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

1. Phát hiện chiến dịch tấn công APT vào các ngân hàng, hạ tầng quan trọng

Thực hiện công tác theo dõi và giám sát trên không gian mạng Việt Nam trong thời gian giáp Tết nguyên đán Kỷ Hợi, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đã ghi nhận chiến dịch tấn công có chủ đích (APT) của tin tặc nhằm vào các hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thống tin hạ tầng quan trọng quốc gia tại Việt Nam.

Với hình thức tấn công có chủ đích này, tin tặc đã tìm hiểu kỹ về đối tượng tấn công và thực hiện các thủ thuật lừa đảo, kết hợp với các biện pháp kỹ thuật cao để qua mặt hệ thống bảo vệ an toàn thông tin (ATTT) của các hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thống tin hạ tầng quan trọng quốc gia nhằm chiếm quyền điều khiển máy tính của người dùng thông qua đó tấn công các hệ thống máy tính nội bộ chứa thông tin quan trọng khác. Mục đích chính của tin tặc là đánh cắp các thông tin quan trọng của hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thống tin hạ tầng quan trọng quốc gia. Với việc sử dụng các kỹ thuật cao để tấn công thì các hệ thống bảo vệ ATTT của hệ thống thông tin của ngân hàng và tổ chức chủ quản hệ thống thống tin hạ tầng quan trọng quốc gia sẽ khó phát hiện kịp thời và đồng thời giúp tin tặc duy trì quyền kiểm soát hệ thống thông tin.

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, Trung tâm VNCERT đã có Công văn hỏa tốc số 37/VNCERT-ĐPƯC ngày 31/01/2019 đề nghị các đơn vị thành viên Mạng lưới ứng cứu sự cố quốc gia thực hiện gấp các biện pháp theo dõi, giám sát, ngăn chặn các kết nối đến máy chủ điều khiển mã độc để kịp thời phát hiện và ngăn chặn cuộc tấn công có chủ đích. Sau khi thực hiện, yêu cầu các đơn vị *báo cáo tình hình về Cơ quan Điều phối ứng cứu sự cố quốc gia (Trung tâm VNCERT) theo địa chỉ email: ir@vncert.gov.vn /điện thoại: 0869100319 trước 12h ngày 12/02/2019*.

Khuyến nghị:

Phòng ATTT đã có email gửi các đầu mối trung tâm điều hành KTM và các đơn vị trực thuộc. Các công việc cụ thể gồm 2 công việc: 1./ Chặn lọc các địa chỉ chứa mã độc theo danh sách; 2./ Rà quét trên các máy tính, máy chủ các file, thư mục có dấu hiệu tương ứng với mã MD5/SHA1 của mã độc (Chi tiết đã gửi các đơn vị qua email). Đối với các phòng chức năng, đề nghị liên hệ với P.ATTT để rà quét các máy tại cơ quan ngay trong ngày đầu năm mới khi bật máy hoạt động để đảm bảo an toàn, an ninh mạng.

Trên đây là những mã độc rất nguy hiểm, có thể đánh cắp thông tin và phá huỷ hệ thống thông tin, đề nghị Lãnh đạo các đơn vị thuộc Cục phối hợp chỉ đạo thực hiện.

2. Apple đã chủ động vô hiệu hóa tính năng FaceTime nhóm, nhằm khắc phục tạm thời lỗ hổng bảo mật nghiêm trọng

Tính năng FaceTime hiện đang bị lỗi khiến người dùng có thể nghe lén và nhìn trộm qua camera của đối phương.

Theo như thông tin mới đây, tính năng FaceTime trên iPhone gặp phải một lỗi bảo mật nghiêm trọng, cho phép người dùng nghe lén và nhìn trộm qua camera của đối phương cho dù họ chưa chấp nhận cuộc gọi. Lỗi bảo mật này được kích hoạt nhờ tính năng gọi nhóm trong FaceTime, mà Apple cập nhật cùng với phiên bản iOS 12.1.1.

Apple đã xác nhận lỗi này và cho biết sẽ sớm ra mắt bản vá vào cuối tuần. Tuy nhiên, để khắc phục tạm thời và tránh những trường hợp đáng tiếc xảy ra, Apple đã chính thức vô hiệu hóa tính năng FaceTime nhóm.

Trêm trang System Status của Apple, tính năng FaceTime hiện đang có trạng thái gặp sự cố và thông báo "Group FaceTime is temporarily unavailable".

Như vậy, người dùng sẽ không thể thêm các số điện thoại mới vào một trò chuyện FaceTime để thực hiện gọi nhóm được nữa. Đồng nghĩa với việc lỗi bảo mật nghiêm trọng trên sẽ không thể được khai thác.

Tất nhiên tính năng FaceTime một-một vẫn sẽ hoạt động bình thường.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng IOS cần cập nhật phiên bản mới nhất ngay khi có thể để bảo đảm an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/apple-vo-hieu-hoa-tinh-nang-facetime-nhom-nham-khac-phuc-tam-thoi-lo-hong-bao-mat-nghiem-trong.11962/

3. Lỗ hổng đe dọa hơn 9.000 Router của Cisco trên toàn cầu

Nếu hệ thống của các công ty bạn dùng Router Cisco RV320 hoặc RV325 Dual Gigabit VPN thì ngay lập tức cần cài đặt bản cập nhât firmware mới nhất từ nhà sản xuất.

Hacker đang tìm cách khai thác lỗ hổng nghiêm trọng mới được vá trong sản phẩm Cisco RV320 hoặc RV325 Dual Gigabit VPN sau khi một chuyên gia bảo mật công bố mã khai thác POC tuần trước.

Các lỗ hổng có tên CVE-2019-1652 và CVE-2019-1653), cho phép kẻ tấn công từ xa kiểm soát hoàn toàn bộ các Router bị ảnh hưởng của Cisco.

Lỗi đầu tiên tồn tại ở router RV320 and RV325 dual gigabit WAN VPN chạy các phiên bản phần mềm 1.4.2.15 đến 1.4.2.19 và lần thứ hai ảnh hưởng đến các phiên bản phần mềm 1.4.2.15 và 1.4.2.17, theo khuyến cáo của Cisco.

Cả hai lỗ hổng, được công ty bảo mật RedTeam Pentesting phát hiện và báo cho phía Cisco, các lỗi đều nằm trong giao diện quản lý trên web được sử dụng cho các bộ định tuyến và có thể khai thác từ xa.

CVE-2019-1652 Lỗ hổng cho phép kẻ tấn công từ xa thực hiện xác thực với các đặc quyền quản trị trên một thiết bị bị ảnh hưởng để thực thi các lệnh tùy ý trên hệ thống.

CVE-2019-1653 Lỗ hổng này không yêu cầu bất kỳ xác thực nào để truy cập cổng quản lý trên web của router, cho phép kẻ tấn công lấy thông tin nhạy cảm bao gồm tệp cấu hình của router có chứa thông tin mật.

Mã khai thác PoC trên các bộ định tuyến Cisco RV320 / RV325 được công khai trên Internet. CVE-2019-1653 bi lợi dụng để lấy tệp cấu hình từ bộ định tuyến để lấy thông tin băm và sau đó khai thác CVE-2019-1652 để thực thi các lệnh tùy ý và giành quyền kiểm soát hoàn toàn của thiết bị bị ảnh hưởng.

Các nhà nghiên cứu từ công ty Bad Packets cho biết họ đã tìm thấy ít nhất 9.657 bộ định tuyến của Cisco (6.247 RV320 và 3.410 RV325) trên toàn thế giới dễ bị ảnh hưởng trước lỗ hổng tiết lộ thông tin, hầu hết ở Hoa Kỳ.

Hãng đã chia sẻ một bản đồ tương tác, hiển thị tất cả các bộ định tuyến Cisco RV320 / RV325 có lỗ hổng ở 122 quốc gia và trên hệ thống mạng của 1.619 nhà cung cấp dịch vụ internet.

Bad Packets cho biết hệ thống honeypot của họ đã phát hiện hành vi quét các bộ định tuyến có thể gây ra các cuộc tấn công từ thứ 7 tuần trước, điều đó cho thấy tin tặc đang tích cực cố gắng khai thác lỗ hổng để kiểm soát hoàn toàn các bộ định tuyến dễ bị tấn công.

Cách tốt nhất để bảo vệ bạn khỏi trở thành mục tiêu của một cuộc tấn công là cài đặt bản phát hành phần mềm Cisco RV320 và RV325 mới nhất 1.4.2.20 càng sớm càng tốt.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị viên cần cập nhật phiên bản mới nhất của các thiết bị Cisco RV320 và RV325 để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/lo-hong-de-doa-hon-9-000-router-cua-cisco-tren-toan-cau.11957/

4. Cảnh giác trò lừa đảo chiếm đoạt tiền qua điện thoại

Theo đó, tội phạm mạng sẽ giả danh công an, tòa án, viện kiểm soát,... thông báo tới người dân rằng họ có liên quan đến đường dây mua bán ma túy lớn, yêu cầu chuyển tiền để phục vụ công tác điều tra. Tin lời, không ít người nhẹ dạ, thiếu hiểu biết đã mắc bẫy lừa đảo tinh vi này.

Theo Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, thủ đoạn của các đối tượng mạo danh lực lượng chức năng rất tinh vi khi dùng Internet thông qua phương thức VoIP để gọi điện nhằm tránh sự truy xét của cơ quan điều tra. Nếu bị hại ở miền Bắc thì chúng mạo danh là cán bộ các cơ quan pháp luật ở trong Nam và ngược lại. Mục đích để gây khó khăn cho việc xác minh. Thêm vào đó, tội phạm mạng còn sử dụng các phần mềm giả số điện thoại của cơ quan chức năng để lừa người dùng.

Để hạn chế các rủi ro có thể xảy ra, người dùng cần thận trọng khi chia sẻ thông tin cá nhân, tài khoản ngân hàng cho người khác, kể cả khi họ xưng là nhân viên ngân

hàng, công an,... Phía ngân hàng cũng đã yêu cầu các tổ chức tín dụng thông báo về thủ đoạn lừa đảo này cho người dùng và nhân viên ngân hàng để tăng cường cảnh giác.

Trước đó, một số ngân hàng lớn tại Việt Nam như Techcombank, Vietcombank,... đều đồng loạt đưa ra thông báo về việc xuất hiện nhiều trang web giả mạo ngân hàng nhằm chiếm đoạt thông tin tài khoản của người dùng.

Kẻ gian sẽ gửi tin nhắn giả mạo ngân hàng đến điện thoại của người dùng với nội dung: "Khách hàng đã nhận được tiền từ dịch vụ chuyển tiền Western Union" hoặc các dịch vụ tương tự, sau đó yêu cầu người dùng đăng nhập vào trang web giả mạo để xác nhận. Nếu làm theo, kẻ gian sẽ ngay lập tức có được thông tin tài khoản ngân hàng, mã OTP và lấy tiền của bạn.

Phía ngân hàng khuyến cáo người dùng chỉ nên đăng nhập tài khoản trên website chính thức của ngân hàng, không nạp hay chuyển tiền theo yêu cầu của người lạ hoặc khi có dấu hiệu nghi vấn. Đồng thời không cung cấp thông tin thẻ (số thẻ, ngày hiệu lực, mã số PIN, địa chỉ, họ tên chủ thẻ,...) khi nhận được email, điện thoại yêu cầu xác nhận thông tin hoặc các cuộc gọi nghi ngờ khác.

Ngoài ra, người dùng cần thay đổi mật khẩu theo định kỳ, sử dụng mật khẩu mạnh bao gồm chữ hoa, chữ thường, số và các ký tự đặc biệt để tăng độ phức tạp. Người dùng cũng nên đăng kí dịch vụ SMS banking để theo dõi biến động tài khoản (tiền vào/tiền ra) nhằm kịp thời phát hiện các dấu hiệu bất thường.

Người dùng cần phải cảnh giác hơn với những tin nhắn lừa đảo thông báo trúng thưởng qua SMS, Facebook, điện thoại,... Hành vi của kẻ gian ngày càng tinh vi và liều lĩnh hơn, nên cần nhớ một điều là tuyệt đối không cung cấp thông tin cá nhân, tài khoản ngân hàng hay địa chỉ email cho người khác.

Đồng thời, khi thực hiện các giao dịch chuyển tiền trực tuyến, hãy để ý đến liên kết trang xem có đúng hay chưa, thường thì các trang web của ngân hàng sẽ sử dụng giao thức bảo mật HTTPS nên ở phần đầu địa chỉ sẽ có biểu tượng ổ khóa màu xanh lá, nghĩa là an toàn.

Nhìn chung, trên đây chỉ là một trong số nhiều chiêu trò lừa đảo chiếm đoạt tài khoản ngân hàng. Tất nhiên, đằng sau đó vẫn còn rất nhiều hình thức và các trang web lừa đảo tương tự, người dùng phải thật sự tỉnh táo, tránh ham rẻ để rồi bị sập bẫy kẻ gian, đến khi mất tiền thì hối hận đã muộn.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần luôn đề cao cảnh giác khi đăng nhập vào các trang web của ngân hàng, không cung cấp thông tin thẻ, khi có những cuộc gọi đến nghi ngờ cần liên hệ với nhà chức trách để tránh bị lừa đảo.

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	Adobe Acrobat	CVE-2018-12830 CVE-2018-15987 CVE-2018-15991 …	Nhóm 88 lỗ hổng trên phần mềm Adobe Acrobat & Readercho phép đối tượng tấn công khai thác lỗi tràn bộ đệm để chèn và thực thi mã lệnh. Nhiều phiên bản Acrobat bị ảnh hưởng.	Đã có thông tin xác nhận và bản vá
2	Cisco	CVE-2019-1657 CVE-2019-1669 CVE-2019-1652	Nhóm 26 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (Cisco Small Business RV320 & RV325, AMP Threat Grid, Firepower Threat Defense, Identity Services Engine, IoT Field Network Director, Webex Network Recording Player, Webex Meetings Server…) cho phép đối tượng tấn công thực hiện một số hình thức tấn công: thu thập thông tin, vượt qua cơ chế bảo mật để truy cập trái phép vào hệ thống, chèn và thực thi đoạn mã độc hại. CVE-2019-1652 đã có mã khai thác và ảnh hưởng tới nhiều quốc gia trên thế giới	Đã có thông tin xác nhận và bản vá Đã có mã khai thác
3	Foxit	CVE-2018-17698 CVE-2018-17702 CVE-2018-17705 ...	Nhóm 65 lỗ hổng phần mềm Foxit Reader và Foxit PhantomPDF cho phép đối tượng tấn công chèn và thực thi mã lệnh trong phạm vi của triến trình	Đã có thông tin xác nhận và bản vá.
4	Drupal	CVE-2019-6339	Nhóm 04 lỗ hổng trên Drupal Core phiên bản 7.x và 8.x.x cho phép đối tượng tấn công đọc và xóa tập tin trên hệ	Đã có thông tin xác nhận và bản vá

			thống, sửa đổi dữ liệu trái phép, chèn và thực thi đoạn mã, tập tin độc hại tùy ý.	
5	Omron CX Supervisor	CVE-2018-19017 CVE-2018-19013 CVE-2018-19011 CVE-2018-19019	Nhóm 04 lỗ hổng phần mềm CX-Supervisor cho pehps đối tượng tấn công chèn lệnh để xóa tập tin trên hệ thống, chèn và thực thi đoạn mã độc hại. Omron CX-Supervisor là phần mềm dùng trong các hệ thống điều khiển công nghiệp dùng để thiết kế và giám sát quy trình hoạt động của thiết bị trong hệ thống	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	plpanaifheaighai.com
2	mokoaehaeihgiaheih.ru
3	and30.blabladomdom.com
4	produkktc.com
5	n.hmiblgoja.ru
6	ajkeahkcueafuiaeuf.ru
7	mel.cloudcontentsmak.com
8	iuefgauiaiduihgs.com
9	https://kisssweetmilf.com/lbjsmbbeuzsg
10	dghfhfgjfhjghj6699.net

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.