BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU THUYẾT MINH CHUYÊN ĐỀ "KIẾN THỨC, KỸ NĂNG PHÒNG CHỐNG MÃ ĐỘC VÀ VI-RÚT"

Hà Nội, năm 2023

I. CÁC LOẠI MÃ ĐỘC VÀ CƠ CHẾ LÂY LAN MÃ ĐỘC

1. Mã độc là gì?

Mã độc hay "Malicious software" là một loại phần mềm được tạo ra và chèn vào hệ thống một cách bí mật với mục đích thâm nhập, phá hoại hệ thống hoặc lấy cắp thông tin, làm gián đoạn, tổn hại tới tính bí mật, tính toàn vẹn và tính sẵn sàng của máy tính nạn nhân.

Mã độc được phân thành nhiều loại tùy theo chức năng, cách thức lây nhiễm, phá hoại: vi-rút, worms (sâu máy tính), trojan, rootkit…

Mọi người hay bị nhầm lẫn mã độc với 1 khái niệm khác là vi-rút máy tính. Thực tế, vi-rút máy tính chỉ là 1 phần nhỏ trong khái niệm mã độc. Vi-rút máy tính hiểu đơn thuần cũng là một dạng mã độc nhưng sự khác biệt ở chỗ vi-rút máy tính có khả năng tự lây lan.

Các loại mã độc càng ngày càng phức tạp từ cách thức lây nhiễm, phương pháp ẩn mình, cách thức thực hiện các hành vi nguy hiểm… Giới hạn giữa các loại mã độc ngày càng hạn hẹp vì bản thân các mã độc cũng phải có sự kết hợp lẫn nhau để hiệu quả tấn công là cao nhất.

Tiếp theo, chúng ta tìm hiểu về các loại mã độc phổ biến.

2. Các loại mã độc phổ biến

2.1. Vi-rút

Vi-rút máy tính là một loại phần mềm độc hại đính kèm vào một chương trình khác (chẳng hạn như tài liệu), có thể sao chép và lây lan sau khi một người dùng chạy vi-rút lần đầu trên hệ thống. Chẳng hạn, bạn có thể nhận được email có tệp đính kèm độc hại, vô tình mở tệp và sau đó vi-rút máy tính chạy trên máy tính của bạn. Vi-rút có hại và có thể phá hủy dữ liệu, làm chậm tài nguyên hệ thống và ghi lại các thao tác gõ phím.

Trước đây, Vi-rút thường được viết bởi một số người am hiểu về lập trình muốn chứng tỏ khả năng của mình nên thường Vi-rút có các hành động phá hoại như làm chương trình không hoạt động đúng như mong muốn, xóa dữ liệu, làm hỏng ổ cứng, những Vi-rút mới được viết trong thời gian gần đây không còn thực hiện các trò đùa hay sự phá hoại đối máy tính của nạn nhân bị lây nhiễm nữa, mà đa phần hướng đến việc lấy cắp các thông tin cá nhân nhạy cảm (các mã số thẻ tín dụng, tài khoản, tài liệu mật…) hay mở cửa hậu để cho tin tặc đột nhập, chiếm

quyền điều khiển hoặc thực hiện các hành động khác nhằm có lợi cho người phát tán Vi-rút.

Qua thống kê của các hãng bảo mật, chiếm trên 90% tổng số Vi-rút đã được phát hiện là nhắm vào hệ thống, máy tính, thiết bị sử dụng hệ điều hành họ Windows, điều này đơn giản bởi hệ điều hành này được sử dụng nhiều nhất trên thế giới. Do tính thông dụng của Windows nên các tin tặc thường tập trung hướng vào chúng nhiều hơn là các hệ điều hành khác. Có hàng triệu vi-rút máy tính, nhưng sau đây là một số loại vi-rút máy tính phổ biến cần lưu ý:

- Boot Sector Vi-rút

Ngày nay hầu như không còn thấy virus Boot nào lây trên các máy tính của chúng ta. Lý do đơn giản là vì virus Boot có tốc độ lây lan rất chậm và không còn phù hợp với thời đại của Internet. Tuy nhiên, virus Boot vẫn là một phần trong lịch sử virus máy tính.

Khi máy tính của bạn khởi động, một đoạn chương trình nhỏ trong ổ đĩa khởi động của bạn sẽ được thực thi. Đoạn chương trình này có nhiệm vụ nạp hệ điều hành (Windows, Linux hay Unix...). Sau khi nạp xong hệ điều hành, bạn mới có thể bắt đầu sử dụng máy. Đoạn mã nói trên thường được để ở vùng trên cùng của ổ đĩa khởi động, và chúng được gọi là Boot sector.

- Macro Vi-rút

Vi-rút macro thường được tìm thấy trong các chương trình xử lý văn bản và bảng tính như Microsoft Word và Excel. Những vi-rút này thường được nhúng trong tài liệu và lây lan khi tệp được chuyển sang máy tính khác, thường là qua tệp đính kèm email.

2.2. Worms

Sâu máy tính - Worm là loại vi-rút có sức lây lan rộng, nhanh và phổ biến nhất hiện nay. Worm kết hợp cả sức phá hoại của vi-rút, đặc tính âm thầm của Trojan và hơn hết là sự lây lan đáng sợ mà những kẻ viết vi-rút trang bị cho nó để trở thành một kẻ phá hoại với vũ khí tối tân. Tiêu biểu như Mellisa hay Love Letter. Với sự lây lan đáng sợ chúng đã làm tê liệt hàng loạt hệ thống máy chủ, làm ách tắc đường truyền Internet.

Thời điểm ban đầu, Worm được dùng để chỉ những virus phát tán bằng cách tìm các địa chỉ trong sổ địa chỉ (Address book) của máy mà nó lây nhiễm và tự gửi chính nó qua email tới những địa chỉ tìm được.

2.3. Trojan

Thuật ngữ này dựa vào một điển tích, đó là cuộc chiến giữa người Hy Lạp và người thành Tơ-roa. Thành Tơ-roa là một thành trì kiên cố, quân Hy Lạp không sao có thể đột nhập vào được. Người Hy Lạp đã nghĩ ra một kế, giả vờ rút lui, sau đó để lại thành Tơ-roa một con ngựa gỗ khổng lồ. Sau khi ngựa được đưa vào trong thành, đêm xuống, những quân lính từ trong bụng ngựa xông ra và đánh chiếm thành từ bên trong.

Phương pháp trên cũng chính là cách mà các Trojan máy tính áp dụng. Khác với virus, Trojan là một đoạn mã chương trình HOÀN TOÀN KHÔNG CÓ TÍNH CHẤT LÂY LAN. Đầu tiên, kẻ viết ra Trojan bằng cách nào đó lừa đối phương sử dụng chương trình của mình hoặc ghép Trojan đi kèm với các vi-rút (đặc biệt là các vi-rút dạng Worm – sâu máy tính) để xâm nhập, cài đặt lên máy nạn nhân. Đến thời điểm thuận lợi, Trojan sẽ ăn cắp thông tin quan trọng trên máy tính của nạn nhân như số thẻ tín dụng, mật khẩu... để gửi về cho chủ nhân của nó ở trên mạng hoặc có thể ra tay xoá dữ liệu nếu được lập trình trước.

Bên cạnh các Trojan ăn cắp thông tin truyền thống, một số khái niệm mới cũng được sử dụng để đặt tên cho các Trojan mang tính chất riêng biệt như sau:

• Backdoor: tạo quyền truy cập từ xa vào hệ thống của nạn nhân. Loại phần mềm độc hại này thay đổi bảo mật của nạn nhân để cho phép tin tặc kiểm soát thiết bị, lấy cắp dữ liệu của nạn nhân và thậm chí tải xuống nhiều phần mềm độc hại hơn.

• Spyware (phần mềm gián điệp) theo dõi khi bạn truy cập tài khoản trực tuyến hoặc nhập chi tiết thẻ tín dụng của bạn. Sau đó, họ truyền lại mật khẩu của bạn và các dữ liệu nhận dạng khác cho tin tặc.

• Botnet, chiếm quyền kiểm soát máy tính của bạn để biến nó thành nô lệ/máy tính ma trong mạng dưới sự kiểm soát của tin tặc. Đây là bước đầu tiên trong việc tạo botnet (robot + mạng), thường được sử dụng để thực hiện một cuộc tấn công từ chối dịch vụ (DDoS) phân tán, được thiết kế để đánh sập một mạng bằng cách làm tràn lưu lượng mạng.

2.4. Ransomware (mã độc tống tiền)

Phần mềm độc hại đòi tiền chuộc, hay ransomware, là một loại phần mềm độc hại ngăn người dùng truy cập hệ thống hoặc tệp cá nhân của họ và yêu cầu thanh toán tiền chuộc để lấy lại quyền truy cập. Mặc dù một số người có thể nghĩ

rằng "vi-rút đã khóa máy tính của tôi", nhưng ransomware thường được phân loại là một dạng phần mềm độc hại khác với vi-rút.

Các biến thể sớm nhất của ransomware được phát triển vào cuối những năm 1980 và khoản thanh toán sẽ được gửi qua thư điện tử. Ngày nay, các tác giả ransomware yêu cầu thanh toán được gửi qua tiền điện tử hoặc thẻ tín dụng và những kẻ tấn công nhắm mục tiêu vào các cá nhân, doanh nghiệp và tổ chức thuộc mọi loại hình.

Ví dụ điển hình cho loại mã độc tống tiền là bùng phát đợt tấn công mã độc tống tiền Wannacry vào Qúy II/2017, ảnh hưởng (200.000 máy tính, của 150 quốc gia), Hàng ngàn công ty và tổ chức trên toàn thế giới đã phải đau đầu trước thông báo hiển thị trên màn hình nêu rõ: "Rất tiếc, các tập tin của bạn đã bị mã hóa", kèm yêu cầu đòi tiền chuộc bằng Bitcoin giá trị từ 300 USD – 600 USD.

2.5. Adware

Adware là một loại phần mềm độc hại tự động cài đặt trên thiết bị của bạn và hiển thị quảng cáo và cửa sổ bật lên không mong muốn. Phần mềm quảng cáo bất hợp pháp thường gây khó chịu cho người sử dụng khi chúng cố tình thay đổi trang web mặc định (home page), các trang tìm kiếm mặc định (search page)… hay liên tục tự động hiện ra màn hình (popup) các trang web quảng cáo khi bạn đang duyệt web, thậm chí điều chuyển chúng ta sang các trang web độc hại như các trang quảng cáo đánh bạc,…. Chúng thường bí mật xâm nhập vào máy của bạn khi bạn vô tình "ghé thăm" những trang web có nội dung không lành mạnh, các trang web bẻ khóa phần mềm… hoặc chúng đi theo các phần mềm miễn phí không đáng tin cậy hay các phần mềm bẻ khóa (crack, keygen).

2.6. Spyware

Phần mềm gián điệp (Spyware) là một loại phần mềm độc hại lây nhiễm máy tính hoặc thiết bị di động của nạn nhân và thu thập thông tin về nạn nhân, bao gồm các trang web đã truy cập, nội dung tải xuống, tên người dùng và mật khẩu, thông tin thanh toán và email của nạn nhân,…. Phần mềm gián điệp hoạt động lén lút. Nó tìm đường vào máy tính của nạn nhân mà nạn nhân không biết hoặc không cho phép. Người dùng máy tính thậm chí có thể vô tình cho phép phần mềm gián điệp tự cài đặt khi đồng ý với các điều khoản và điều kiện của một chương trình có vẻ hợp pháp.

Dù phần mềm gián điệp tìm cách xâm nhập vào máy tính, thiết bị của bạn theo cách nào thì phương pháp hoạt động nói chung là giống nhau - nó chạy ngầm (background), duy trì sự hiện diện bí mật, thu thập thông tin hoặc giám sát các hoạt động của nạn nhân nhằm kích hoạt các hoạt động độc hại liên quan đến máy tính của nạn nhân. Và ngay cả khi nạn nhân phát hiện ra sự hiện diện không mong muốn của nó trên hệ thống của mình, Phần mềm gián điệp không đi kèm với tính năng gỡ cài đặt dễ dàng.

Spyware lây lan trên máy tính hoặc điện thoại thông minh thường xảy ra theo ba cách:

• Wi-fi miễn phí không an toàn, phổ biến ở những nơi công cộng như sân bay và quán cà phê. Nếu bạn đăng nhập vào một mạng không an toàn, kẻ xấu có thể thấy mọi thứ bạn làm trong khi kết nối. Hãy tự bảo vệ mình bằng cách tránh các kết nối không an toàn như vậy.

• Lỗ hổng hệ điều hành (OS), mở ra các lỗ hổng có thể cho phép kẻ tấn công lây nhiễm thiết bị di động. Các nhà sản xuất điện thoại thông minh thường xuyên phát hành các bản cập nhật hệ điều hành để bảo vệ người dùng, đó là lý do tại sao bạn nên cài đặt các bản cập nhật ngay khi có (và trước khi tin tặc cố gắng lây nhiễm các thiết bị lỗi thời).

• Các ứng dụng độc hại ẩn trong các ứng dụng có vẻ hợp pháp, đặc biệt khi chúng được tải xuống từ trang web hoặc tin nhắn thay vì từ cửa hàng ứng dụng (apple store hoặc google play). Ở đây, điều quan trọng là phải xem các thông báo cảnh báo khi cài đặt ứng dụng, đặc biệt nếu chúng xin phép truy cập email hoặc thông tin cá nhân khác của bạn. Điểm mấu chốt: Tốt nhất là bạn nên sử dụng các nguồn đáng tin cậy cho ứng dụng dành cho thiết bị di động và tránh mọi ứng dụng của bên thứ ba.

3. Cơ chế lây lan mã độc

3.1. Tải phần mềm độc hại

Ngày nay, bạn có thể tải được vô số loại phần mềm trên mạng từ các trang khác nhau. Sự tiện lợi này đi kèm với nguy cơ trở thành con mồi của tội phạm mạng, những kẻ đang muốn lây nhiễm mã độc cho thiết bị một cách nhanh nhất.

Nếu không truy cập đúng trang của nhà phát triển hay nhà phân phối, bạn sẽ có nguy cơ tải trúng chương trình độc hại, đó có thể là phần mềm quảng cáo (adware) hay, thậm chí là mã độc tống tiền (ransomware). Do mọi người thường

không có thói quen kiểm tra tập tin có an toàn không trước khi tải về, chiêu thức lây lan này đặc biệt phổ biến trong giới tội phạm mạng.

Làm thế nào để tránh tải về chương trình độc hại? Đầu tiên, bạn phải đảm bảo chỉ tải tập tin từ website đáng tin cậy. Tiếp theo, nếu phần mềm tính phí hay mất tiền, bạn đừng bấm vào phiên bản miễn phí tìm thấy đâu đó trên mạng vì nó có thể đang mạo danh phần mềm hợp pháp.

Bạn nên dùng phần mềm diệt vi-rút để quét tập tin trước khi tải hoặc sử dụng các trang web như: https://www.virustotal.com/

3.2. Email giả mạo (phishing)

Phishing là một trong các hình thức được hacker yêu thích nhất vì hầu như ai cũng liên lạc qua email, tin nhắn hay SMS. Trên hết, thủ phạm dễ dàng lừa nạn nhân chỉ bằng một số chi tiết như ngôn ngữ chuyên ngành, có tính thuyết phục, hình ảnh quen thuộc.

Trong các sự cố phishing, kẻ tấn công sẽ gửi cho con mồi một tin nhắn có vẻ đáng tin. Chẳng hạn, ai đó có thể nhận được email từ hãng chuyển phát nhanh thông báo về bưu kiện và yêu cầu cung cấp thông tin để nhận hàng an toàn. Nó rất hiệu quả trong việc tạo ra cảm giác gấp gáp, khiến người nhận đáp ứng ngay lập tức.

Một liên kết sẽ được gửi kèm trong email để nạn nhân mở ra, nhập thông tin, xác minh… Tuy nhiên, thực tế đây lại là liên kết độc hại. Trang web sẽ đánh cắp mọi dữ liệu bạn nhập vào, chẳng hạn thông tin liên lạc, thanh toán. Chúng cũng có thể trở thành công cụ phát tán mã độc ngay khi người dùng bấm vào liên kết.

Để tránh trở thành nạn nhân, bạn nên ghi nhớ kiểm tra kỹ các email phát hiện sai sót, địa chỉ người gửi bất thường hay các tập đính kèm đáng nghi. Ví dụ, nếu nhận được email từ FedEx nhưng địa chỉ email là “f3dex”, bạn nên bỏ qua.

3.3. Remote Desktop Protocol

Giao thức Remote Desktop Protocol (RDP) là công nghệ cho phép máy tính của một người dùng kết nối với máy tính của người khác qua một mạng. Dù giao thức này do Microsoft phát triển, hiện nay nó có thể dùng trên nhiều hệ điều hành khác nhau. Tội phạm mạng cũng tìm ra cách để khai thác giao thức.

Đôi khi, RDP không được bảo vệ nghiêm ngặt, bỏ ngỏ trên một hệ điều hành cũ, giúp kẻ tấn công có cơ hội hoàn hảo để triển khai. Ngay khi chúng tìm

ra kết nối có vấn đề và chiếm quyền truy cập máy tính từ xa qua giao thức, chúng có thể cấy mã độc, thậm chí lấy đi dữ liệu từ thiết bị mà chủ nhân không hay biết.

Ransomware là một vấn đề phổ biến với người dùng RDP. Theo báo cáo năm 2020 của Paloalto, trong số 1.000 vụ tấn công mã độc tống tiền được ghi nhận, 50% sử dụng RDP làm trung gian lây nhiễm ban đầu. Ransomware sẽ mã hóa tập tin của người dùng, giữ chúng làm con tin để đòi tiền chuộc.

Nhằm bảo vệ thiết bị, bạn nên sử dụng mật khẩu mạnh, kích hoạt xác minh hai bước và cập nhật máy chủ bất cứ khi nào có thể.

3.4. Ổ đĩa flash

Dù có thể lây nhiễm mã độc từ xa, hacker cũng yêu thích loại hình truyền thống, đó là các ổ đĩa flash hay USB. Nếu tin tặc có cơ hội tiếp xúc trực tiếp với thiết bị của nạn nhân, sử dụng USB là một cách nhanh và đơn giản.

USB sẽ được cài sẵn mã độc, thu thập dữ liệu trên thiết bị. Chẳng hạn, ổ đĩa flash cấy keylogger vào máy tính để theo dõi mọi thứ mà nạn nhân nhập, bao gồm thông tin đăng nhập, thanh toán hay dữ liệu nhạy cảm. Chúng có thể cấy mọi thứ, từ ransomware, spyware, vi-rút đến sâu máy tính "worms".

Đó là lý do vì sao nên cài đặt mật khẩu cho thiết bị và khóa chúng ngay khi rời khỏi tầm mắt. Bạn cũng nên vô hiệu hóa các cổng USB nếu không dùng tới máy tính. Ngoài ra, nên thận trọng khi sử dụng USB không rõ nguồn gốc, hay quét bằng phần mềm diệt vi-rút.

Tội phạm mạng không ngừng tìm ra những cách thức mới để phát tán mã độc và tấn công nạn nhân. Vì vậy, bạn nên bảo vệ thiết bị bằng mọi cách và kiểm tra kỹ càng bất kỳ phần mềm, tập tin, liên kết nào trước khi tải hay truy cập.

- Emails và Tệp đính kèm: Mã độc thường được phát tán qua email dưới dạng tệp đính kèm. Khi người dùng mở tệp, mã độc sẽ được kích hoạt và mã độc có thể lây nhiễm vào hệ thống.

- Trang Web độc hại: Các trang web độc hại có thể cài đặt mã độc mà không cần sự đồng ý của người sử dụng. Điều này có thể xảy ra thông qua các lỗ hổng trong trình duyệt hoặc phần mềm không được cập nhật.

- USB và Thiết bị di động: Mã độc cũng có thể lây lan thông qua các thiết bị lưu trữ di động như USB hoặc ổ cứng ngoại vi. Khi thiết bị này được kết nối vào một hệ thống, mã độc có thể chuyển sang máy tính đó.

• Mạng nội bộ (LAN): Mã độc có thể lây lan trong mạng nội bộ của một tổ chức, tận dụng các lỗ hổng bảo mật hoặc sử dụng kỹ thuật lan truyền từ máy tính này sang máy tính khác.

II. PHÒNG CHỐNG MÃ ĐỘC VÀ GIỚI THIỆU CÁC CHƯƠNG TRÌNH DIỆT VI-RÚT

1. Phòng chống mã độc

Phòng chống mã độc là quá trình triển khai các biện pháp và chiến lược nhằm ngăn chặn, phát hiện, và loại bỏ các loại mã độc (malware) khỏi hệ thống máy tính và mạng. Mã độc là phần mềm có hạng cụ thể được thiết kế để gây hại hoặc thâm nhập vào hệ thống mà không được sự cho phép của người sử dụng. Các biện pháp phòng chống mã độc thường bao gồm:

- Sử dụng Phần mềm diệt vi-rút: Sử dụng các ứng dụng diệt vi-rút để quét và loại bỏ mã độc khỏi hệ thống. Phần mềm này thường được cập nhật định kỳ để nhận diện các mối đe dọa mới.

- Cập nhật hệ thống: Đảm bảo rằng hệ điều hành và các ứng dụng đều được cập nhật với bản vá bảo mật mới nhất để bảo vệ khỏi các lỗ hổng bảo mật.

+ Kiểm tra email cẩn thận: Hạn chế mở các email không cần thiết và không nhận diện được. Cảnh báo người dùng về nguy cơ của các tệp đính kèm và liên kết có thể chứa mã độc.

+ Sử dụng Tường lửa (Firewall): Kích hoạt và cấu hình tường lửa để kiểm soát và giám sát lưu lượng mạng, ngăn chặn các kết nối không mong muốn.

+ Sao lưu Dữ Liệu thường xuyên (backup): Thực hiện sao lưu đều đặn dữ liệu để có khả năng khôi phục nhanh chóng sau một tấn công và giảm thiểu mất mát thông tin.

+ Quản lý Quyền truy cập: Thiết lập quyền truy cập đặc biệt để giảm khả năng một mã độc có thể lây lan và gây hại trong hệ thống.

+ Đào tạo Người dùng: Cung cấp đào tạo đề phòng để người dùng có thể nhận diện và tránh các hành động có thể mở cửa cho mã độc, như mở email độc hại.

+ Sử dụng phần mềm an toàn: Lựa chọn và triển khai phần mềm chỉ từ các nguồn đáng tin cậy để giảm khả năng cài đặt mã độc từ phần mềm không an toàn.

2. Các chương trình diệt vi-rút

Dưới đây là Danh sách sản phẩm phòng chống mã độc đáp ứng yêu cầu triển khai giải pháp mã độc tập trung theo Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại; và có khả năng kết nối chia sẻ dữ liệu về mã độc theo hướng dẫn tại văn bản số 2290/BTTTT-CATTT, cập nhật đến tháng 10/2023, cụ thể:

1. Giải pháp tổng thể phòng chống vi-rút cho các cơ quan, doanh nghiệp Bkav Endpoint AI, Công ty Cổ phần phần mềm diệt vi-rút Bkav

2. Viettel Endpoint Detection & Response (VEDR), Công ty An ninh mạng Viettel, Tập đoàn Công nghiệp – Viễn thông Quân đội

3. CMC Malware Detection and Defence, Công ty TNHH An ninh An toàn thông tin CMC

4. Veramine Advanced Endpoint Security Suite, Công ty Veramine.

5. CyRadar Endpoint Detection and Response (CyRadar EDR), Công ty Cổ phần An toàn thông tin CyRadar

6. Kaspersky Endpoint Security for Business (KESB) và Kaspersky Security Centr (KSC), Công ty Kaspersky Lab SEA

7. FPT.EagleEye MDR, Công ty TNHH Hệ thống Thông tin FPT

8. VNPT Smart Incident Response, Công ty Công nghệ thông tin VNPT, Tập đoàn VNPT

9. McAfee Endpoint Security, Công ty Cổ phần tin học MI (nhà phân phối)

10. BCY Endpoint Security, Công ty TNHH Một thành viên 129, Ban Cơ yếu Chính phủ

11. Bitdefender Endpoint Security, Công ty TNHH Phát triển B (Việt Nam

12. F-Secure Business Suite Premium, Công ty Cổ phần Centect Interative

13. VSEC VADAR, Công ty Cổ phần An ninh mạng Việt Nam (VSEC)

14. Giải pháp phòng chống mã độc tập trung Trend Micro, Công ty Cổ phần phát triển phần mềm và Hỗ trợ công nghệ

15. Eset Endpoint Detection & Response (EEDR), Công ty TNHH Tài Nguyên HTECH Việt Nam

III. CẤU HÌNH AN TOÀN CHO USB ĐỂ PHÒNG CHỐNG VI-RÚT

USB thực sự linh hoạt và thường là công cụ mặc định để chia sẻ tệp và sạc thiết bị của chúng ta. Nhưng trong khi chúng ta sử dụng chúng một cách bình thường thì việc sử dụng USB cũng gặp một số thách thức về bảo mật.

Rất nhiều cơ quan, tổ chức đã yêu cầu và ra quy định không được cắm các USB vào các máy tính, máy trạm của cơ quan và vô hiệu hóa cổng USB trên các máy chủ, máy trạm và thiết bị có cổng kết nối USB.

Mọi người sẽ đặc câu hỏi, cắm USB vào máy tính có khả năng bị nhiễm vi-rút không? Câu trả lời: Chắc chắn là có.

Vậy có cách nào để giữ an toàn khi cắm USB vào thiết bị của bạn không? Tất nhiên là có.

Phần này chúng ta đi tìm hiểu để trả lời 02 câu hỏi này.

USB, hay Universal Serial Bus, là một tiêu chuẩn giao tiếp dùng để kết nối và truyền dữ liệu giữa máy tính và các thiết bị ngoại vi như máy in, ổ đĩa, điện thoại di động, và nhiều thiết bị khác. Thiết kế tiện lợi và khả năng tương thích rộng rãi đã làm cho USB trở thành giao tiếp chuẩn trên hầu hết các thiết bị điện tử ngày nay.

1. Tấn công USB là gì?

Cái này đơn giản. Tấn công USB gần như là bất kỳ hoạt động truyền, phát tán, lây lan phần mềm độc hại nào qua thiết bị USB. Có rất nhất kiểu tấn công phần mềm độc hại vào USB khác nhau có khả năng được thực hiện theo nhiều cách khác nhau. Dưới đây là những cái phổ biến nhất:

Thông qua ổ USB. USB có thể vô tình tải xuống một tệp bị nhiễm từ máy tính xách tay của ai đó, sau đó chuyển nó sang máy tính của bạn. Hoặc ổ USB có thể bị lây nhiễm có chủ đích, sau đó được trao trực tiếp hoặc gián tiếp cho nạn nhân. Giống như, thả vào bãi đậu xe để nạn nhân tìm thấy nó (nó được gọi là cuộc tấn công đánh rơi USB và phổ biến hơn bạn tưởng tượng).

Thông qua cổng USB trong các thiết bị hoặc trạm sạc. Điều này được gọi là juice-jacking và không có bất kỳ thông tin hay hướng dẫn nào về cách bảo vệ USB khỏi vi-rút trong tình huống này. Cách duy nhất để giữ an toàn là tránh sử dụng các trạm sạc công cộng. Chỉ cần mang theo bộ sạc cắm thông thường bên mình hoặc luôn mang theo một cục sạc dự phòng bên mình.

2. Các Loại tấn công USB

Sau đây chúng ta đi vào chi tiết một số tình huống tiêu biểu

a). Tấn công AutoRun

- Mô Tả: Loại tấn công này sử dụng tính năng AutoRun của hệ điều hành để tự động thực thi mã độc hại từ USB khi thiết bị được kết nối.

- Biện Pháp Phòng Chống: Tắt chế độ AutoRun trên hệ điều hành và kiểm tra định kỳ để đảm bảo sự an toàn.

b) Tấn công mã độc hại

- Mô Tả: Mã độc hại có thể ẩn trong các tệp tin trên USB và tự động thực thi khi người dùng mở tệp tin đó.

- Biện Pháp Phòng Chống: Sử dụng phần mềm diệt vi-rút để quét và loại bỏ mã độc hại từ USB.

c) Tấn công đánh cắp thông tin

- Mô Tả: USB có thể chứa các phần mềm gián điệp hoặc keyloggers để đánh cắp thông tin quan trọng từ máy tính khi kết nối.

- Biện Pháp Phòng Chống: Mã hóa dữ liệu trên USB và thực hiện kiểm tra định kỳ để phát hiện các hoạt động đáng ngờ.

d) Tấn Công Edu-Phishing

- Mô Tả: USB được sử dụng để truyền tải tệp tin giáo dục giả mạo, giả mạo người sử dụng và làm cho họ mở các tệp tin chứa mã độc hại.

- Biện Pháp Phòng Chống: Giáo dục người sử dụng về rủi ro của Edu-Phishing và cảnh báo về việc mở tệp tin từ nguồn không đáng tin cậy.

đ) Tấn công tự động hóa

- Mô Tả: USB có thể chứa các công cụ tự động hóa tấn công, sử dụng kỹ thuật như BadUSB để tận dụng các lỗ hổng trong hệ điều hành và ứng dụng.

- Biện Pháp Phòng Chống: Cập nhật hệ điều hành và ứng dụng, cũng như sử dụng phần mềm diệt vi-rút để phát hiện và ngăn chặn các công cụ tự động hóa.

e) Cách mà vi-rút USB tấn công thiết bị

- Mô tả: Một vi-rút USB có thể tấn công vào thiết bị qua nhiều cách khác nhau. Dưới đây là ba loại tấn công malware thông qua USB phổ biến:

+ Mã độc hại: Đây là loại tấn công USB phổ biến nhất. Khi người dùng nhấp chuột vào một tệp trên một ổ đĩa USB bị nhiễm vi-rút, nó sẽ khởi chạy mã độc hại để tải xuống phần mềm độc hại từ internet.

+ Social Engineering: Khi người dùng mở tệp cần thiết trên một USB bị nhiễm vi-rút, họ sẽ bị chuyển hướng đến một trang web lừa đảo được thiết kế để lừa họ nhập thông tin cá nhân và thông tin đăng nhập (mật khẩu email, chi tiết thẻ tín dụng, v.v.).

+ Giả mạo thiết bị giao diện người dùng (HID): Được thiết kế giống một ổ đĩa USB, thiết bị này giải mạo máy tính của người dùng để cho rằng nó là một bàn phím. Khi kết nối, nó sẽ ra lệnh cho thiết bị cấp quyền truy cập từ xa cho hacker.

- Một số cách phòng chống

+ Tắt chế độ AutoRun

Một trong những biện pháp quan trọng nhất để ngăn chặn vi-rút từ USB là tắt chế độ AutoRun. Chế độ này có thể tự động chạy các tệp tin khi USB được kết nối, tạo điều kiện lý tưởng cho các tập tin có chứa mã độc hại tự động thực thi. Để tắt chế độ này, bạn có thể thực hiện các bước sau trên Windows:

Mở "Run" bằng cách nhấn tổ hợp phím Win + R.

Gõ "gpedit.msc" và nhấn Enter để mở Group Policy Editor.

Trong cửa sổ Group Policy Editor, điều hướng đến "Computer Configuration" > "Administrative Templates" > "Windows Components" > "AutoPlay Policies."

Chọn "Turn off AutoPlay" và chọn "Enabled."

+ Sử Dụng Phần Mềm Diệt Vi-rút

Cài đặt một phần mềm diệt vi-rút chất lượng là một phần quan trọng của chiến lược bảo vệ USB của bạn. Phần mềm này sẽ quét và loại bỏ mọi đoạn mã độc hại có thể tồn tại trên USB. Đảm bảo rằng phần mềm của bạn được cập nhật định kỳ để phát hiện và loại bỏ các mối đe doạ mới nhất.

+ Mật Khẩu cho USB

Đặt mật khẩu cho USB là một cách hiệu quả để bảo vệ dữ liệu của bạn khỏi truy cập trái phép. Nếu USB của bạn hỗ trợ chức năng mật khẩu, hãy kích hoạt và

đặt mật khẩu mạnh để ngăn chặn người không mong muốn truy cập vào dữ liệu của bạn.

+ Sử Dụng Tường Lửa

Tường lửa là một tuyến phòng thủ quan trọng để ngăn chặn truy cập không mong muốn vào USB. Cấu hình tường lửa để kiểm soát truy cập từ các thiết bị di động và ngăn chặn các kết nối không mong muốn.

+ Cập Nhật Hệ Điều Hành và Phần Mềm

Đảm bảo rằng hệ điều hành của bạn và các chương trình an ninh đều được cập nhật. Các bản cập nhật thường bao gồm các bản vá an ninh mới nhất, giúp bảo vệ hệ thống của bạn khỏi các lỗ hổng bảo mật.

+ Kiểm Tra Thường Xuyên

Thực hiện kiểm tra định kỳ để đảm bảo rằng không có phần mềm độc hại nào trên USB của bạn. Nếu phát hiện bất kỳ dấu hiệu nào của mối đe doạ, hãy xử lý ngay lập tức để ngăn chặn sự lan truyền.

+ Bật Windows Defender

Windows Defender là công cụ chống malware tích hợp trong Windows 10. Đảm bảo rằng nó đang hoạt động và được cập nhật để có khả năng phòng ngừa cao.

+ Sử Dụng BitLocker

BitLocker là một công cụ tích hợp trong Windows 10 giúp bạn mã hóa đĩa và USB. Nếu sử dụng phiên bản Pro hoặc Enterprise, hãy sử dụng BitLocker để bảo vệ dữ liệu.

+ Mã Hóa Dữ Liệu

Mã hóa dữ liệu là một biện pháp an ninh quan trọng để bảo vệ dữ liệu trên USB khỏi việc truy cập trái phép. Sử dụng công nghệ mã hóa để biến dữ liệu thành dạng không thể đọc được nếu không có khóa phù hợp. Điều này đặc biệt quan trọng khi USB của bạn có chứa thông tin nhạy cảm.

Tóm lại, làm thế nào để ngăn chặn các cuộc tấn công USB?

Trước hết, hãy nhớ rằng chúng ta chịu trách nhiệm về sự an toàn của chính mình, vì vậy hãy tuân thủ các quy tắc cơ bản sau để giữ an toàn:

- Giữ riêng USB cá nhân và công việc

- Nếu bạn không biết ổ USB đến từ đâu thì đừng sử dụng nó

- Thỉnh thoảng thay đổi và cập nhật các phím USB của bạn

- Thường xuyên quét ổ USB và thiết bị của bạn bằng phần mềm chống vi-rút.

- Tắt tính năng tự động chạy trên tất cả các thiết bị của bạn (điều này sẽ ngăn mọi tệp không xác định khởi chạy mà bạn không biết hoặc không cho phép)

- Nếu bạn thực sự cần lấy thông tin từ một nguồn USB không xác định, hãy cắm nó vào một loại thiết bị đệm nào đó và quét phần mềm độc hại

- Nếu bạn đã cắm một ổ USB đáng ngờ vào, hãy ngắt kết nối Internet ngay lập tức để ngăn mọi hoạt động tải xuống và khởi động lại thiết bị của bạn

- Hoặc tránh sử dụng thẻ nhớ USB mọi lúc! Đùa thôi. Thay vào đó hãy mua phần mềm chống vi-rút chất lượng.

IV. BẢO ĐẢM AN TOÀN VÀ XỬ LÝ TỆP TIN TRƯỚC KHI SỬ DỤNG (VĂN BẢN, MEDIA…)

Trong thời đại kỹ thuật số ngày nay, việc bảo vệ dữ liệu trở nên ngày càng quan trọng. Một trong những khía cạnh quan trọng nhất của an ninh thông tin là bảo đảm an toàn và xử lý tệp tin trước khi chúng ta sử dụng chúng. Điều này áp dụng cho cả tệp tin văn bản và media, đặt ra một loạt các thách thức và cơ hội để tăng cường bảo mật thông tin.

Quy trình bảo đảm an toàn tệp tin như sau:

1. Quét mã độc

Sử dụng phần mềm diệt vi-rút mạnh mẽ và được cập nhật định kỳ để quét mọi tệp tin được tải lên vào hệ thống. Điều này giúp phát hiện và loại bỏ mọi mã độc có thể gây hại cho dữ liệu và hệ thống.

2. Kiểm tra chữ ký số

Xác minh chữ ký số của tệp tin để đảm bảo tính toàn vẹn và độ tin cậy. Điều này ngăn chặn việc sửa đổi không mong muốn và đảm bảo rằng tệp tin đến từ nguồn đáng tin cậy.

3. Đặt mật khẩu

Áp dụng mật khẩu cho các tệp tin nhạy cảm để ngăn chặn truy cập trái phép và bảo vệ dữ liệu quan trọng khỏi sự xâm phạm.

4. Xử lý tệp tin văn bản, tệp media,…

- Kiểm tra ngôn ngữ và định dạng

Xác định ngôn ngữ và định dạng của tệp tin văn bản để đảm bảo tính tương thích với hệ thống và ứng dụng sử dụng. Điều này giúp tránh lỗi không mong muốn khi mở và xử lý tệp tin.

- Kiểm Tra Metadata

Loại bỏ thông tin cá nhân hoặc metadata không mong muốn từ tệp tin media để bảo vệ quyền riêng tư của cá nhân và tổ chức.

- Sử dụng công nghệ tự động hóa ngăn chặn phần mềm độc hại

Triển khai các công nghệ tự động hóa để nhận diện và ngăn chặn tự động các tấn công mạng của phần mềm mã độc. Điều này giúp giảm thiểu thời gian phản ứng và tăng cường khả năng đối phó với các mối đe doạ.

5. Chính sách an toàn dữ liệu

- Xây dựng chính sách an toàn dữ liệu:

Phát triển và duy trì chính sách an ninh dữ liệu chi tiết, đồng thời đảm bảo rằng mọi thành viên trong tổ chức được đào tạo về việc thực hiện chính sách này.

- Đào tạo người sử dụng:

Tổ chức đào tạo định kỳ cho người sử dụng về các nguy cơ an ninh và cách xử lý thông tin đúng cách. Điều này giúp xây dựng ý thức an ninh trong tổ chức và giảm nguy cơ từ sơ hở của con người./.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG