh Cách mạng Công nghiệp 4.0, bảo vệ an ninh mạng ngày càng quan trọng hơn bao giờ hết, nhằm bảo vệ an ninh quốc gia, trật tự an toàn xã hội, xây dựng không gian mạng thực sự lành mạnh và an toàn. Để đảm bảo An toàn không gian mạng trong kỷ nguyên số, chúng ta cần phát huy sức mạnh tổng hợp và đồng bộ của các lực lượng, trong đó mỗi cá nhân có vai trò hết sức quan trọng. Không gian mạng ngày nay trở thành một không gian xã hội mới, nơi con người có thể thực hiện các hành vi giao tiếp, sáng tạo, lao động, sản xuất, tiêu dùng, học tập và vui chơi giải trí, không bị giới hạn bởi không gian và thời gian. Tuy nhiên, cùng với những lợi ích to lớn, không gian mạng đang tạo ra các nguy cơ và thách thức đối với an ninh quốc gia, an ninh con người và trật tự an toàn xã hội. Thời gian qua, không ít những vụ lừa đảo qua mạng gây ảnh hưởng xấu đến sức khỏe, danh dự, uy tín của tổ chức, cá nhân. Các cuộc tấn công này đều có mục đích cụ thể như: Lấy cắp dữ liệu, tống tiền, lừa đảo… Vì vậy, bài viết sẽ đưa ra các giải pháp phòng chống để hạn chế các thiệt hại nhất định từ các cuộc tấn công APT.*

Từ khoá: *APT; an ninh mạng; an toàn thông tin; tấn công có chủ đích; giáo dục an ninh mạng; phòng chống tấn công mạng.*

APT ATTACKS AND PREVENTION SOLUTIONS IN CURRENT CYBER SECURITY EDUCATION

Abstract: *In the context of the Fourth Industrial Revolution, cybersecurity is more important than ever to protect national security, social order and safety, and build a truly healthy and safe cyberspace. To ensure cybersecurity in the digital age, we need to leverage the combined and synchronized strength of various forces, in which each individual plays a crucial role. Today's cyberspace has become a new social space where people can engage in communication, creativity, work, production, consumption, learning, and entertainment without being limited by space and time. However, along with its immense benefits, cyberspace is creating risks and challenges to national security, human security, and social order and safety. In recent times, numerous online scams have negatively impacted the health, honor, and reputation of organizations and individuals. These attacks all have specific objectives such as: data theft, extortion, fraud, etc. Therefore, this article will present preventative solutions to minimize the damage from APT attacks.*

Keywords: *APT; cybersecurity; information security; targeted attacks; cybersecurity education; cyberattack prevention.*

Nhận bài: 29.12.2025 Phản biện: 21.01.2026 Duyệt đăng: 25.01.2026

I. ĐẶT VẤN ĐỀ

Mạng Internet ngày càng phát triển và phổ biến rộng khắp mọi nơi, lợi ích của nó rất lớn. Tuy nhiên cũng có rất nhiều ngoại tác không mong muốn đối với các cá nhân hay tổ chức, doanh nghiệp, cơ quan nhà nước,... như các trang Web không phù hợp với lứa tuổi, nhiệm vụ, lợi ích, đạo đức, pháp luật hoặc trao đổi thông tin bất lợi cho cá nhân, doanh nghiệp,... Năm 2024, trung tâm Giám sát an toàn không gian mạng đã phát hiện hơn 56.300 điểm yếu, lỗ hổng an toàn thông tin tại các hệ thống thông tin của cơ quan tổ chức nhà nước.

Hiện nay, môi trường mạng máy tính đang ngày một phát triển đi lên nhằm phục vụ các nhu cầu thiết yếu cho cuộc sống hằng ngày. Bên cạnh sự phát triển đó thì cũng có không ít những kẻ muốn lợi dụng những lỗ hổng từ môi trường mạng máy tính để đánh cắp thông tin và dùng chúng với những mục đích xấu. Cũng từ đó, thuật ngữ Advanced Persistent Threat - APT ra đời. Vậy APT là gì? Hiện nay tình trạng tấn công APT ở Việt Nam thế nào? Cách phòng chống ra sao? Bài viết dưới đây sẽ giải đáp những thắc mắc đó.

II. NỘI DUNG NGHIÊN CỨU

2.1. Khái niệm APT

Thuật ngữ APT (Advanced Persistent Threat) được sử dụng để mô tả kiểu tấn công dai dẳng và có chủ đích vào một thực thể được nhắm đến. APT là loại tấn công âm thầm, không phá hỏng file/máy tính. APT đã trở thành một mối quan tâm lớn cho các chuyên gia bảo mật trên toàn thế giới. Ngay từ đầu năm 2013, đã có một loạt danh sách nối dài những nạn nhân của loại tấn công này như Facebook, Twitter, …

Các thành phần của từ viết tắt APT:

Advanced (Nâng cao): Hacker sử dụng các kĩ thuật nâng cao để tấn công vào hệ thống mục tiêu một cách bài bản. Các tấn công APT phối kết hợp nhiều các kĩ thuật khác nhau một cách khoa học. Tính "Advanced" thể hiện ở khả năng ẩn mình, thay đổi liên tục khiến cho việc phát hiện trở nên rất khó khăn.

Persistent (Dai dẳng): Hacker xác định cụ thể mục tiêu cần khai thác để thực hiện việc tấn công, ẩn mình và khai thác theo từng giai đoạn. Sử dụng nhiều các kĩ thuật, phương pháp khác nhau để tấn công vào mục tiêu đến khi thành công.

Threat (Nguy cơ hay mối đe dọa): APT là một mối đe dọa bởi vì nó có tiềm lực và chủ đích. Các cuộc tấn công APT được thực hiện bởi các hoạt động kết hợp, có mục tiêu cụ thể và kẻ tấn công có kĩ năng, có tổ chức và có nguồn tài trợ dồi dào.

2.2. Các phương pháp phòng chống tấn công APT

2.2.1. Bảo mật theo lớp

Trong các chiến lược phòng chống và bảo vệ an ninh mạng, giải pháp bảo mật theo lớp hay còn gọi là phòng thủ kiên cố theo chiều sâu luôn được đưa vào sự ưu tiên hàng đầu. Phương pháp phòng chống tấn công APT này luôn mang lại hiệu quả rất cao.

Lý do là vì với giải pháp này, mạng nội bộ sẽ được bảo vệ triệt để thông qua một thiết bị tường lửa nhằm mục đích kiểm soát các điểm ra vào mạng, triển khai các hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS), hệ thống SIEM – hệ thống giám sát thông tin và sự cố bảo mật, bổ sung hệ thống quản lý và vá lỗ hổng, thực hiện bảo vệ đầu cuối, sử dụng các phương thức xác thực và quản lý danh tính truy cập một cách gắt gao nhưng chắc chắn.

Mục tiêu chính của việc sử dụng tường lửa bảo mật này nhằm làm cho việc xâm nhập vào mạng ban đầu trở nên khó khăn; nếu Hacker vượt qua, các lớp bảo mật bổ sung tiếp theo sẽ phải có mức trở ngại cao hơn, có thể ngăn cuộc tấn công lan rộng hoặc làm sự tiến triển của mã độc chậm lại đủ lâu để hệ thống mạng phát hiện và xử lý.

2.2.2. Sử dụng dịch vụ giám sát, đánh giá và phân tích mối đe dọa

Giám sát chặt chẽ việc kiểm soát an ninh giúp mạng nội bộ nhận diện sớm các dấu hiệu cảnh báo của một cuộc tấn công có chủ đích. Chúng thường xuất hiện dưới dạng File Log, các hoạt động bất thường hay các dạng lưu lượng dữ liệu có sự thay đổi bất thường.

Việc giám sát các thiết bị truy cập mạng, tất cả lưu lượng ra vào mạng, lưu lượng nội bộ là những điều hết sức quan trọng. Việc giám sát liên tục rất có ích trong việc phòng thủ và lên chiến lược tấn công cho các mối đe dọa.

2.2.3. Đào tạo và huấn luyện đội ngũ IT

Hầu hết các cuộc tấn công APT sử dụng kỹ thuật xã hội để đạt được một chỗ đứng ban đầu trong môi trường mạng của mục tiêu. Spear phishing được sử dụng trong các cuộc tấn công APT. Việc sử dụng phổ biến của kỹ thuật xã hội trong các cuộc tấn công APT nhằm nhấn mạnh tầm quan trọng của đào tạo con người để nhận ra những email bất thường và các cuộc tấn công sử dụng kỹ thuật xã hội, cũng như các biện pháp ứng phó và thông báo sự cố.

Đào tạo người dùng về các cuộc tấn công spear phishing và giải thích làm thế nào để xác định các tấn công rõ ràng là rất quan trọng và nên được thực hiện. Các vấn đề cơ bản với APT là những kẻ tấn công thực hiện việc nghiên cứu và những email của kẻ tấn công trông giống như những email thực sự. Vì vậy, người sử dụng sẽ click vào email APT. Từ góc độ người dùng, không có một sự khác biệt nào giữa một email hợp pháp và một cuộc tấn công giả mạo email. Sự tinh vi của kẻ tấn công thể hiện ở việc thực hiện những nghiên cứu và chắc chắn rằng email trông có vẻ hợp pháp để người sử dụng không thể phân biệt được.

2.2.4. Con người

Sử dụng các công nghệ bảo mật là chưa đủ, tấn công APT thường mở đầu bằng cuộc tấn công giả mạo email do vậy việc đào tạo, huấn luyện con người luôn phải được thực hiện.

Các chuyên gia An ninh mạng trên thế giới cũng thường đề cập đến vấn đề đào tạo và huấn luyện đội ngũ IT của doanh nghiệp, tổ chức trong việc phòng chống các cuộc tấn công có chủ đích nhằm bảo vệ an ninh mạng.

Tạo nhiều điều kiện để nhân viên thấu hiểu cặn kẽ các rủi ro trong việc bị tấn công APT, nhất là các vấn đề xoay quanh việc nhấn vào những liên kết không rõ ràng trong Email và cung cấp các dấu hiệu để nhận biết những kỹ thuật lừa đảo bằng mã độc với mục đích đánh cắp thông tin và dữ liệu, đánh sập mạng nội bộ.

Hãy chỉ ra cho họ thấy rằng việc bị mất đi thông tin và dữ liệu là điều rất nguy hiểm với sự tồn tại và phát triển của doanh nghiệp, tổ chức. Thậm chí điều đó có thể gây ảnh hưởng đến tình trạng tài chính của Công ty và thu nhập cá nhân của họ.

2.2.5. Lập sẵn kế hoạch ứng phó

Việc chuẩn bị sẵn một kế hoạch chỉnh chu luôn là bước đệm vững chắc và an toàn để chúng ta thực hiện mục tiêu của chính mình. Việc phòng tránh tấn công APT cũng không ngoại lệ. Dù có trang bị hệ thống công nghệ tân tiến và tốn kém, bản thân mỗi doanh nghiệp hay tổ chức vẫn phải

tự ý thức trong việc hiểu cách thức hoạt động của APT để có kế hoạch xây dựng hệ thống phòng thủ tốt nhất trong khả năng của nội bộ mình.

III. KẾT LUẬN

Trong năm 2023, Việt Nam có 12 triệu tài khoản bị xâm nhập và 48 triệu bản ghi dữ liệu cá nhân, tổ chức bị rò rỉ và được rao bán trên không gian mạng. Tấn công đe dọa, đòi tiền chuộc (ransomware) diễn ra với 300GB dữ liệu bị mã hóa.

Hầu hết những cuộc tấn công hiện nay đều được thực hiện bởi các tổ chức tội phạm toàn cầu. Những nhóm này có nguồn lực lớn và trình độ chuyên sâu. Việc truy vết cũng rất khó khăn bởi không gian mạng xuyên biên giới và có thể rửa tiền qua tiền mã hóa.

Nhiều tổ chức, doanh nghiệp không chuyên về an toàn thông tin dẫn đến thiếu hụt nguồn nhân sự. Ngoài ra, chi phí dành cho an toàn thông tin cũng rất lớn, trong khi việc vận hành như thế nào để hiệu quả vẫn luôn là một vấn đề.

Để đối phó với những nhóm tội phạm tấn công có chủ đích (tấn công APT), chúng ta cần phải học Luật an ninh mạng, tự trau dồi kiến thức về an toàn thông tin cho bản thân, cũng như nâng cao ý thức phòng tránh, tự vệ khi tham gia mạng xã hội.

Từ những phân tích về bản chất và phương thức hoạt động của các cuộc tấn công APT, có thể rút ra nhiều hàm ý quan trọng đối với công tác giáo dục và đào tạo an toàn thông tin trong bối cảnh chuyển đổi số hiện nay.

Trước hết, giáo dục về an ninh mạng cần được xem là một nội dung thiết yếu trong chương trình đào tạo ở các cơ sở giáo dục, đặc biệt là trong các ngành liên quan đến công nghệ thông tin, quản trị hệ thống và quản lý nhà nước. Việc trang bị cho người học kiến thức nền tảng về các hình thức tấn công mạng, trong đó có tấn công APT, sẽ giúp nâng cao khả năng nhận diện rủi ro và chủ động phòng tránh ngay từ sớm.

Thứ hai, công tác đào tạo cần chú trọng phát triển kỹ năng thực hành và tư duy phản biện cho người học, thay vì chỉ tập trung vào lý thuyết. Các tình huống mô phỏng tấn công APT, các bài tập phân tích email lừa đảo (spear phishing), hay các kịch bản ứng phó sự cố an ninh mạng sẽ giúp người học hình thành thói quen cảnh giác và kỹ năng xử lý tình huống trong môi trường thực tế.

Bên cạnh đó, giáo dục ý thức và trách nhiệm của mỗi cá nhân khi tham gia không gian mạng là yếu tố then chốt. Con người chính là mắt xích quan trọng nhất, đồng thời cũng là điểm yếu dễ bị khai thác nhất trong các cuộc tấn công APT. Do đó, việc giáo dục nhận thức về bảo vệ dữ liệu cá nhân, tuân thủ quy định an toàn thông tin và chấp hành pháp luật về an ninh mạng cần được triển khai thường xuyên, liên tục và phù hợp với từng nhóm đối tượng.

Cuối cùng, các cơ sở giáo dục và tổ chức đào tạo cần tăng cường phối hợp với cơ quan quản lý nhà nước và doanh nghiệp trong lĩnh vực an toàn thông tin để cập nhật kịp thời các xu hướng tấn công mới, từ đó điều chỉnh nội dung đào tạo sát với thực tiễn. Điều này không chỉ góp phần nâng cao chất lượng nguồn nhân lực an toàn thông tin mà còn đóng vai trò quan trọng trong việc xây dựng không gian mạng an toàn, lành mạnh và bền vững.

TÀI LIỆU THAM KHẢO

Bộ thông tin và truyền thông, *Phòng chống mã độc và tấn công mạng cho người dùng máy tính,* NXB thông tin và truyền thông, 2019.

TS. Thái Thanh Tùng, *Mật mã học và an toàn thông tin, nhà xuất bản thông tin và truyền thông*, 2011.

Phan Đình Diệu, *Lý thuyết mật mã và an toàn thông tin,* NXB Đại học Quốc gia Hà Nội, 2004.

Nguồn: https://baotintuc.vn/khoa-hoc-cong-nghe/cong-nghe-moi-va-an-ninh-mang-trong-ky-nguyen-chuyen-doi-so-tri-tue-nhan-tao-20230803161212010.htm