BẢN TIN NỘI BỘ
CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Tội phạm quốc tế đến Việt Nam hack thẻ ATM, tẩu tán bằng tiền ảo

Ngân hàng và hệ thống thẻ ATM đang là mục tiêu của tội phạm mạng

Trong 6 tháng đầu năm 2019, cơ quan chức năng đã phát hiện trên 2.500 trang tin, cổng thông tin điện tử tên miền quốc gia bị tấn công, hàng trăm ngàn máy tính bị nhiễm mã độc. Việt Nam đang xếp thứ 4 trong top 10 quốc gia bị kiểm soát bởi mạng máy tính ma botnet, bị tin tặc sử dụng để tấn công nước khác.

Hệ thống thông tin của các cơ quan, chính phủ, nhất là các tổ chức tài chính, ngân hàng là mục tiêu tấn công thường xuyên của giới tin tặc. Nhiều cuộc tấn công nhằm vào Sở giao dịch chứng khoán, các ngân hàng và tổ chức tài chính trong nước.

Chia sẻ tại hội thảo - triển lãm quốc gia về an ninh, bảo mật 2019 (Security World 2019), Đại tá Đỗ Anh Tuấn - Phó Cục trưởng Cục An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao (Bộ Công an) cho biết, trên thế giới, tình hình tội phạm mạng tấn công vào các ngân hàng đang có chiều hướng ngày càng gia tăng.

Tiêu biểu là vụ tấn công bằng phần mềm độc hại vào Ngân hàng Trung ương Bangladesh tháng 3/2016 gây thiệt hại 81 triệu USD. Ở cùng thời điểm, ngân hàng Banco del Austro (Ecuador) đã bị tin tặc tấn công gây thiệt hại lên tới 12 triệu USD. Bên cạnh đó là hàng ngàn vụ tấn công vào hệ thống ATM của các ngân hàng trên thế giới.

Tại Việt Nam, hoạt động của loại tội phạm trộm cắp thông tin thẻ, làm thẻ giả để chiếm đoạt tài sản (Skimming) diễn ra phức tạp. Người đứng đầu cơ quan chuyên trách về phòng chống tội phạm công nghệ cao của Bộ Công an cho rằng, với 70 triệu thẻ nội địa đang lưu hành, nếu chậm chuyển đổi từ thẻ từ sang thẻ chip, Việt Nam có thể trở thành tâm điểm của tội phạm thẻ.

Trong 2 năm 2018 và 2019, Bộ Công an đã phát hiện nhiều nhóm tội phạm người nước ngoài, chủ yếu là người Trung Quốc, Đài Loan, Philippines và các nước Châu Phi thực hiện hành vi chiếm đoạt hàng trăm triệu USD.

Nhóm người này nhập cảnh vào Việt Nam theo đường du lịch, thuê nhà và đường truyền Internet để tổ chức các hoạt động lừa đảo, làm giả thẻ ngân hàng để rút tiền hoặc thanh toán hóa đơn, dịch vụ qua hệ thống máy POS. Chỉ tính riêng từ đầu năm 2019 đến nay, lực lượng chức năng Bộ Công an đã bắt giữ trên 120 đối tượng người nước ngoài về hành vi phạm tội này.

Tiền ảo, tiền điện tử biến thành phương thức tẩu tán của tội phạm mạng

Hiện có 26 tổ chức cung ứng dịch vụ ví điện tử, 10.000 đơn vị chấp nhận thanh toán ví điện tử. Tính đến hết năm 2018, cả nước có 4,2 triệu ví đã liên kết với tài khoản ngân hàng, toàn hệ thống ngân hàng đã xử lý thông suốt 73 triệu tỷ đồng, mỗi ngày xử lý 300.000 tỷ đồng.

Sự đa dạng của các tổ chức tài chính cũng như loại hình thanh toán đã gây không ít khó khăn cho cơ quan quản lý trong việc kiểm soát dòng tiền của tội phạm mạng, tội phạm công nghệ cao trong ngành tài chính, ngân hàng.

Theo Đại tá Đỗ Anh Tuấn, một trong những nguyên nhân dẫn đến tình hình tội phạm công nghệ cao diễn biến phức tạp là sự phát triển quá nhanh của khoa học công nghệ. Tội phạm luôn tận dụng những công nghệ mới nhất để thực hiện hành vi phạm tội. Trong khi đó, trang thiết bị và kiến thức về khoa học công nghệ của Bộ Công an còn nhiều hạn chế.

Trong gian đoạn vừa qua, Bộ Công an đặc biệt chú ý đến loại tội phạm lợi dụng hình thức kinh doanh đa cấp để lừa đảo tài chính như Pincoin và iFan. Theo tố cáo của các nạn nhân, tổng số tiền mà bọn tội phạm chiếm đoạt có thể lên tới 15.000 tỷ đồng, tương đương với thu nhập một vài tỉnh.

Đại tá Đỗ Anh Tuấn cũng nhắc đến vụ lừa đảo liên quan đến HTX đào tiền Skymining, tội phạm đã lợi dụng sự cả tin và hám lời của một bộ phận người dân để huy động tiền nhằm mua những máy đào tiền ảo. Mỗi máy đào trị giá khoảng 5.000 USD. Người tham gia cũng phải bỏ chi phí để Skymining vận hành hệ thống máy đào này.

Ông Đỗ Anh Tuấn cũng cho rằng, sự xuất hiện của nhiều hình thức thanh toán và loại tài sản mới mang tới những thách thức đối với cơ quan quản lý. Đó là việc phải quản lý thế nào đôi với tiền ảo và tài sản ảo?

Trong khi đó, các tổ chức tội phạm đang lợi dụng tiền ảo và tài sản ảo sử dụng để tài trợ cho khủng bố, mua bán ma túy, vũ khí và cả hành vi rửa tiền. Những giao dịch bằng tiền ảo có tính ẩn danh cao đã trở thành một công cụ đắc lực cho hoạt động của giới tội phạm mạng.

Do vậy, cơ quan quản lý nhà nước cần sớm tìm ra các giải pháp để nhận diện rõ hơn về hành vi và phương thức của các loại tội phạm mới, từ đó mới có thể tìm ra những biện pháp đấu tranh thích hợp.

Khuyến nghị:

Phòng ATTT khuyến nghị: không tham gia vào các hoạt động đào tiền ảo, đề cao cảnh giác khi sử dụng thẻ ATM để tránh bị lộ thông tin dẫn đến bị hack và mất tiền trong thẻ.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/toi-pham-mang-tan-cong-rut-tien-tu-the-atm-tau-tan-bang-tien-ao-535959.html

2. Google: xác thực 2 yếu tố có thể ngăn chặn 100% hack bot tự động

Nhiều người phàn nàn rằng xác thực hai yếu tố là một tính năng khá phiền nhiễu, thậm chí còn gây khó khăn trong nhiều tình huống. Thế nhưng không phải ngẫu nhiên mà xác thực hai yếu tố lại là một trong những biện pháp bảo mật cơ bản được sử dụng phổ biến nhất trên thế giới. Nguyên nhân chẳng có gì "bí hiểm", đó là nhờ vào hiệu quả thực tế mà nó mang lại. Nếu bạn có bất kỳ nghi ngờ nào về việc liệu tính năng xác thực hai yếu tố có thực sự giúp bạn an toàn hơn nhiều hay không, hãy tham khảo dữ liệu sau đây của Google để xua tan mọi sự ngờ vực từ trước đến nay.

Có thể nhiều người trong số chúng ta vẫn đang sử dụng xác thực hai yếu tố nhưng lại không hề hay biết, xin được nhắc lại đôi chút về tính năng bảo mật này. Về cơ bản, xác thực hai yếu tố (2FA) là một phương thức bảo mật yêu cầu hai cách khác nhau để chứng minh danh tính của bạn. Khác với xác thực một yếu tố "cổ lỗ sĩ", xác thực hai yếu tố sẽ yêu cầu sử dụng thêm một lớp bảo mật bổ sung để chứng minh người đăng nhập vào tài khoản hoặc thiết bị thực sự là người giữ quyền sử dụng tài khoản hoặc thiết bị đó. Ngay cả khi ai đó đánh cắp hoặc đoán được ra mật khẩu của bạn, họ vẫn sẽ không thể giành được quyền truy cập thông tin của bạn nếu không sở hữu thông tin bảo mật thứ cấp. Thông tin bảo mật thứ cấp này có thể là một đoạn mã xác thực riêng biệt được gửi đến thiết bị mà bạn đã đăng ký trước đó. Nếu yêu cầu mức độ bảo mật cao hơn, bạn thậm chí có thể lấy một thiết bị vật lý kết nối với máy tính để xác minh danh tính của mình. Lấy ví dụ đơn giản, các hoạt động thanh toán bằng thẻ tín dụng hay chuyển khoản ngân hàng hiện nay không chỉ yêu cầu thẻ, mật khẩu đăng nhập, mà còn yêu cầu thêm cả mã PIN, chữ ký, ID, hoặc mã xác thực. Để hiểu thêm về tính năng bảo mật này, bạn có thể tham khảo bài viết: "Xác thực hai yếu tố là gì và tại sao bạn nên sử dụng nó".

Một nhà cung cấp dịch vụ lớn như Google đương nhiên có hỗ trợ các hình thức 2FA và nhiều phương pháp bảo mật khác. Sau nhiều năm triển khai tính năng bảo mật này, công ty đã quyết định hợp tác với các nhà nghiên cứu đến từ Đại học New York và Đại học California, San Diego thực hiện một dự án nghiên cứu kéo dài 12 tháng nhằm xem xét mức độ hiệu quả của 2FA.

Theo đó, việc nhận được mã SMS xác thực thứ cấp đã giúp ngăn chặn gần như 100% các cuộc tấn công tự động, 96% các cuộc tấn công lừa đảo hàng loạt và 76% các cuộc tấn công nhắm mục tiêu trực tiếp - tương tự như những chiến dịch tấn công được thực hiện bởi các tin tặc có tài trợ. Trong khi đó, việc sử dụng lời nhắc trên thiết bị mang lại những con số tương ứng lên tới 100%, 99% và 90%. Tất nhiên, sử dụng khóa bảo mật vật lý vẫn là phương pháp là an toàn nhất, giúp ngăn chặn tới gần 100% cả 3 loại hình tấn công trong quá trình điều tra của Google.

Ngoài ra, các hình thức 2FA khác như cung cấp địa chỉ email phụ, số điện thoại hoặc địa điểm đăng nhập cuối cùng cũng là những phương pháp được nhiều người lựa chọn sử dụng, nhưng có phần kém an toàn hơn nhiều. Cụ thể, phương pháp sử dụng email phụ chỉ giúp ngăn chặn được 73% các cuộc tấn công tự động, 68% các trường hợp tấn công lừa đảo hàng loạt và 79% các vụ tấn công nhắm mục tiêu trực tiếp. Mặt khác, các phương pháp như yêu cầu cung cấp số điện thoại và địa điểm đăng nhập cuối cùng tuy vẫn có thể ngăn chặn được 100% hình thức cuộc tấn công tự động, nhưng khả năng ứng phó với các cuộc tấn công lừa đảo hàng loạt và nhắm mục tiêu trực tiếp lại quá tệ, chỉ dừng lại ở mức 26% và 50% đối với phương pháp yêu cầu cung cấp số điện thoại, trong khi phương pháp yêu cầu cung cấp điểm đăng nhập cuối cùng còn tệ hơn, chỉ ngăn chặn được 10% tấn công lừa đảo hàng loạt và không thể ứng phó được với kiểu tấn công nhắm mục tiêu trực tiếp.

Như vậy có thể thấy việc sử dụng 2FA nhìn chung vô cùng cần thiết. Đối với hầu hết mọi người, chỉ cần thêm số điện thoại khôi phục vào tài khoản Google cũng đã có thể giúp giữ an toàn cho tài khoản của bạn tốt hơn rất nhiều, đồng thời giúp Google phát hiện các hoạt động đáng ngờ dễ dàng hơn.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng nên sử dụng xác thực 2 yếu tố để đảm bảo an toàn thông tin.

Link tham khảo: https://quantrimang.com/xac-thuc-2-yeu-to-co-the-ngan-chan-100-hack-bot-tu-dong-163997

3. Phát hiện lỗ hổng bảo mật nguy hiểm trên Mac

Một lỗ hổng bảo mật mang tên Gatekeeper vừa được phát hiện bởi nhà nghiên cứu Filippo Cavallarin, cho phép kẻ tấn công cài đặt phần mềm độc hại mà không cần yêu cầu giấy phép thông thường.

Theo Engadget, vì Gatekeeper coi các chia sẻ mạng là vị trí "an toàn" không yêu cầu kiểm tra quyền, kẻ xâm nhập chỉ cần lừa người dùng gắn một trong những chia sẻ đó để chạy các ứng dụng mà họ thích.

Ví dụ, một tập tin ZIP độc hại được tạo với liên kết tượng trưng phù hợp có thể tự động đưa người dùng đến một trang web thuộc sở hữu của kẻ tấn công, và thật dễ dàng để lừa ai đó khởi chạy một ứng dụng xấu, chẳng hạn virus giả mạo như một thư mục tài liệu.

Cavallarin cho biết ông đã thông báo cho Apple về lỗ hổng này vào ngày 22.2, và vấn đề được cho là đã giải quyết kể từ macOS 10.14.5. Tuy nhiên, ông nói rằng điều đó đã không xảy ra và Apple đã ngừng trả lời email của ông. Ông đã xuất bản lỗ hổng sau khi cho Apple 90 ngày để giải quyết vấn đề.

Hiện tại Apple vẫn chưa đưa ra nhận xét về vấn đề. Khả năng tiếp xúc vô tình sẽ không cao khi người dùng phải mở tập tin ZIP cũng như bất cứ thứ gì trong mạng chia sẻ, nhưng điều này có thể khiến những người không quen với chia sẻ từ xa hoặc rủi ro các tập tin không được yêu cầu. Nó cũng nhấn mạnh những rủi ro của việc tin tưởng vào một số môi trường mạng nhất định, ngay cả khi thường có một lý do chính đáng cho nó.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Mac cần cập nhật ngay các bản vá mới để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/phat-hien-lo-hong-bao-mat-nguy-hiem-tren-mac-1086189.html

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	IBM	CVE-2019-4279 CVE-2019-4078 CVE-2018-1991 CVE-2019-4058 ...	Nhóm 09 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (API Connect, DB2 Linux/ Windows, Rational Engineering Lifecycle Manage, IBM SDK, WebSphere Application Server...) cho phép đối tượng tấn công thực hiện thu thập thông tin, khai thác các lỗi tràn bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	Google	CVE-2019-5799 CVE-2019-5800 CVE-2019-5801 CVE-2019-5803 …..	Nhóm 17 lỗ hổng dựa trên một số sản phẩm của Google (Chrom) cho phép kẻ tấn công bỏ qua chính sách bảo mật và giả mạo tên miền.	Đã có thông tin xác nhận và bản vá
3	Cybozu	CVE-2019-5930 CVE-2019-5931 CVE-2019-5933 CVE-2019-5934 ……..	Nhóm 12 lỗ hổng sản phẩm Cybozu có phép kẻ tấn công truy cập trái phép vào hệ thống, thay đổi thông tin, quyền quản trị thực thi câu lệnh SQL hay chuyển hướng người dùng đến những trang web tùy thực hiện lừa đảo.	Đã có thông tin xác nhận và bản vá.
4	Intel	CVE-2019-0098 CVE-2019-0153 CVE-2019-0119 CVE-2019-0172 ……	Nhóm 30 lỗ hổng trên một số sản phẩm xử lý của Intel (TXE, Xeon, D Family, CSME …) lỗ hổng logic không xác thực người dùng, tràn bộ đệm, không kiểm soát quyền truy cập.	Đã có thông tin xác nhận và bản vá.
5	Abobe	CVE-2019-7130 CVE-2019-7837 CVE-2019-7107 CVE-2019-7105 …..	Nhóm 206 lỗ hổng trên một số sản phẩm của Adobe (bridge, flash Player, acrobat) lỗ hổng tràn heap, hỏng bộ nhớ, lỗ hổng trong việc truyền tải đường dẫn hay xử lý siêu liên kết không an toàn.	Đã có thông tin xác nhận và bản vá.

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	iri914a7.ru
6	xjpakmdcfuqe.com
7	104.244.14.252
8	1wh1ze3dpc.ru
9	1952w4ddc.ru
10	kukutrustnet777.info

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:

- Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
- Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.