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

1. Cảnh báo nhóm tấn công mạng Platinum quay trở lại

Theo Kaspersky, chiến dịch kéo dài gần 6 năm và có mối liên hệ với các cuộc tấn công gần đây được phát hiện trong khu vực. Dựa vào những công cụ và phương pháp sử dụng, Kaspersky tin Platinum - một nhóm hacker những tưởng đã ngừng hoạt động - là nhóm đứng sau các cuộc tấn công. Để che giấu hoạt động trong một thời gian dài, Platinum đã mã hóa thông tin của mình bằng cách sử dụng kỹ thuật ẩn mã (steganography) để che giấu thông tin muốn truyền tải.

Kỹ thuật ẩn mã là phương thức truyền tải thông điệp một cách bí mật, sao cho ngoại trừ người gửi và người nhận thì không ai biết đến sự tồn tại của thông điệp. Cách thức này khác với mật mã ở chỗ mật mã chỉ dùng để che giấu dữ liệu. Bằng cách sử dụng kỹ thuật ẩn mã, các nhóm hacker có thể khiến hệ thống bị nhiễm mã độc trong một thời gian dài mà không hề bị nghi ngờ.

Đây là phương thức được sử dụng bởi nhóm Platinum, một nhóm hacker chống lại chính phủ và các tổ chức liên quan ở khu vực Nam Á và Đông Nam Á - với hoạt động cuối cùng được biết đến của chúng diễn ra vào năm 2017.

Để phát hiện phần mềm độc hại, các nhà nghiên cứu đã phải kiểm tra các chương trình có khả năng tải tệp lên thiết bị, sau đó nhận thấy một hoạt động khác thường - như truy cập Dropbox và chỉ hoạt động vào một số thời điểm nhất định. Theo Kaspersky, mục đích của việc này là để che giấu hoạt động tấn công của phần mềm độc hại trong giờ hành chính - thời điểm hành vi tấn công không bị nghi ngờ.

Link tham khảo: https://thanhnien.vn/cong-nghe/canh-bao-nhom-tan-cong-mang-platinum-quay-tro-lai-1091993.html

2. Ham khuyến mãi, nhiều người chia sẻ tin nhắn lừa tặng 3.000 đôi giày Adidas

Sáng 14/6, nhiều người dùng di động phản ánh họ nhận được những tin nhắn từ đầu số lạ trên các ứng dụng OTT như WhatsApp, Viber. Nội dung tin nhắn phát đi thông điệp về một chiến dịch khuyến mãi của nhãn hàng Adidas.

Theo đó, Adidas đang tặng 3.000 đôi giày và áo phông miễn phí để kỷ niệm 95 năm ngày thành lập công ty này. Cùng với thông tin trên là một đường dẫn trỏ đến địa chỉ adidas-sneakers.club. Nhận thấy đường dẫn có dấu hiệu bất thường, nhiều người dùng di động cho biết họ nghi ngờ tin nhắn này đến từ những kẻ lừa đảo.

Khi Pv. VietNamNet liên hệ với một cửa hàng thuộc hệ thống phân phối của Adidas trên đường Hai Bà Trưng (Hà Nội), nhân viên cửa hàng khẳng định Adidas không hề có chiến dịch khuyến mãi nào giống như tin nhắn kể trên.

Người này cũng cho biết Adidas vừa kỷ niệm 70 năm thành lập, do vậy thông tin về đợt khuyến mãi nhân dịp 95 năm thành lập hãng là hoàn toàn không chính xác.

Theo nhân viên của Adidas, tất cả chiến dịch khuyến mãi của Adidas sẽ được đưa lên fanpage hoặc website. Adidas thường chỉ nhắn tin khuyến mãi thông qua tin nhắn di động thông thường tới những khách hàng đã từng mua và đăng ký dịch vụ này với phía hãng.

Tiến hành kiểm tra về địa chỉ website có trong tin nhắn, công cụ truy vấn tên miền của iNet cho biết, địa chỉ adidas-sneakers.club chỉ mới được đăng ký ngày 13/6/2019, tức là chỉ một ngày trước khi các tin nhắn lừa đảo được gửi đi. Website này cũng không được đăng ký các tiêu chuẩn bảo mật phổ biến.

Thực tế cho thấy, những kẻ lừa đảo thường đánh vào lòng tham của nhiều người bằng việc tạo ra fake news (thông tin giả mạo) về các chương trình khuyến mãi của những thương hiệu lớn để thu hút, lôi kéo người xem.

Theo nhận định của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an), các hoạt động sử dụng không gian mạng để lừa đảo đang diễn ra ngày một phức tạp.

Cách thức của bọn tội phạm tập trung chủ yếu vào các hành vi như lừa đảo qua tin nhắn rác, tin nhắn trúng thưởng, giả danh người nước ngoài nhắn tin làm quen và gửi quà tặng về Việt Nam, giả danh cán bộ công an, viện kiểm sát, tòa án yêu cầu người dân chuyển tiền vào tài khoản.

Không chỉ vậy, xuất hiện nhiều vụ việc mà các đối tượng xấu đã chiếm quyền điều khiển tài khoản mạng xã hội của người dùng, sau đó nhắn tin lừa đảo mọi người trong danh sách bạn bè của nạn nhân. Ngoài ra, xuất hiện nhiều hành vi lừa đảo từ hoạt động trao đổi, mua bán qua mạng, kinh doanh đa cấp.

Với những trường hợp như tin nhắn kể trên, nếu click vào đường link lừa đảo, người sử dụng di động có thể vô tình tải về các mã độc lên chính thiết bị của mình. Do vậy, khi nhận được tin nhắn không rõ nguồn gốc, người dùng di động cần hết sức cảnh giác, tránh click vào đường link lạ mà mắc mưu những kẻ lừa đảo.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần nâng cao cảnh giác với các tin nhắn không rõ nguồn gốc, tránh click vào đường link lạ để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/ca-tin-ham-khuyen-mai-nhieu-nguoi-dinh-tin-nhan-lua-dao-tang-3-000-doi-giay-adidas-541617.html

3. Hệ thống Linux của bạn có thể bị hack chỉ bằng cách mở một tệp trong Vim hoặc Neovim Editor

Nhà nghiên cứu bảo mật nổi tiếng Armin Razmjou gần đây đã phát hiện ra lỗ hổng nghiêm trọng liên quan đến thực thi lệnh hệ điều hành tùy ý (CVE-2019-12735) trong Vim và Neovim - 2 ứng dụng chỉnh sửa văn bản dòng lệnh phổ biến và mạnh mẽ nhất, thường được cài đặt sẵn trên hầu hết các hệ điều hành dựa trên Linux.

Trên các hệ thống Linux, trình soạn thảo Vim cho phép người dùng tạo, xem hoặc chỉnh sửa bất kỳ tập tin nào, bao gồm văn bản, tập lệnh lập trình và cả tài liệu.

Do Neovim chỉ là một phiên bản mở rộng của Vim (với trải nghiệm người dùng, plugin và GUI tốt hơn), đương nhiên lỗ hổng thực thi mã nghiêm trọng nêu trên cũng sẽ xuất hiện trong ứng dụng này.

Chuyên gia bảo mật Armin Razmjou đã phát hiện ra một lỗ hổng trong cách thức trình soạn thảo Vim xử lý "modelines" - tính năng được bật theo mặc định để tự

động tìm và áp dụng một tập hợp các tùy chọn tùy chỉnh được đề cập bởi người tạo tệp, gần với dòng bắt đầu và kết thúc trong tài liệu.

Mặc dù trình chỉnh sửa chỉ cho phép áp dụng một tập hợp con các tùy chọn trong mô hình (vì lý do bảo mật) và sử dụng sandbox protection nếu nó có chứa biểu thức không an toàn, thế nhưng Armin Razmjou tiết lộ rằng việc sử dụng lệnh ":source!" (với một sửa đổi [!]) có thể vượt qua được sandbox protection.

Do đó, người dùng chỉ cần mở một tệp được tạo thủ công đặc biệt bằng cách sử dụng Vim hoặc Neovim cũng đã có thể cho phép kẻ tấn công bí mật thực thi các lệnh trên hệ thống Linux của họ, cũng như kiểm soát hệ thống từ xa.

Hiện nhà nghiên cứu bảo mật này cũng đã phát hành công khai 2 Proof of Concept (PoC) về cách thức exploit lỗ hổng nêu trên. Một trong số đó thể hiện kịch bản tấn công ngoài đời thực khi kẻ tấn công từ xa có quyền truy cập vào reverse shell từ hệ thống của nạn nhân ngay khi anh ta mở tệp nó.

Các nhà phát triển chịu trách nhiệm bảo trì cho Vim (phiên bản vá 8.1.1365) và Neovim (phát hành trong v0.3.6) cũng đã tung ra bản cập nhật cho cả hai tiện ích này để giải quyết vấn đề. Đồng thời khuyến nghị người dùng nên cài đặt phiên bản mới càng sớm càng tốt.

Bên cạnh đó, nhà nghiên cứu Armin Razmjou cũng đã đưa ra một số khuyến nghị bổ sung cho người dùng như sau:

* Vô hiệu hóa tính năng modelines.

* Vô hiệu hóa "modelineexpr" để không cho phép các biểu thức xuất hiện trong modelines.

* Chuyển sang sử dụng "securemodelines plugin" như một sự thay thế an toàn cho các mô hình Vim.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị cần cập nhật phiên bản mới nhất của Vim và Neovim để đảm bảo an toàn thông tin.

Link tham khảo: https://quantrimang.com/he-thong-linux-co-the-bi-hack-bang-cach-mo-tep-trong-vim-hoac-neovim-editor-164426

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	HP	CVE-2019-11982 CVE-2019-11983 CVE-2018-7121 CVE-2018-7123 CVE-2018-7124 ...	Nhóm 106 lỗ hổng trên một số sản phẩm của HP (máy chủ Gen9, Máy chủ Gen10) cho phép khai thác lỗi tràn bộ đệm từ xa, chèn và thực thi mã lệnh từ xa.	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2019-4257 CVE-2019-4070 CVE-2019-4069 CVE-2019-4068 …..	Nhóm 17 lỗ hổng trên một số sản phẩm của IBM (Máy chủ thông tin InfoSphere, IOC, ISIQ) cho phép kẻ tấn công nhúng các đoạn mã JavaScript để lấy thông tin và thay đổi chức năng trong hệ thống, lỗ hổng làm lộ thông tin, dữ liệu nhạy cảm do không mã hóa khi truyền đi.	Đã có thông tin xác nhận và bản vá
3	Foxitsoftware	CVE-2019-5930 CVE-2019-5931 CVE-2019-5933 CVE-2019-5934 ……..	Nhóm 28 lỗ hổng trên một số sản phẩm của Foxitsoftware (Foxit Reader, Foxit PhantomPDF, ...) cho phép kẻ tấn công thực hiện thu thập thông tin nhạy cảm, thực thi mã lệnh trong phạm vi của tiến trình.	Đã có thông tin xác nhận và bản vá.
4	Linux	CVE-2019-12614 CVE-2019-12615 CVE-2019-3846 ……	Nhóm 03 lỗ hổng trên một số thành phần của nhân Linux cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, tấn công leo thang	Đã có thông tin xác nhận và bản vá.
5	Cisco	CVE-2019-1870 CVE-2019-1881 CVE-2019-1842 CVE-2019-1845 CVE-2019-1872 …..	Nhóm 09 lỗ hổng trên một số sản phẩm của Cisco (Cisco Enterprise, Industrial Network Director (IND)) cho phép kẻ tấn công thực thi mã lệnh tùy ý, thu thập thông tin nhạy cảm.	Đã có thông tin xác nhận và bản vá.

6	Vim	CVE-2019-12735	Lỗ hổng trong trình soạn thảo trên dòng lệnh VIM cho phép đối tượng tấn công thực thi lệnh của hệ điều hành. Lỗi này có thể được khai thác khi người dùng mở một tập tin bằng vim.	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	646u38k6.ru
6	xjpakmdcfuqe.com
7	rbmeke.info
8	www.cityofangelsmagazine.com
9	plpanaifheaighai.com
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.