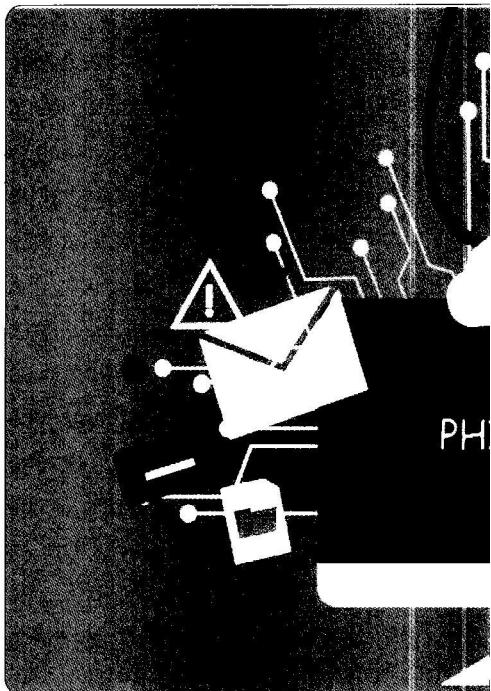




TÌM HIỂU VỀ MỘT SỐ HÌNH THỨC TẤN CÔNG MẠNG PHỔ BIẾN VÀ CÁCH PHÒNG, CHỐNG

ThS. NGUYỄN THỊ HẬU
Đại học Đà Nẵng

Với sự phát triển không ngừng của công nghệ, những cuộc tấn công mạng thông qua Internet cũng ngày càng trở nên đa dạng hơn. Nếu các tổ chức, cá nhân không trang bị đủ kiến thức liên quan đến vấn đề này, sẽ dẫn đến việc các thông tin kinh doanh quan trọng bị xâm phạm. Bài viết này đề cập đến các hình thức tấn công mạng phổ biến hiện nay và đưa ra một số giải pháp giúp người sử dụng phòng, chống chúng hiệu quả nhất.



1. Tấn công giả mạo (Phishing)

Mục tiêu và phương thức

Thuật ngữ gốc tiếng Anh: Phishing là biến thể từ Fishing, nghĩa là câu cá. Hình thức tấn công này bắt đầu bằng việc “nhử” người dùng tiết lộ thông tin mật. Đây là một trong những hình thức tấn công mạng phổ biến nhất hiện nay. Tấn công Phishing hướng đến việc triển khai các hoạt động nhằm lấy cắp các thông tin nhạy cảm như tên người dùng, mật khẩu và các chi tiết thẻ tín dụng bằng cách giả dạng thành một chủ thẻ tín dụng trong một giao dịch điện tử, chủ yếu thông qua Internet. Để tấn công Phishing, các hacker thường dùng các phương thức sau:

Macro Office

Trong các cuộc tấn công Phishing, đầu tiên, các hacker sẽ sử dụng thủ thuật tâm lý để thuyết phục nạn nhân mở và tương tác với các thư điện tử độc hại (đính kèm liên kết hoặc file thực thi chứa mã độc). Kỹ thuật này bao gồm việc tạo email ngụy trang, tự nhận đến từ các thương hiệu nổi tiếng, hóa đơn

giả mạo, thậm chí là email được gửi đến từ đối tác, đồng nghiệp của người sử dụng.

Theo kết quả thống kê của các nhà nghiên cứu tại công ty an ninh mạng Proofpoint, Macro Office chính là kỹ thuật phổ biến nhất để hacker đạt được điều này. Macro là một chức năng của Microsoft Office, cho phép người dùng kích hoạt các lệnh tự động để thực thi hàng loạt tác vụ khác nhau. Vì các Macro thường được bật theo mặc định để chạy lệnh, chúng cũng có thể bị lợi dụng để thực thi mã độc và từ đó vô tình trở thành cầu nối giúp hacker nắm được quyền truy cập và quyền kiểm soát PC của nạn nhân.

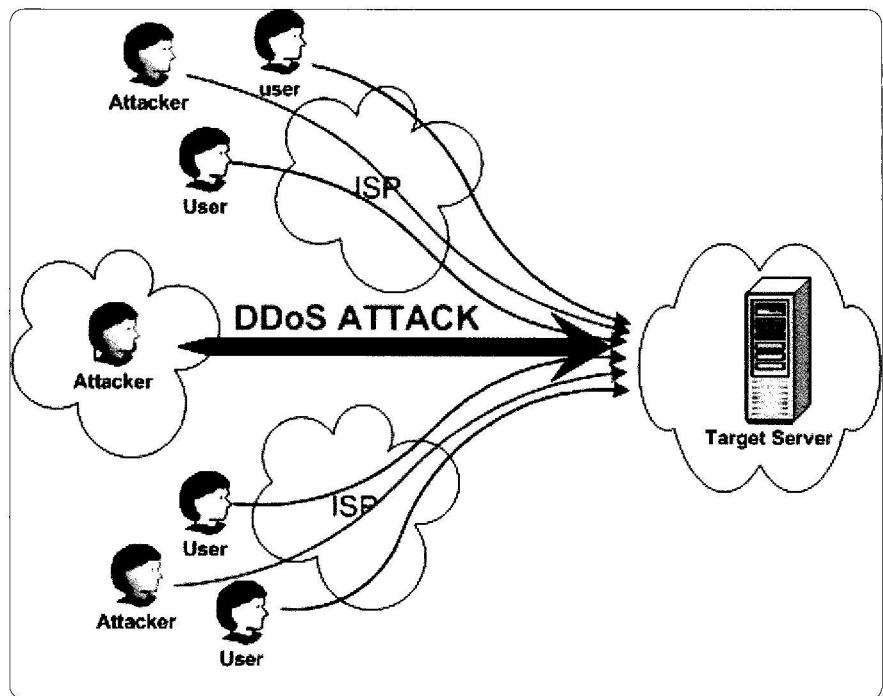
Các trường hợp tấn công kiểu này sẽ kết hợp với các kỹ thuật xã hội để khuyến khích nạn nhân bật Macro độc hại bằng cách tuyên bố rằng đó là một chức năng cần thiết để xem tệp đính kèm Microsoft Word hoặc Microsoft Excel. Phương pháp này chiếm gần 1/10 trên tổng số các cuộc tấn công mạng được ghi nhận.

PowerShell

PowerShell cũng thường xuyên bị những kẻ tấn công sử dụng như một phương tiện để giành quyền truy cập vào các mạng sau khi sử dụng email lừa đảo. Những cuộc tấn công dạng này thường dựa vào việc gửi và thuyết phục nạn nhân nhấp vào một liên kết chứa mã độc để thực thi PowerShell. Các cuộc tấn công này thường rất khó phát hiện vì chúng sử dụng chức năng hợp pháp của Windows.

Whaling

Whaling là kiểu tấn công Phishing tinh vi và tiên tiến khác. Kiểu này chỉ nhắm vào một nhóm người cụ thể là các giám đốc điều hành doanh nghiệp cấp cao như quản lý hoặc CEO. Hacker sẽ dành nhiều thời gian để nghiên cứu về người đó và tạo ra một thông điệp chuyên biệt nhắm mục tiêu vào những người chủ chốt trong một tổ chức, những người thường có quyền truy cập vào quỹ hoặc thông tin nhạy cảm. Hacker sẽ gửi một liên kết đến trang đăng nhập giả mạo, chúng sẽ lừa nạn



nhân để lấy mã truy cập hoặc thông tin đăng nhập. Một số hacker sẽ yêu cầu nạn nhân tải xuống file đính kèm để xem phần còn lại của một bức thư. Các file đính kèm này chứa phần mềm độc hại có thể truy cập vào máy tính.

Angler Phishing

Angler Phishing là thủ đoạn tấn công tương đối mới, sử dụng mạng xã hội để thu hút mọi người chia sẻ thông tin nhạy cảm. Các hacker theo dõi những người đăng các thông tin về ngân hàng, ví dụ một bài báo về khoản tiền gửi bị trì hoãn hoặc một số dịch vụ ngân hàng chất lượng kém... và các dịch vụ khác trên mạng xã hội.

Tội phạm mạng sẽ sử dụng thông tin này liên hệ với người sử dụng giả vờ rằng chúng đến từ ngân hàng và sau đó yêu cầu người sử dụng nhấp vào một liên kết để có thể nói chuyện với đại diện dịch vụ khách hàng, sau đó chúng sẽ yêu cầu cung cấp thông tin để xác minh danh tính, từ đó, thực hiện các hành vi lừa đảo.

CEO Fraud Phishing

Kiểu tấn công CEO Fraud Phishing gần giống Whaling, nó nhắm mục tiêu đến các CEO và người quản lý nhưng kiểu tấn công này thậm chí còn nguy hiểm hơn, vì mục tiêu không chỉ là lấy thông tin từ CEO mà là mạo danh vị CEO đó. Kẻ tấn công giả danh CEO hoặc người có chức danh tương tự, sau đó sẽ gửi email cho đồng nghiệp của họ yêu cầu chuyển tiền thông qua hình thức chuyển khoản hoặc yêu cầu gửi thông tin bí mật ngay lập tức.

Kiểu tấn công này thường nhắm vào một người nào đó trong công ty được ủy quyền thực hiện việc chuyển khoản ngân hàng, như thủ quỹ, người từ bộ phận tài chính hoặc những người nắm giữ thông tin nhạy cảm. Thông báo thường mang nghĩa rất khẩn cấp, vì vậy, nạn nhân sẽ không có thời gian để suy nghĩ.

Search Engine Phishing

Search Engine Phishing sử dụng các công cụ tìm kiếm hợp pháp. Hacker

sẽ tạo ra một trang web không có thật cung cấp các ưu đãi, những mặt hàng miễn phí và giảm giá cho các sản phẩm, thậm chí cả những lời mời làm việc. Sau đó, chúng sẽ sử dụng kỹ thuật SEO (tối ưu hóa trang web cho giai đoạn thu thập thông tin và chỉ mục). Vì vậy, khi người sử dụng tìm kiếm một thứ gì đó, công cụ tìm kiếm sẽ hiển thị cho kết quả bao gồm các trang web giả mạo này. Sau đó, người sử dụng sẽ bị lừa đăng nhập hoặc cung cấp thông tin nhạy cảm cho tội phạm mạng. Một số kẻ lừa đảo đang trở nên thạo trong việc sử dụng các kỹ thuật tiên tiến để thao túng những công cụ tìm kiếm nhằm thu hút lưu lượng truy cập vào trang web.

Cách phòng, chống

- Sử dụng các công cụ hạn chế Phishing:

- + *SpoofGuard*: Là một trình duyệt tương thích với Microsoft Internet Explorer. SpoofGuard sẽ đặt “cảnh báo” trên thanh công cụ của trình



duyệt. Nó sẽ chuyển từ màu xanh sang màu đỏ nếu bạn vô tình truy cập vào website giả mạo. Nếu bạn cố nhập các thông tin quan trọng vào một trang giả mạo, SpoofGuard sẽ lưu dữ liệu của bạn và đưa ra cảnh báo.

+ *Anti-phishing Domain Advisor*: Là một thanh công cụ giúp cảnh báo những trang web lừa đảo, dựa theo dữ liệu của công ty Panda Security.

+ *Netcraft Anti-phishing Extension*: Netcraft là đơn vị uy tín trong việc cung cấp các dịch vụ bảo mật. Trong số đó, tiện ích mở rộng chống Phishing của Netcraft như Anti-phishing Extension được đánh giá cao với nhiều tính năng cảnh báo thông minh cho người dùng.

- Cảnh giác với các email có xu hướng thúc giục bạn nhập thông tin cá nhân, thông tin nhạy cảm (thông tin thẻ tín dụng, thông tin tài khoản...).

- Không click vào các đường dẫn được gửi đến các email nếu không chắc chắn an toàn.

- Không trả lời những thư rác, lừa đảo.

- Luôn cập nhật phần mềm, ứng dụng để phòng các lỗ hổng bảo mật có thể bị tấn công.

2. Malware - Tấn công bằng phần mềm độc hại

Mục tiêu và phương thức

Tấn công Malware là một trong những hình thức tấn công qua mạng phổ biến nhất hiện nay, tấn công này gồm: Spyware (phần mềm gián điệp); Ransomware (mã độc tống tiền); Virus; Worm (phần mềm độc hại lây lan với tốc độ nhanh).

Hacker sẽ tiến hành tấn công người dùng thông qua các lỗ hổng bảo mật. Hoặc lừa người dùng click vào một đường link hoặc email để cài phần

mềm độc hại tự động vào máy tính. Khi được cài đặt thành công, Malware sẽ gây ra những hậu quả nghiêm trọng như: Chặn các truy cập vào hệ thống mạng và dữ liệu quan trọng; cài đặt thêm phần mềm độc hại khác vào máy tính người dùng; đánh cắp dữ liệu; phá hoại phần cứng, phần mềm, làm hệ thống bị té liệt, không thể hoạt động.

Cách phòng, chống

- Sao lưu dữ liệu thường xuyên giúp người sử dụng không phải lo lắng khi dữ liệu bị phá hủy.

- Thường xuyên cập nhật phần mềm, Các bản cập nhật của phần mềm (trình duyệt, hệ điều hành, phần mềm diệt virus,...) sẽ vá lỗi bảo mật còn tồn tại trên phiên bản cũ, đảm bảo an toàn thông tin cho người dùng.

- Cảnh thận với các link hoặc file lạ: Đây là phương thức lừa đảo khá phổ biến của hacker. Chúng sẽ gửi email hoặc nhắn tin qua Facebook, đính kèm link download và nói rằng đó là file quan trọng hoặc chứa nội dung hấp dẫn. Khi tải về, các file này thường nằm ở dạng .docx, .xlsx, .pptx hay .pdf, nhưng thực chất là File .exe (chương trình có thể chạy được). Ngay lúc người dùng click mở file, mã độc sẽ lập tức bắt đầu hoạt động.

3. Tấn công từ chối dịch vụ (DoS và DDoS)

Mục tiêu và phương thức

DoS (Denial of Service) có nghĩa là “đánh sập tạm thời” một hệ thống, máy chủ hoặc mạng nội bộ. Để thực hiện được điều này, các hacker thường tạo ra một khối lượng các hoạt động khổng lồ ở cùng một thời điểm, khiến cho hệ thống bị quá tải. Vì thế, người dùng sẽ không thể truy cập vào dịch vụ trong khoảng thời gian mà cuộc tấn công DoS diễn ra.

Một hình thức biến thể của DoS là DDoS (Distributed Denial of Service): Tin tức sử dụng một mạng lưới các máy tính (Botnet) để tấn công người dùng. Các máy tính thuộc mạng lưới Botnet sẽ không biết bản thân đang bị lợi dụng trở thành công cụ tấn công.

Một số hình thức tấn công DDoS

Tấn công gây nghẽn mạng: Gây quá tải hệ thống mạng bằng lượng truy cập lớn đến từ nhiều nguồn để chặn các truy cập thực của người dùng với phương thức gây nghẽn đối tượng bằng các gói UDP và ICMP.

Tấn công khuếch đại hệ thống phân giải tên miền (DNS): Làm quá tải hệ thống bằng phản hồi từ các bộ giải mã DNS với phương thức mạo danh địa chỉ IP của máy bị tấn công để gửi yêu cầu nhiều bộ giải mã DNS. Các bộ giải mã hồi đáp về IP của máy có kích thước gói dữ liệu có thể lớn hơn kích thước của yêu cầu tới 50 lần.

Cách phòng, chống

- Theo dõi lưu lượng truy cập để có thể phát hiện được các vụ tấn công DDoS nhỏ mà tin tức vẫn thường dùng để kiểm tra năng lực của mạng lưới trước khi tấn công thật sự.

- Nếu có thể xác định được địa chỉ của các máy tính thực hiện tấn công, người sử dụng có thể tạo một danh sách quản lý truy cập trong tường lửa để thực hiện chặn các IP này.

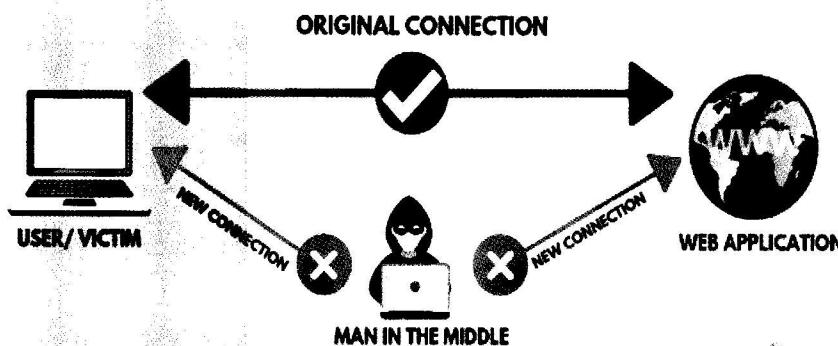
4. Tấn công trung gian (Man in the middle - MitM)

Mục tiêu và phương thức

Tấn công MitM còn gọi là tấn công nghe lén, xảy ra khi kẻ tấn công xâm nhập vào một giao dịch hay một cuộc giao tiếp giữa hai đối tượng. Khi đã chen vào thành công, chúng có thể đánh cắp dữ liệu trong giao dịch đó.



HOW MAN IN THE MIDDLE ATTACKS WORK



Các phương thức tấn công như sau:

- *Sniffing*: Sniffing hoặc Packet Sniffing là kỹ thuật được sử dụng để nắm bắt các gói dữ liệu vào và ra của hệ thống. Packet Sniffing cũng tương tự với việc nghe trộm trong điện thoại. Sniffing có thể được xem là hợp pháp nếu được sử dụng đúng cách, doanh nghiệp có thể thực hiện để tăng cường bảo mật.

- *Packet Injection*: Kẻ tấn công sẽ đưa các gói dữ liệu độc hại vào với dữ liệu thông thường. Bằng cách này, người dùng thậm chí không nhận thấy tệp/phần mềm độc hại bởi chúng đến như một phần của luồng truyền thông hợp pháp. Những tập tin này rất phổ biến trong các cuộc tấn công trung gian cũng như các cuộc tấn công từ chối dịch vụ.

- *Gỡ rối phiên*: Khoảng thời gian từ lúc người sử dụng đăng nhập vào tài khoản ngân hàng đến khi đăng xuất khỏi tài khoản đó được gọi là một phiên. Các phiên này là mục tiêu của tin tặc. Bởi chúng có khả năng chứa thông tin bí mật. Trong hầu hết các trường hợp, hacker thiết lập sự hiện diện của mình trong phiên và nắm quyền kiểm soát nó.

- *Loại bỏ SSL*: SSL Stripping hoặc SSL Downgrade Attack khá hiếm khi

nói đến các cuộc tấn công MiTM, nhưng cũng là một trong những hình thức nguy hiểm nhất. Chứng chỉ SSL/TLS giữ liên lạc an toàn trực tuyến thông qua mã hóa, trong các cuộc tấn công SSL, kẻ tấn công loại bỏ kết nối SSL/TLS và chuyển giao thức từ HTTPS an toàn sang HTTP không an toàn.

Cách phòng, chống

- Đảm bảo các website truy cập đã cài SSL.
- Không mua hàng hoặc gửi dữ liệu nhạy cảm khi dùng mạng công cộng.
- Không nhấp vào link hoặc email độc hại.
- Sử dụng các công cụ bảo mật thích hợp được cài đặt trên hệ thống máy tính.

5. Khai thác lỗ hổng Zero-day

Mục tiêu và phương thức

Lỗ hổng Zero-day thực chất là những lỗ hổng bảo mật của phần mềm hoặc phần cứng mà người dùng chưa phát hiện ra. Chúng tồn tại trong nhiều môi trường khác nhau như: Website, Mobile Apps, hệ thống mạng doanh nghiệp, phần mềm, phần cứng máy tính, thiết bị IoT, Cloud,... Sự khác nhau giữa một lỗ hổng bảo mật thông thường và một lỗ hổng Zero-day nằm ở chỗ: Lỗ hổng Zero-day là những lỗ hổng chưa được biết tới bởi đối tượng sở hữu hoặc cung cấp sản phẩm chứa lỗ hổng.

Thông thường ngay sau khi phát hiện ra lỗ hổng, bên cung cấp sản phẩm sẽ tung ra bản vá bảo mật cho lỗ hổng này để người dùng được bảo mật tốt hơn. Tuy nhiên trên thực tế, người dùng ít khi cập nhật phiên bản mới của phần mềm ngay lập tức. Điều đó khiến cho Zero-day được biết đến là những lỗ hổng rất nguy hiểm. Có thể gây thiệt hại nghiêm trọng cho doanh nghiệp và người dùng.

Cách phòng, chống

- Thường xuyên cập nhật phần mềm và hệ điều hành;
- Triển khai giám sát bảo mật theo thời gian thực;
- Triển khai hệ thống phát hiện xâm nhập IDS và IPS;
- Sử dụng phần mềm quét lỗ hổng bảo mật.

Bên cạnh các giải pháp cụ thể cho các hình thức tấn công mạng nêu trên, các chuyên gia đã đưa ra những khuyến nghị đối với các tổ chức, doanh nghiệp: Cần xây dựng một chính sách bảo mật với các điều khoản rõ ràng, minh bạch; Lựa chọn các phần mềm, đối tác một cách kỹ càng; ưu tiên những bên có cam kết bảo mật và cam kết cập nhật bảo mật thường xuyên; tuyệt đối không sử dụng các phần mềm bẻ khóa; luôn cập nhật phần mềm phiên bản mới nhất; sử dụng các dịch vụ đám mây uy tín cho mục đích lưu trữ; đánh giá bảo mật và xây dựng một chiến lược an ninh mạng tổng thể cho doanh nghiệp, bao gồm các thành phần: Bảo mật website, bảo mật hệ thống máy chủ, mạng nội bộ, hệ thống quan hệ khách hàng (CRM), bảo mật IoT, bảo mật hệ thống công nghệ thông tin, vận hành; thường xuyên tổ chức các buổi đào tạo kiến thức sử dụng Internet an toàn cho nhân viên...■