BẢN TIN NỘI BỘ

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

1. Phần mềm độc hại sử dụng ứng dụng web biến PC thành nguồn tấn công

Các nhà nghiên cứu từ Talos (Microsoft) và Cisco đã xác định một chủng phần mềm độc hại mới sử dụng các ứng dụng web để biến các hệ thống thành proxy cho lưu lượng truy cập internet độc hại.

Theo Engadget, cuộc tấn công khiến nạn nhân chạy tập tin HTA (ứng dụng HTML) thông qua quảng cáo lừa đảo hoặc tải xuống và khởi chạy một chuỗi sự kiện phức tạp. JavaScript trong trình HTA tải một tập tin JavaScript riêng biệt, xong lần lượt chạy một lệnh PowerShell để tải và chạy một loạt công cụ, bao gồm cả những công cụ vô hiệu hóa Windows Defender, yêu cầu kiểm soát nhiều hơn, các gói dữ liệu chụp và tạo proxy dự định.

Điều quan trọng, sự lây nhiễm phụ thuộc vào các chương trình hợp pháp để hoàn thành nhiệm vụ của mình, cho dù chúng được tích hợp vào Windows hay được tải xuống từ bên thứ ba. Cách tiếp cận khiến các nhóm bảo mật khó khăn hơn trong việc nghiên cứu mã và đưa ra các biện pháp đối phó.

Chưa rõ nhóm đứng sau phần mềm độc hại có tên Nodersok (hoặc Divergent) nói trên nhưng dường như đó là do tin tặc thông thường mà không phải do các tổ chức chính phủ hậu thuẫn. Cisco tin rằng phần mềm độc hại được thiết kế chủ yếu để gian lận nhấp chuột hoặc thực hành tự động tạo các nhấp chuột quảng cáo để tăng doanh thu từ các trang web. Hầu hết các mục tiêu là người dùng ở châu Âu và Mỹ mà không phải người dùng doanh nghiệp hoặc chính phủ.

Cả Microsoft và Cisco đều muốn phát huy khả năng của các hệ thống phòng thủ cấp doanh nghiệp của họ để ngăn chặn phần mềm độc hại. Tuy nhiên, hầu hết mọi người không có quyền truy cập vào những tài nguyên đó và phần mềm chống vi-rút dựa trên chữ ký thông thường chậm chạp hơn nhiều trong việc đối phó với phần mềm độc hại như vậy. Theo Microsoft, Nodersok đã nhắm mục tiêu đến hàng ngàn máy tính trong những tuần gần đây.

Link tham khảo: https://thanhnien.vn/cong-nghe/phan-mem-doc-hai-su-dung-ung-dung-web-bien-pc-thanh-nguon-tan-cong-1131606.html

2. Tội phạm ngân hàng: Mạo danh Western Union lừa đảo nhà bán hàng online

Thời gian gần đây, các ngân hàng liên tục đưa ra cảnh báo với khách hàng về thủ đoạn của bọn tội phạm công nghệ cao liên tiếp dùng các thủ đoạn lừa đảo tinh vi lợi dụng thông tin lừa cung cấp mã OTP, hoặc yêu cầu đăng nhập vào các trang web giả mạo để chiếm đoạt tài khoản của khách hàng và gây tổn hại đến uy tín của các ngân hàng.

Tuy nhiên tình trạng lừa đảo vẫn tái diễn, mới đây nhất, một nhà bán hàng online ở Hà Nội đã bị kẻ gian dẫn dắt nhằm mục đích lừa đảo, nhưng rất may chị đã không sa bẫy của bọn tội phạm.

Cụ thể, chị Q.P, một người kinh doanh online qua Facebook ở Hà Nội cho biết, vào tối ngày 27/9/2019, khi đang chuẩn bị đi ngủ thì chị nhận được tin nhắn của

người lạ qua Facebook (nick Nguyễn Thị Hồng) hỏi mua 4kg sen khô Huế, sau khi thống nhất giá cả giữa hai bên, nick Nguyễn Thị Hồng nhắn một địa chỉ ở Trần Phú, Vĩnh Yên, Vĩnh Phúc và số điện thoại của một người nhận tên là Nguyễn Thị Hương.

Chị Q.P nói sẽ chuyển hàng theo hình thức COD (giao hàng thu tiền) thì người mua nói là đợi cô ấy nhờ chuyển tiền vào tài khoản rồi hãy chuyển hàng, vì cô ấy đang ở Nhật. Sau đó cô ta xin số điện thoại và tài khoản ngân hàng của chị Q.P. Hai bên thống nhất sau khi chị Q.P nhận được tiền sẽ chuyển hàng ngay cho người mua.

Sáng ngày 28/9/2019, chị Q.P nhận được một SMS vào điện thoại có nội dung "KH nhận tiền từ DV chuyển tiền Western Union. Truy cập kiểm tra thông tin nhận tiền tại website: xyz…"

Sau đó, nick Nguyễn Thị Hồng nhắn tin qua Facebook bảo chị Q.P chờ tin nhắn báo về rồi chụp hình chờ cô ta hướng dẫn. Một lát sau điện thoại của chị Q.P có tiếp một SMS từ VERIFY báo số tài khoản ngân hàng của chị đã nhận được 1.520.000 VNĐ. Nhưng chị Q.P chưa thấy tài khoản của mình báo có tiền trong tài khoản.

Sau đó, nick Nguyễn Thị Hồng tiếp tục hướng dẫn chị bấm vào đường link trong tin nhắn đầu tiên để làm theo hướng dẫn, theo lời người này mục đích để kiểm tra đúng thông tin tài khoản ngân hàng của chị Q.P để bên nước ngoài còn còn duyệt giao dịch. Cô ta hối thúc chị kiểm tra nhanh đi, chỉ 5 phút sau là tiền sẽ vào tài khoản của chị.

Khi bấm vào đường link là một trang có rất nhiều logo của các ngân hàng Việt Nam, nick Nguyễn Thị Hồng tiếp tục hướng dẫn chị Q.P chọn ngân hàng của chị, sau đó hướng dẫn nhập tên, tuổi, số CMND, điện thoại và số tài khoản ngân hàng tiếp. Do theo dõi thông tin trên báo chí về các chiêu lừa đảo của tội phạm ngân hàng, chị Q.P đã không làm theo hướng dẫn.

Không may mắn như chị Q.P, chị P.T chủ một shop đồ phượt online ở Hà Nội mới đây đã bị bọn tội phạm lấy cắp 7 triệu đồng trong tài khoản với chiêu thức lừa đảo mua hàng, chuyển tiền qua Western Union tương tự như trên.

Đa phần nan nhân đều làm theo hướng dẫn của kẻ gian, sau khi có mã OTP của ngân hàng, bọn chúng sẽ hướng dẫn cung cấp OTP để đánh cắp tiền trong tài khoản của nạn nhân sang tài khoản của chúng.

Hồi tháng 6/2019, Hãng cung cấp giải pháp bảo mật toàn cầu Trend Micro cho biết, Việt Nam nằm trong Top 3 khu vực Đông Nam Á (ASEAN) bị tấn công bởi các loại mã độc ngân hàng. Trong quý I/2019, Việt Nam đứng trong số những nước bị tấn công bởi nhiều mối đe dọa bảo mật hàng đầu của Đông Nam Á bao gồm mã độc tống tiền (Ransomware), mã độc ngân hàng (Banking Malware), mã độc Macro (Macro Malware) và mối đe dọa email. Việt Nam đứng đầu về mã độc tống tiền tại khu vực Đông Nam Á, xếp trên Indonesia và Phillipines. Trong đó, khối ngân hàng Việt Nam tiếp tục là mục tiêu tấn công của tội phạm CNTT. Với tổng số loại mã độc ngân hàng được phát hiện là 1.989 loại, Việt Nam đứng thứ 3 sau Thái Lan, Malaysia về nguy cơ bị tấn công bởi các loại mã độc ngân hàng.

Thời gian gần đây, các ngân hàng của Việt Nam đã liên tục đưa ra khuyến cáo tới khách hàng của mình về một số thủ đoạn lừa đảo nổi lên gần đây như sau: Lừa khách hàng tự chuyển tiền (như trường hợp chị Q.P mới gặp ở trên), thông báo trúng thưởng, yêu cầu hoàn tất thủ tục nhận thưởng bằng cách nạp tiền vào số điện thoại chỉ định và chuyển trước một khoản phí nhận thưởng vào tài khoản của bọn tội phạm.

Bọn chúng thường dùng chiêu thức dùng email giả mạo gửi từ các tổ chức thẻ quốc tế: Visa, Mastercard, Amex, JCB… với nội dung thông báo giao dịch bị từ chối, trong khi khách hàng không hề thực hiện giao dịch qua thẻ, hoặc email thông báo thẻ của quý khách bị khóa và yêu cầu quý khách cung cấp lại thông tin cá nhân, thông tin thẻ để kích hoạt, mở lại thẻ hoặc yêu cầu cung cấp bổ sung thông tin cá nhân, thông tin tài khoản thẻ vào link sẵn có.

Bọn tội phạm còn giả danh người thân, bạn bè nhờ nhận tiền từ nước ngoài chuyển về. Qua đó, yêu cầu khách hàng đăng nhập vào đường dẫn trang web được cung cấp sẵn bằng tên đăng nhập (username) và mật khẩu tài khoản Internet banking của khách hàng, và sau đó nhập tiếp mã OTP được ngân hàng gửi vào số điện thoại hoặc email của khách hàng.

Một chiêu thức khác, đó là bọn tội phạm giả danh là nhân viên ngân hàng yêu cầu khách hàng cung cấp số thẻ, mật khẩu và mã xác thực OTP đã được gửi vào điện thoại của khách hàng do có khoản tiền treo cần chuyển về tài khoản. Hoặc giả danh nhân viên ngân hàng thông báo tài khoản bị tội phạm xâm nhập và yêu cầu cung cấp số tài khoản, mật khẩu, OTP giao dịch.

Trên thực tế các Ngân hàng, tổ chức tín dụng "không bao giờ" yêu cầu khách hàng cung cấp các thông tin cá nhân hoặc thông tin bảo mật như số tài khoản ngân hàng, số PIN thẻ ATM, mã truy cập, mã OTP và mật khẩu Internet Banking qua email hay điện thoại. Vì vậy, nếu nhận được những yêu cầu dạng này đồng nghĩa với việc kẻ gian đang tìm cách chiếm đoạt tài sản của khách hàng gửi tại ngân hàng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cảnh giác khi nhận được những tin nhắn có nội dung yêu cầu cung cấp thông tin thẻ ngân hàng, gặp những trường hợp nghi ngờ cần liên hệ với ngân hàng hoặc người có chuyên môn để tránh nguy cơ bị lừa đảo.

Link tham khảo: https://ictnews.vn/cntt/bao-mat/toi-pham-ngan-hang-mao-danh-western-union-lua-dao-nha-ban-hang-online-191026.ict

3. CVE-2019-16928: Lỗ hổng trong mail server Exim cho phép thực thi mã từ xa

Một lỗ hổng an ninh nghiêm trọng vừa được phát hiện và vá trong máy chủ mail Exim, có thể cho phép kẻ tấn công từ xa thực thi mã tùy ý trên máy chủ mục tiêu.

Theo các nhà phát triển Exim, lỗ hổng này, CVE-2019-16928, ảnh hưởng đến các phiên bản từ 4.92.2 trở về trước.

Đây là lỗi tràn vùng dữ liệu heap trong hàm string_vformat tồn tại trong file mã nguồn string.c của Exim. Bằng cách khai thác lỗ hổng này, kẻ tấn công có thể gây ra

một cuộc tấn công từ chối dịch vụ vào Exim server hoặc thực thi mã từ xa tới Exim server.

Theo thông báo chính thức từ Exim, hiện tại mã khai thác lỗ hổng này đã được tiết lộ công khai nhưng mã này chỉ gây ra một cuộc tấn công từ chối dịch vụ tới Exim server mà không có khả năng thực thi mã từ xa.

Exim đã phát hành phiên bản 4.92.3 để vá lỗi này.

Exim là một trong những dịch vụ mail server lớn nhất hiện nay. Theo thống kê trên trang Shodan, hiện khoảng 5 triệu máy, chủ yếu tại Mỹ. Chính điều này khiến Exim trở thành mục tiêu hấp dẫn của kẻ xấu.

Vào giữa tháng 6 năm nay, các chuyên gia và các công ty cảnh báo về lỗ hổng CVE-2019-10149 của Exim (đã có bản vá) bị khai thác để phát tán mã độc đào tiền ảo. Và gần đây nhất là lỗi hổng CVE-2019-15846 của Exim cho phép thực thi mã từ xa với đặc quyền root.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị cần cập nhật bản vá mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/cve-2019-16928-lo-hong-trong-mail-server-exim-cho-phep-thuc-thi-ma-tu-xa.12765/

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	Advantech	CVE-2019-13550 CVE-2019-13558 CVE-2019-13552 CVE-2019-13556	Nhóm 04 lỗ hổng trên các sản phẩm, phần mềm của Advantech (WebAccess versions 8.4.1) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau bao gồm: thu thập thông tin, chèn và thực thi mã từ xa. 2 lỗ hổng có điểm CVSS cao là 9.0	Đã có thông tin xác nhận và bản vá.
2	Linux	CVE-2019-14821 CVE-2019-16413 CVE-2019-15031	Nhóm 06 lỗ hổng trên sản phẩm của Linux (Linux kernel, SUSE Linux Enterprise Server 12) cho phép đối tượng tấn công từ chối dịch vụ, chèn và thực thi mã từ xa. 1 lỗ hổng có điểm đặc biệt ngiêm trọng là 10.0	Đã có thông tin xác nhận và bản vá
3	Draytek	CVE-2019-16533 CVE-2019-16534	Nhóm 02 Lỗ hổng trên phiên bản firmware của thiết bị Draytek (vigor 2925, firmware 3.8.4.3) cho phép đối tượng tấn công truy cập trái phép và khai thác XSS.	Chưa có thông tin xác nhận và bản vá
4	Dlink	CVE-2019-16057	Nhóm 01 lỗ hổng trên một số phiên bản firmware của thiết bị Dlink (DNS-320) cho phép đối tượng tấn công chèn và thực thi lệnh độc hại qua nhiều thành phần khác nhau; lỗ hổng có điểm CVSS là 10.0 đặc biệt nghiêm trọng	Đã có thông tin xác nhận và bản vá
5	Cisco	CVE-2019-12620 CVE-2019-1975	Nhóm 02 lỗ hổng trên một số sản phẩm, phần mềm của Cisco (HyperFlex Software)cho phép đối tượng tấn công thực thi mã lệnh từ xa, hướng người dùng đến	Đã có thông tin xác nhận và bản vá

			trang web độc hại	
6	Apache	CVE-2019-0195 CVE-2019-0207 CVE-2019-10071	Nhóm 03 lỗ hổng trên một số sản phẩm, phần mềm của Apache cho phép đối tượng tấn công khai thác đường link của các tệp trong hệ thống để tiêm mã độc trên nền tảng Windows, thực thi mã lệnh từ xa.	Đã có thông tin xác nhận và bản vá
7	Wordpress	CVE-2016-11008 CVE-2016-11010 CVE-2014-10397 …	Nhóm 24 lỗ hổng trên nhiều thành phần của WordPress cho phép đối tượng tấn công khai thác lỗi XSS, truy cập trái phép vào thông tin người dùng trên hệ thống hay chuyển hướng người dùng đến trang web độc hại, chèn và thực thi mã từ xa, tấn công leo thang.	Chưa có thông tin xác nhận và bản vá
8	Gitlab	CVE-2019-15721 CVE-2019-15722 CVE-2019-15724 …	Nhóm 21 lỗ hổng trên một số phiên bản của Gitlab (GitLab Community) cho phép đối tượng tấn công khai thác và chỉnh sửa cài đặt, thu thập thông tin, địa chỉ IP của người sử dụng, tấn công từ chối dịch vụ, thực thi mã lệnh từ xa.	Đã có thông tin xác nhận và bản vá
9	Codesys	CVE-2019-13538 CVE-2019-9008	Nhóm 02 lỗ hổng trên một số sản phẩm và thành phần của Codesys cho phép đối tượng tấn công khai thác nội dung thư viện trong hệ thống và tấn công từ chối dịch vụ, thực thi mã lệnh từ xa.	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	soplifan.ru

5	2iq7vrzg.ru
6	xjpakmdcfuqe.com
7	xdqzpbcgrvkj.ru
8	www.cityofangelsmagazine.com
9	morphed.ru
10	kt00quqt.ru

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.