Bạn đã biết bao nhiêu loại malware và đã biết cách phòng chống chúng chưa?

Tội phạm máy tính sử dụng rất nhiều phần mềm độc hại (malware) khác nhau để tấn công hệ thống. Dưới đây là một số loại phần mềm độc phổ biến nhất và cách phòng chống.

Các chuyên gia bảo mật CNTT thường sử dụng các thuật ngữ chung mà không định nghĩa chính xác ý nghĩa của chúng. Điều đó có thể khiến người dùng băn khoăn về những câu hỏi cơ bản như *phần mềm độc là gì? hay phần mềm độc và virus khác nhau như thế nào? Crimemare và malware có gì giống nhau? Và phần mềm gián điệp (ransomware) được hiểu chính xác là gì?* Trong bài viết dưới đây, chúng tôi sẽ giải đáp hết những thắc mắc này.

Vậy Malware là gì?

Malware thực chất là tên viết tắt của malicious software. Về cơ bản, malware là những phần mềm mà bạn không muốn xuất hiện trên máy tính hay thiết bị di động của mình. Rõ ràng đây là một nhóm phần mềm lớn bao gồm nhiều loại phần mềm độc khác nhau. Malware gồm virus, worm, trojan, adware và ransomware.....

Các mục dưới đây sẽ cung cấp định nghĩa cho một số loại malware phổ biến nhất.

Adware

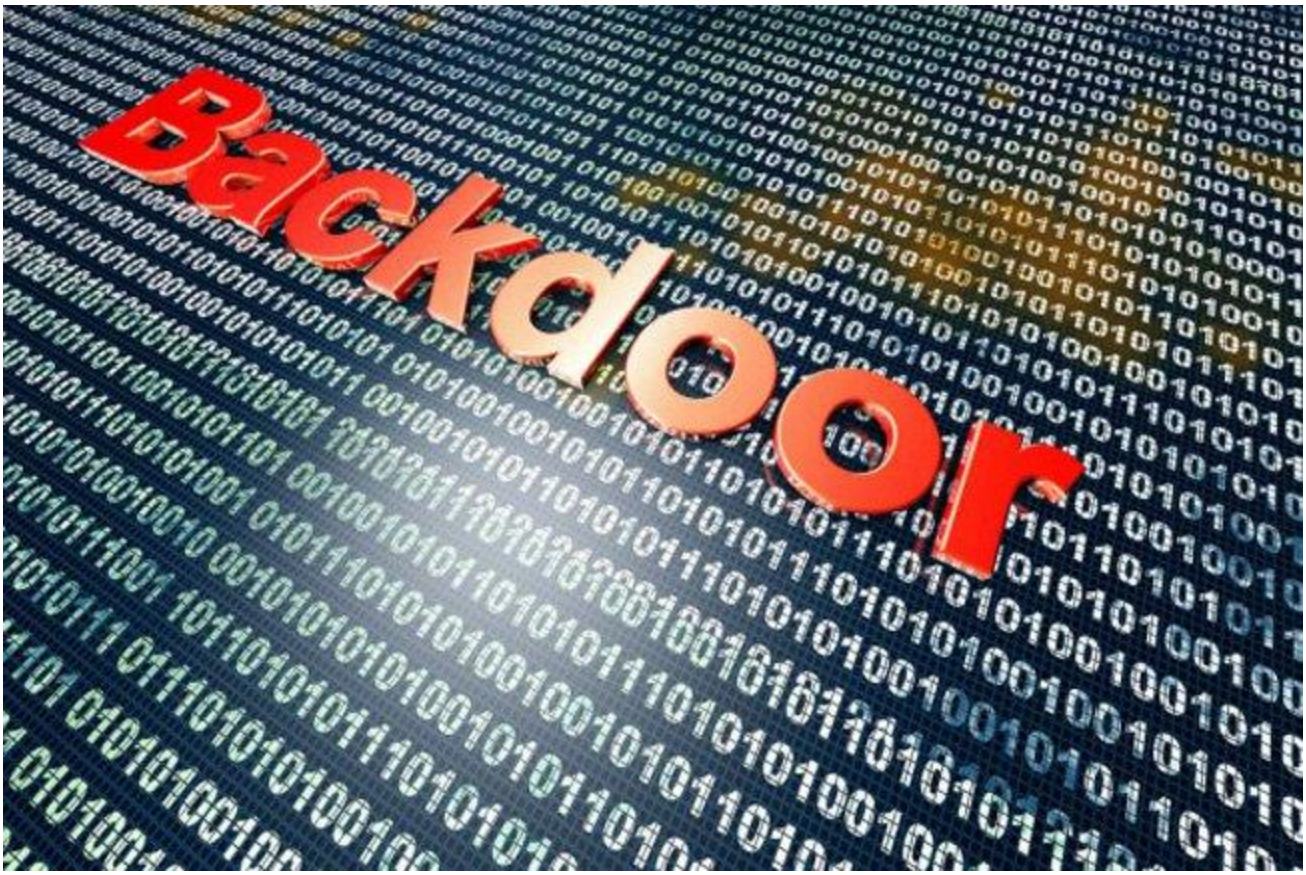
Adware là một loại phần mềm độc hại tải xuống hoặc hiển thị pop-up quảng cáo trên thiết bị của người dùng. Thông thường, Adware không lấy cắp dữ liệu từ hệ thống, nhưng nó buộc người dùng phải xem những quảng cáo mà họ không muốn trên hệ thống. Một số hình thức quảng cáo cực kì gây khó chịu cho người dùng đó là tạo ra pop-up trên trình duyệt mà không thể đóng lại được. Đôi khi người dùng tự lây nhiễm adware được cài đặt mặc định khi tải về những ứng dụng khác mà không hề hay biết.

Vậy làm cách nào để chặn các adware này?

Giải pháp là cài đặt anti-malware có khả năng chặn các phần mềm quảng cáo. Vô hiệu hóa pop-up trên các trang trình duyệt và quan sát quá trình cài đặt các phần mềm mới, đảm bảo bỏ chọn những ô cài đặt phần mềm bổ sung mặc định.

Backdoor

Backdoor là một chương trình bí mật có thể truy cập thiết bị hay hệ thống mạng của người dùng. Thông thường, các nhà sản xuất thiết bị hay phần mềm tạo ra backdoor trong sản phẩm của họ hoặc cố ý để nhân viên công ty xâm nhập vào hệ thống thông qua việc thực hành mã hóa. Backdoor cũng có thể được cài đặt bởi các phần mềm độc hại khác như virus hoặc rootkit.



Cách phòng chống backdoor

Backdoor là một trong những mối đe dọa lớn nhất rất khó để phòng chống. Các chuyên gia cho biết: chiến lược bảo vệ tốt nhất là cài đặt firewall, phần mềm chống malware, giám sát mạng, ngăn chặn xâm nhập và bảo vệ dữ liệu.

Bot và botnet

Nói chung, bot là phần mềm chạy nhiệm vụ tự động, cũng có nhiều loại bot có ích. Ví dụ, các chương trình thu thập dữ liệu Internet và các trang chỉ mục cho các công cụ tìm kiếm và chatbot đôi khi cũng trả lời các câu hỏi của khách hàng trên website công ty.

Tuy nhiên, khi thảo luận về bảo mật CNTT, bot thường được dùng để chỉ một thiết bị đã bị nhiễm phần mềm độc có thể gây hại máy tính mà người dùng không hề cho phép hay biết đến. Bonet là một nhóm lớn bao gồm các bot được tập trung lại để làm cùng một nhiệm vụ. Những kẻ tấn công thường sử

dụng bonet để gửi hàng loạt các tin nhắn spam, lừa đảo hoặc thực hiện tấn công từ chối dịch vụ (distributed denial of service - DDoS) tới các trang web. Gần đây, các Attacker đã bắt đầu kết hợp các thiết bị mạng lưới vạn vật kết nối Internet (IoT) vào các cuộc tấn công bonet của họ.

Hướng dẫn cách chống lại bonet

Các tổ chức có thể giúp ngăn chặn máy tính khỏi việc trở thành một phần của bonet bằng cách cài đặt phần mềm anti-malware, sử dụng firewall, cập nhật phần mềm liên tục và buộc người dùng sử dụng mật khẩu mạnh. Ngoài ra, phần mềm giám sát mạng có thể hữu ích trong việc xác định hệ thống đã trở thành một phần của bonet chưa. Bên cạnh đó, bạn cũng nên thường xuyên thay đổi mật khẩu mặc định cho bất kì thiết bị IoT nào mà bạn cài đặt.

Browser hijacker

Browser hijacker, hay còn được gọi là Hijackware có thể làm thay đổi hành vi trình duyệt web của bạn, ví dụ như bằng cách gửi đến người dùng một trang tìm kiếm mới, thay đổi trang chủ, cài đặt các thanh công cụ, chuyển hướng người dùng tới các trang web không mong muốn và hiển thị quảng cáo mà người dùng không muốn xem. Các Attacker thường kiếm tiền từ loại phần mềm độc này qua việc nhận phí quảng cáo. Họ cũng có thể sử dụng trình duyệt bị tấn công để chuyển hướng người dùng tới các trang web tải phần mềm độc hại hơn vào hệ thống.

Cách ngăn chặn browser hijacker

Phải rất cẩn thận khi cài đặt một phần mềm mới trên hệ thống bởi rất nhiều browser hijacker sẽ chèn thêm vào phần mềm bạn đã cài đặt, ví dụ như phần mềm quảng cáo. Ngoài ra, bạn nên cài đặt và chạy phần mềm anti-malware trên hệ thống và cài đặt bảo mật cho trình duyệt lên cấp độ cao hơn.

Bug

Bug là một thuật ngữ chung chung chỉ lỗ hổng trong một đoạn code. Tất cả các phần mềm đều có lỗi nhưng hầu như không được chú ý đến hay chỉ gây những khó chịu nhỏ. Tuy nhiên, cũng có lúc bug đại diện cho một lỗ hổng bảo mật nghiêm trọng, sử dụng phần mềm chứa loại bug này để tấn công hệ thống của người dùng.

Cách phòng chống bug

Cách tốt nhất để ngăn chặn cuộc tấn công từ việc khai thác lỗ hổng bảo mật trong phần mềm là cập nhật các phần mềm liên tục. Khi Attacker biết đến các lỗ hổng thì các nhà cung cấp thường nhanh chóng phát hành một bản vá để ngăn ngừa thiệt hại cho hệ thống của khách hàng.

Các tổ chức muốn ngăn chặn lỗi bảo mật trên phần mềm mà họ viết thì nên thực hiện các phương pháp mã hóa an toàn và sửa lỗi càng sớm càng tốt. Họ cũng sẽ thưởng cho những nhà nghiên cứu nào tìm ra lỗ hổng bảo mật trong các sản phẩm của họ.

Crimeware

Một số nhà cung cấp sử dụng thuật ngữ "crimeware" để chỉ phần mềm độc hại được sử dụng để phạm tội, thường là một tội phạm liên quan đến lợi ích tài chính. Cũng giống như malware, crimeware là một phạm trù rộng gồm hàng loạt các phần mềm độc khác.

Làm cách nào để ngăn chặn crimeware?

Để bảo vệ hệ thống của bạn khỏi crimeware, bạn nên thực hiện các biện pháp bảo mật tốt nhất, bao gồm sử dụng firewall, ngăn chặn xâm nhập, giám sát mạng và đăng nhập, bảo vệ dữ liệu và các thông tin bảo mật, hệ thống giám

sát an toàn mạng (SIEM) và các công cụ bảo mật thông minh. Bạn cũng nên sử dụng mật khẩu mạnh và cập nhật mật khẩu thường xuyên.

Keylogger

Keylogger là trình theo dõi thao tác bàn phím ghi lại tất cả các phím mà người dùng nhấn vào, bao gồm email, các tài liệu và password đã nhập cho mục đích nhất định. Thông thường, những kẻ tấn công thường dùng loại phần mềm độc này để lấy mật khẩu và đột nhập vào hệ thống mạng hoặc account người dùng. Tuy nhiên, các nhà tuyển dụng đôi khi cũng sử dụng keylogger để xác định xem nhân viên của họ có bất kì hành vi phạm tội trong hệ thống của công ty không.

Cách phòng chống Keylogger

Thay mật khẩu là một trong những cách tốt nhất để ngăn ngừa hoặc giảm nhẹ thiệt hại gây ra bởi keylogger. Hãy nhớ sử dụng mật khẩu mạnh và cập nhật thường xuyên. Ngoài ra, bạn cũng nên sử dụng network firewall và giải pháp chống phần mềm độc hại.

Ứng dụng di động độc hại

Không phải tất cả các ứng dụng có sẵn trên App Store của Apple hay Google Play đều là ứng dụng an toàn. Mặc dù các nhà khai thác ứng dụng đã cố gắng ngăn chặn các ứng dụng độc hại nhưng một số vẫn trót lọt. Những ứng dụng này có thể ăn cắp thông tin người dùng, tống tiền hoặc cố truy cập vào hệ thống mạng của công ty, buộc người dùng xem những quảng cáo không mong muốn hay tham gia vào các hoạt động không mong muốn khác.

Cách chặn các ứng dụng di động độc hại

Trang bị kiến thức cho người dùng là một trong những cách mạnh nhất để ngăn chặn các ứng dụng di động độc hại bởi người dùng có thể tránh những phần mềm này bằng cách không download hay truy cập các app store của bên thứ ba và cẩn thận khi download các ứng dụng mới vào thiết bị di động. Ứng

dụng chống phần mềm độc hại trên di động cũng giúp người dùng tránh khỏi các ứng dụng xấu này.

Các tổ chức có thể chặn các ứng dụng mã độc này bằng cách tạo ra chính sách bảo mật di động mạnh mẽ và triển khai giải pháp bảo mật di động để thực thi các chính sách đó

Phishing

Phishing là một loại tấn công email nhằm lừa người dùng tiết lộ mật khẩu, tải file đính kèm hoặc truy cập một trang web đã được cài phần mềm độc trên hệ thống của chúng. Spear phishing là chiến dịch lừa đảo nhắm vào người dùng hoặc tổ chức cụ thể.

Cách phòng chống phishing

Bởi phishing dựa trên kỹ thuật social engineering (thuật ngữ bảo mật để lừa người dùng làm một việc gì đó) nên việc trang bị kiến thức cho người dùng là một trong những biện pháp tốt nhất để tránh bị tấn công. Người dùng nên triển khai các giải pháp chống thư rác và chống phần mềm độc hại cũng như không được tiết lộ thông tin cá nhân hoặc mật khẩu email. Ngoài ra, họ cần được cảnh báo về việc cẩn thận khi tải các file đính kèm hay nhấp vào các liên kết trong thư ngay cả khi chúng xuất hiện từ một nguồn phổ biến bởi những kẻ tấn công thường giả dạng một công ty hay một người nào đó mà người dùng quen biết. Email cũng thường là đối tượng Ransomware hoạt động.

Ransomware

Trong những năm gần đây, Ransomware nhanh chóng trở thành một trong những loại phần mềm độc hại phổ biến nhất. Trên thực tế, theo báo cáo của Malwarebytes, sự cố do Ransomware gây ra đã tăng 267% từ giữa tháng 1 đến tháng 11 năm 2016. Các biến thể phần mềm phổ biến nhất này sẽ khóa hệ thống, chặn bất kì thao tác nào thực hiện cho đến khi nạn nhân trả một khoản tiền chuộc cho những kẻ tấn công. Các dạng Ransomware khác sẽ đe dọa công khai các thông tin không hay về người dùng, chẳng hạn như hoạt động của người dùng trên các trang web người lớn nếu người dùng không trả tiền chuộc.

Cách ngăn chặn nhiễm Ransomware

Thông thường các tổ chức có thể giảm bớt các cuộc tấn công bằng cách cập nhật các bản sao lưu. Thêm vào đó, các tổ chức nên đào tạo người dùng về các mối đe dọa, vá phần mềm khi cần thiết và thiết lập các phương pháp bảo mật thông thường. Tuy nhiên, một số loại Ransomware được cho là rất khó để chặn, nên rất nhiều cá nhân và tổ chức đã phải mất tiền oan.

Phần mềm bảo mật giả mạo Rogue

Rogue security software thường được mô tả như một dạng của Ransomware và Scareware. Phần mềm này đánh lừa người dùng rằng hệ thống máy tính có vấn đề về bảo mật và gợi ý họ mua một phần mềm bảo mật giả mạo để giải quyết vấn đề. Trên thực tế, thay vì cung cấp tính năng bảo mật, các phần mềm giả mạo thường cài vào hệ thống những phần mềm độc hại hơn.

Cách phòng chống Rogue security software

Cũng giống như hầu hết các phần mềm độc hại khác, bạn có thể chặn các phần mềm bảo mật giả bằng cách cài firewall hay sử dụng các phương pháp phòng tránh như đối với Phishing.

Rootkit

Rootkit là một trong những loại malware nguy hiểm nhất bởi chúng cho phép những kẻ tấn công có quyền truy cập cấp admin vào hệ thống mà người dùng không hay biết. Khi kẻ tấn công truy cập vào hệ thống, chúng có thể làm bất cứ điều gì với hệ thống, gồm các hoạt động ghi âm, thay đổi cài đặt hệ thống, truy cập dữ liệu và tấn công lên hệ thống khác. Các cuộc tấn công nổi tiếng như Stuxnet và Flame là hai ví dụ điển hình của rootkit.

Cách phòng tránh

Cách phòng tránh rootkit cũng tương tự với các loại phần mềm độc trên. Tuy nhiên có một điều đáng chú ý là nếu rootkit lây nhiễm vào hệ thống, người dùng rất khó để phát hiện và gỡ bỏ. Trong nhiều trường hợp, bạn phải xóa sạch ổ cứng và bắt đầu lại từ đầu để loại bỏ nó.

Spam

Trong bảo mật CNTT, Spam là những email không mong muốn. Thông thường, thư rác bao gồm những quảng cáo không cần thiết, nhưng cũng có thể nó chứa các liên kết hoặc file đính kèm cài đặt phần mềm độc vào hệ thống người dùng.

Cách ngăn chặn

Hầu hết các giải pháp hoặc dịch vụ email đều bao gồm những tính năng chống spam. Sử dụng những cách đó là phương thức tốt nhất để ngăn tin nhắn spam xuất hiện trên hệ thống.

Spyware

Phần mềm gián điệp Spyware là những loại phần mềm thu thập thông tin về người dùng mà họ không hề hay biết hoặc đồng ý. Ví dụ, website bật cookies theo dõi trình duyệt web của người dùng có thể được coi là một hình thức của Spyware. Các loại phần mềm Spyware khác có thể ăn cắp thông tin của cá nhân hoặc doanh nghiệp. Đôi khi, các cơ quan chính phủ và lực lượng cảnh sát cũng sử dụng phần mềm gián điệp này để điều tra nghi phạm hoặc chính phủ nước ngoài.

Cách phòng chống

Bạn có thể cài đặt phần mềm anti-spyware trên máy tính, hoặc các gói anti-virus và anti-malware cũng chứa tính năng ngăn spyware. Tương tự, bạn cũng nên sử dụng firewall và cẩn thận mỗi khi cài phần mềm trên hệ thống.

Trojan

Trong thần thoại Hy Lạp, một số chiến binh trong quân đội Hy Lạp ẩn náu bên trong một con ngựa gỗ ngoài thành Troy sau đó rút hết quân. Khi người Trojan mang con ngựa này vào thành vì nghĩ đây là chiến lợi phẩm, các chiến binh Hy Lạp chui khỏi bụng ngựa và mở cổng thành cho quân Hy Lạp vào tấn công và chiếm giữ thành Troy. Trong bảo mật máy tính, con ngựa Trojan hay còn được gọi tắt là Trojan - là một phần mềm độc ẩn mình dưới một chương trình vô hại nhưng thực chất lại phục vụ cho một mục đích xấu. Ví dụ

Trojan có thể xuất hiện dưới dạng một trò chơi miễn phí, nhưng khi đã được cài đặt, nó có thể phá hủy ổ cứng của bạn, ăn cắp dữ liệu, cài đặt phần mềm độc backdoor hoặc thực hiện các hành động gây hại khác.

Cách ngăn chặn

Tương tự các phương pháp phòng chống phần mềm độc khác.

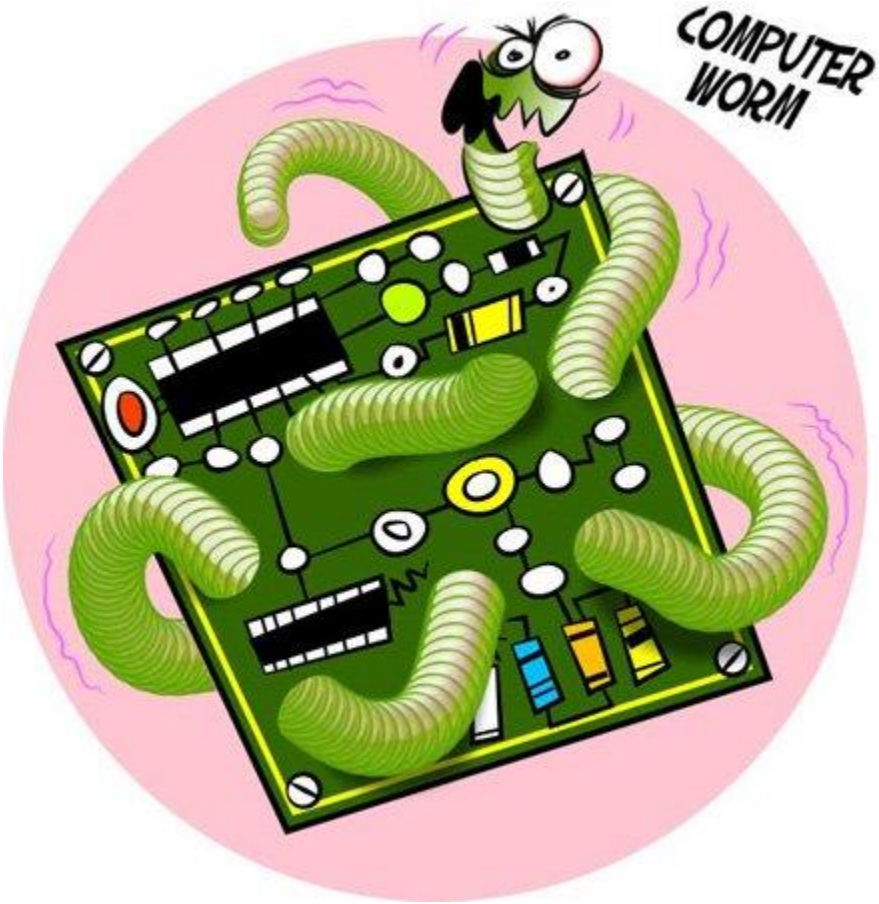
Virus

Đôi khi người ta sử dụng từ "virus" và "malware" để thay thế cho nhau, nhưng thực ra virus là một loại cụ thể của malware. Để được coi là virus, phần mềm độc hại phải lây nhiễm các chương trình khác và các hệ thống khác. Virus cũng thường thực hiện một số hoạt động không mong muốn trên hệ thống lây nhiễm như kết hợp các hệ thống thành botnet, gửi thư rác, ăn cắp thông tin thẻ tín dụng, mật khẩu hoặc khóa hệ thống.

Cách ngăn chặn tương tự các phần mềm độc hại khác.

Worm

Worm được tạo ra tương tự như virus vì nó tự lây lan chính nó, nhưng một điểm khác là nó không lây nhiễm sang các chương trình khác. Thay vào đó, nó là một phần độc lập của các phần mềm độc hại, lây lan từ máy này sang máy khác hoặc từ mạng này sang mạng khác. Nó có thể gây ra các loại thiệt hại tương tự như virus trên hệ thống.



Cách phòng chống

Giống như virus, cách tốt nhất để tránh bị nhiễm Worm là sử dụng phần mềm diệt virus hoặc anti-malware. Cũng tương tự như đối với các loại phần mềm

độc khác, người dùng chỉ nên nhấp vào các liên kết email hay file đính kèm khi thực sự biết rõ về nội dung đó.

Còn loại Malware phổ biến nào mà Quản Trị Mạng chưa đề cập trong bài thì bạn có thể cho ý kiến bằng cách comment phía dưới nhé! Quản Trị Mạng mong rằng bài viết sẽ mang lại những thông tin hữu ích cho bạn.