NHẬN DIỆN VÀ PHÒNG TRÁNH CÁC CUỘC TẤN CÔNG TRÊN KHÔNG GIAN MẠNG
IDENTIFICATION AND PREVENTION OF ATTACK ON THE CYBERSPACE

Nguyễn Minh Thắng
Trường Đại học Kinh tế - Tài chính TP.HCM,, thangnm@uef.edu.vn

Tóm tắt*: Ngày nay, giá trị mà internet mạng lại cho chúng ta trong cuộc sống, học tập, công việc là không thể phủ nhận. Bên cạnh những giá trị tích cực đó, thực tế cho thấy rằng có rất nhiều cuộc tấn công mạng diễn ra nhằm đánh cắp thông tin cá nhân và các cuộc tấn công trên mạng ngày càng gia tăng với mức độ nguy hiểm cao và rất khó kiểm soát. Nhận thức về an ninh mạng của mỗi cá nhân chưa tốt là một trong những nguyên nhân cơ bản để kẻ tấn công lừa đảo. Bài báo này cung cấp một số cách nhận diện các loại hình tấn công phổ biến hiện nay và đưa ra các giải pháp nhằm phòng tránh các mối đe dọa mà kẻ tấn công có thể khai thác.*

Từ khóa*: Không gian mạng, giả mạo, phần mềm độc hại, lừa đảo, OpenBTS, tấn công mạng.*

Abstract*: Today, the value that the internet gives us in life, study and work is undeniable. Besides those positive values, the reality shows that there are many cyber attacks taking place to steal personal information and cyber attacks are increasing with a high level of danger and very difficult. control. The low awareness of each individual's network security is one of the basic reasons for attackers to cheat. This article provides some ways to identify common types of attacks today and offer solutions to prevent threats that attackers can exploit.*

Keywords*: Cyberspace, phishing, malware, fraud, OpenBTS, network attack.*

1. Giới thiệu

Không gian mạng là mạng lưới kết nối toàn cầu của các cơ sở hạ tầng công nghệ thông tin, bao gồm Internet, các mạng viễn thông, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, là môi trường đặc biệt mà con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian. Không gian mạng đang càng ngày càng mở rộng và trở nên phổ biến, các hình thức tấn công mạng ngày một tinh vi hơn, tần xuất ngày càng nhiều hơn làm ảnh hưởng rất lớn đến cá nhân người dùng và doanh nghiệp [1].

An ninh mạng là việc bảo vệ an ninh và quyền riêng tư trước các cuộc tấn công mạng do các lỗ hổng và rủi ro gây ra. Ưu tiên của an ninh mạng là bảo vệ khả năng truy cập, tính toàn vẹn và quyền riêng tư của dữ liệu [2]. Bất kỳ hoạt động nào ngăn cản việc cung cấp an ninh mạng đều được coi là một cuộc tấn công mạng. Mục tiêu của tấn công mạng là truy cập trái phép, chặn dịch vụ và giả mạo dữ liệu (sửa đổi, phá hủy, tiết lộ, chia sẻ). Tấn công mạng luôn là vấn đề nóng đối với cá nhân và tổ chức, nhất là khi số lượng và mức độ phức tạp của các đợt tấn công ngày càng tăng, và chúng được chia thành các nhóm cơ bản trong không gian mạng: Tấn công giả mạo tin nhắn SMS; Tấn công phần mềm độc hại (Malicious software); Tấn công phi kỹ thuật (Social Engineering).

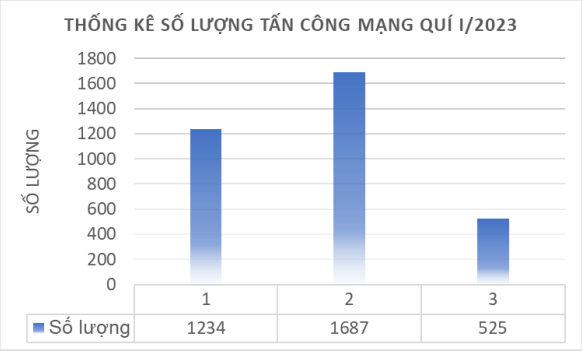
Chúng tôi trình bày bài báo như sau: Phần 2 giới thiệu về tình hình an ninh mạng hiện nay; các hình thức tấn công mạng phổ biến được trình bày trong phần 3; sau cùng, chúng tôi đưa ra một số giải pháp nhằm ngăn chặn các cuộc tấn công trên không gian mạng.

2. Tình trạng tấn công mạng hiện nay

Việt Nam hiện nay là một trong những quốc gia có tốc độ phát triển và ứng dụng Internet cao nhất thế giới. Theo báo cáo của Vietnam Digital Report, tính đến đầu năm 2023, Việt Nam có 77.93 triệu người sử dụng Internet, tương đương 79.1% trên tổng dân số [3]. Tuy nhiên, người dùng Internet tại Việt

Nam vẫn có thói quen dùng phần mềm bẻ khóa hoặc phần mềm không bản quyền mà không quan tâm rằng phần mềm không bản quyền thường không được cập nhật kịp thời các bản vá cho điểm yếu, lỗ hổng bảo mật, điều này dẫn tới việc máy tính, thiết bị của người dùng không được bảo vệ liên tục và rất dễ bị nhiễm mã độc do phần mềm bẻ khóa thường cài cắm sẵn mã độc một cách có chủ đích.

Theo thống kê của Trung tâm giám sát an toàn thông tin Quốc gia, trong quý I/2023 đã ghi nhận, cảnh báo và hướng dẫn xử lý 3.446 cuộc tấn công mạng. Trong đó, tấn công phổ biến nhất là giả mạo SMS, Phishing, malware, H.1 thống kê số lượng các cuộc tấn công mạng.



Hình 1. Thống kê số lượng tấn công mạng quí I/2023

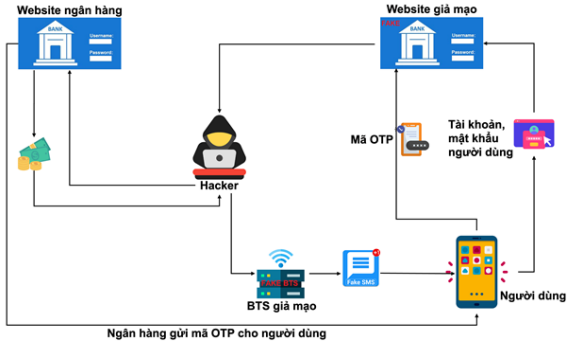
3. Các loại hình tấn công mạng phổ biến

Hiện nay, có rất nhiều người dùng trở thành nạn nhân của các đợt tấn công mạng do các hacker gây ra.

3.1. Phát tán tin nhắn rác thông qua trạm OpenBTS

Đây là hình thức tấn công sử dụng tin nhắn lừa đảo, dụ người dùng truy cập đường link để cài phần mềm độc hại hoặc đánh cắp thông tin tài khoản. Trạm BTS giả sẽ làm nhiễu tín hiệu 3G, 4G xung quanh trạm BTS của nhà mạng, sau đó phát sóng công suất lớn, khiến thiết bị điện thoại nằm trong vùng phủ sẽ nhận được tin nhắn và nhiều người trong cùng một khu vực sẽ nhận được tin nhắn tương tự nhau [4].

H.2 mô tả cách thức hoạt động của loại hình tấn công này, khi người dùng nhận được tin nhắn, nếu không cẩn thận khi truy cập vào các website lừa đảo sẽ bị dẫn dụ để cung cấp thông tin cá nhân như tài khoản, mật khẩu, mã OTP…; Sau khi người dùng cung cấp thông tin, website giả mạo sẽ điều hướng sang website khác, lúc này, đối tượng sẽ sử dụng thông tin cá nhân của người dùng để đăng nhập vào website chính thức của các tổ chức tài chính, ngân hàng để lấy mã xác thực OTP. Cuối cùng, sau khi điện thoại người dùng nhận được mã xác thực OTP, website giả mạo sẽ được điều hướng sang trạng thái yêu cầu người dùng cung cấp mã xác thực OTP. Người dùng mà không cảnh giác sẽ cung cấp thông tin mã OTP để đối tượng hoàn tất quá trình chiếm đoạt tiền trong tài khoản.



Hình 2. *Mô hình giả mạo trạm BTS*

3.2. Social Engineering – Tấn công phi kỹ thuật

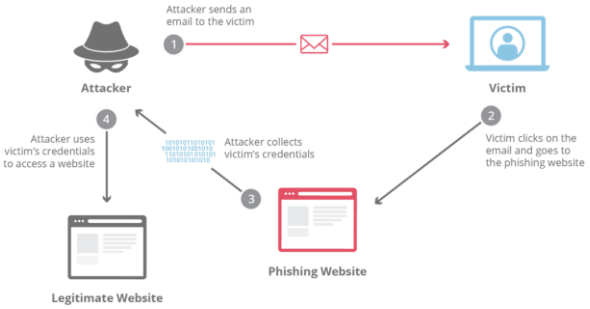
Social engineering (SE) là hình thức tấn công mà đối tượng tấn công tác động trực tiếp đến tâm lý con người để đánh cắp thông tin, dữ liệu của cá nhân và tổ chức. Nhóm tin tặc sẽ đặt câu hỏi để thu thập thông tin từ người dùng, nếu không thể thu thập đủ thông tin từ một nguồn đối tượng tấn công có thể liên hệ với một nguồn khác cùng tổ chức và dựa vào những thông tin đánh cắp được trước đó để tăng thêm độ tin cậy [5].

3.2.1. Phishing

Phishing là hình thức tấn công Social engineering phổ biến nhất hiện nay. Các cuộc tấn công Phishing sử dụng email hoặc các trang web độc hại để thu thập thông tin cá nhân bằng cách giả mạo cơ quan, tổ chức, ngân hàng, công ty cung cấp dịch vụ thiết yếu như điện, nước. Đối tượng tấn công có thể gửi email giả mạo để thông báo về các mối nguy hại và yêu cầu người dùng cung cấp thông tin. Sau khi người dùng cung cấp

thông tin nhóm tấn công có thể sử dụng những thông tin đó để đánh cắp tài khoản của người dùng.

Đầu tiên, kẻ tấn công sẽ lựa chọn những trang chính thức có các giao dịch có liên quan đến thông tin cần đánh cắp như trang Facebook, gmail, ngân hàng, ... Sau đó, thực hiện hành vi nhân bản trang chính thức và xây dựng lại với ý đồ thu thập thông tin người dùng. Mặt khác, tạo email chứa liên kết tới trang giả mạo, người dùng truy cập liên kết tới trang giả mạo thực hiện giao dịch và từ đó thông tin bị đánh cắp lưu vào cơ sở dữ liệu của kẻ tấn công. H.3 mô tả cách thức hoạt động của loại hình tấn công này.

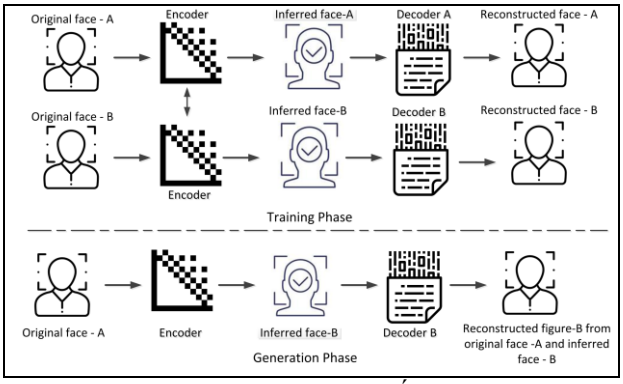


Hình 3. *Cách thức hoạt động của tấn công Phishing*

Các loại tấn công Phishing được tiếp cận rất đa dạng và biến hóa khôn lường. Một số các loại tấn công Phishing có thể kể đến như: Email Phishing, Spear Phishing, Vishing, Smisshing, …

3.2.2. Deepfake

Deepfake là một kỹ thuật gần đây và có tính thuyết phục cao được sử dụng để tiến hành các cuộc tấn công SE, là sự kết hợp giữa học sâu (Deep learning) và giả mạo (Fake). Tội phạm mạng sử dụng deepfakes để giả mạo hình ảnh, âm thanh và video nhằm đạt được một mục tiêu cụ thể. Trong an ninh mạng, deepfake là một mối đe dọa nguy hiểm cho sự an toàn và bảo mật. Một trong những thuật toán nổi tiếng nhất để tạo nội dung deepfake là mạng đối GAN [6]. GAN là sự kết hợp của hai mạng thần kinh nhân tạo (ANN). Các ANN này được gọi là bộ phát hiện và bộ tổng hợp, được đào tạo bằng cách sử dụng bộ dữ liệu lớn gồm hình ảnh, âm thanh và video clip thực. Sau đó, ANN tổng hợp tạo ra nội dung deepfake và ANN dò tìm cố gắng phân biệt tính xác thực của nội dung. Chu kỳ tạo nội dung deepfake tiếp tục cho đến khi máy dò ANN không còn có thể xác định nội dung giả mạo được tạo là giả mạo. Do quy trình tạo và xác thực nghiêm ngặt này, nội dung giả mạo do GAN tạo ra rất khó xác định là giả mạo [7]. H.4 minh họa tổng quan về quá trình tạo dữ liệu deepfake. Trong đó, có thể thấy rằng hai khuôn mặt khác nhau là Mặt A và Mặt B được sử dụng để huấn luyện mạng. Sau đó, mạng được sử dụng để tạo ra Mặt A với các biểu cảm hoặc âm thanh từ Mặt B. Hình ảnh mới được tạo với cách diễn giải Mặt-A ban đầu của Mặt-B có thể được sử dụng để gây nhầm lẫn hoặc gây ảnh hưởng đến nạn nhân. Deepfake đã được sử dụng cho cuộc tấn công SE được tiến hành nhằm vào một công ty năng lượng có trụ sở tại Vương quốc Anh. Trong cuộc tấn công, giọng nói deepfake đã được sử dụng để lừa đảo CEO của công ty [8]. Ngoài lừa đảo, deepfake cũng đã được sử dụng trong một số hoạt động tội phạm khác như tống tiền, gây tổn hại danh tiếng, lan truyền tin giả, thông tin sai lệch, ...



Hình 4. *Cách thức hoạt động của tấn công* Deepfake

Người dùng thường xuyên đăng tải hình ảnh, video lên các trang mạng xã hội là cách để các Hacker có cơ hội thực hiện tấn công này.

3.3. Malware – Tấn công bằng phần mềm độc hại

Tấn công malware là hình thức tấn công qua mạng rất phổ biến hiện nay, bao gồm: Spyware (phần mềm gián điệp), Ransomware (phần mềm tống tiền), Virus Worm (phần mềm độc hại), Backdoor.

Hacker sẽ tấn công người dùng thông qua các lỗ hổng bảo mật hoặc đánh lừa người

dụng nhấn vào các đường dẫn (link) hay email để các phần mềm độc hại tự cài vào máy tính nạn nhân để đánh cắp thông tin, dữ liệu, gây hại cho phần cứng máy tính. Nguy hiểm hơn, loại hình tấn công này có thể lây lan ra cho cả toàn bộ hệ thống máy tính trong một công ty hay tổ chức [9].

Hình 5. *Các loại Malware*

Khi các phần mềm độc hại được cài vào máy tính nạn nhân, chúng sẽ âm thầm theo dõi và ghi lại các hoạt động của người dùng, khi đó kẻ tấn công sẽ có được thông tin về hệ thống file, registry, tiến trình, hoạt động mạng trên máy tính của nạn nhân. Nói chung, các hành vi của malware bao gồm ba bước: (1) cài đặt malware; (2) thay đổi hệ thống; (3) đánh cắp thông tin, lây nhiễm sang hệ thống máy tính khác.

4. Các giải pháp

Tấn công mạng vẫn đang diễn ra hàng ngày, nhiêu nhà nghiên cứu đã đưa ra các giải pháp nhằm giảm thiểu các đợt tấn công mạng. Trong bài báo này, chúng ta chia thành hai nhóm giải pháp là: (1) đảm bảo an toàn các dữ liệu trên máy tính cá nhân và (2) có kiến thức cũng như sử dụng Internet một cách an toàn nhất.

4.1 An toàn máy tính cá nhân

Để hạn chế các cuộc tấn công malware, chúng ta cần sao lưu dữ liệu thường xuyên giúp người sử dụng không phải lo lắng khi sự cố xảy ra; Sử dụng các phần mềm diệt Virus có bản quyền để phát hiện, ngăn chặn các loại virus mới; Không sử dụng bẻ khóa (crack) cho các phần mềm được cài trên máy tính, vì hành động bẻ khóa chính là tự chúng ta đưa virus vào máy tính; Thường xuyên kiểm tra máy tính xem có phần mềm nào lạ hoặc không sử dụng trên máy tính hay không; Khuyến khích tải và cài đặt phần mềm từ các website chính thống.

4.2 An toàn khi sử dụng Internet

Đối với các hình thức tấn công SE, chúng ta cần cảnh giác với các email có nội dung gây sự tò mò hoặc thúc giục bạn nhập thông tin cá nhân; Không nhấn vào các đường dẫn được gửi từ các email nếu bạn cảm thấy không chắc chắn; Không tùy tiện cung cấp mã OTP; Thường xuyên cập nhật phần mềm để vá các lỗ hổng ứng dụng; Sử dụng bảo mật tài khoản mạng xã hội nhiều lớp và mật khẩu có cấp độ mạnh. Ngoài ra, chúng ta có thể sử dụng một số công cụ (tool) để hạn chế bị lừa đảo như:

- SpoofGuard: được tích hợp trong trình duyệt web Microsoft Internet Explorer, công cụ này sẽ cảnh báo nếu chúng ta truy cập vào các website giả mạo.
- Anti-phishing Domain Advisor: công cụ này được công ty Panda Security đưa ra để cảnh báo cho người dùng biết các website lừa đảo.
- ChongLuaDao.vn: đây là tiện tích dùng để kiểm ra các đường dẫn (link) có an toàn hay không do Trung tâm giám sát an ninh mạng Quốc gia đề xuất. Hiện tại, chúng ta có thể sử dụng tiện ích này trên các trình duyệt web như Google Chrome, CocCoc, … và tải ứng dụng trên các thiết bị di động.

Trong các giải pháp nhằm hạn chế tấn công mạng thì theo chúng tôi, yếu tố con người vẫn là quan trọng nhất. Sự nhận biết cũng như có kiến thức về an ninh mạng của mỗi cá nhân sẽ quyết định đến sự thành công hay thất bại của các đợt tấn công mạng do Hacker gây ra. Do đó, nâng cao nhận thức cho người sử dụng luôn là vấn đề nên được ưu tiên hàng đầu.

5. Kết luận

Các cuộc tấn công mạng luôn là mối đe dọa lớn đối với các tổ chức và cá nhân. Chúng có thể gây ra rủi ro rất lớn cho các nạn nhân. Trong bài báo này, chúng ta đã trình bày và phân tích các hình thức tấn công mạng phổ biến hiện nay, đánh giá các rủi ro

mà cá nhân và tổ chức có thể gặp phải khi trở thành nạn nhân. Bên cạnh đó, chúng tôi đưa ra một số giải pháp để mỗi cá nhân tránh khỏi hoặc giảm mức độ thấp nhất trước các đợt tấn công mạng.

Tài liệu tham khảo

[1] Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., & Li, J. (2015). *Survey on cyberspace security*. Science China Information Sciences, 58, 1-43.

[2] Thames, L., & Schaefer, D. (2017). *Cybersecurity for industry 4.0* (pp. 1-33). Heidelberg: Springer.

[3] https://datareportal.com/reports/digital-2023-global-overview-report

[4] Muhaimin, A., *Senastri, N. M. J., & Karma, N. M. S. (2021). Perlindungan Hukum Terhadap Pengguna Jasa Telekomunikasi dalam Pelanggaran Data Pribadi Melalui sms Broadcast*. Jurnal Preferensi Hukum, 2(2), 238-242.

[5] Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). *A study on the psychology of social engineering-based cyberattacks and existing countermeasures*. Applied Sciences, 12(12), 6042..

[6] Albahar, M., & Almalki, J. (2019). *Deepfakes: Threats and countermeasures systematic review*. Journal of Theoretical and Applied Information Technology, 97(22), 3242-3250.

[7] Chi, H., Maduakor, U., Alo, R., & Williams, E. (2021). *Integrating deepfake detection into cybersecurity curriculum*. In Proceedings of the Future Technologies Conference (FTC) 2020, Volume 1 (pp. 588-598). Springer International Publishing.

[8] Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. Available online: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

[9] Hồ, A. K. N., & Minh, C. T. (2021). *Sự phát triển của malware trong 10 năm trở lại đây*. Tạp chí Khoa học và Kinh tế phát triển, (12), 21-34.