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

1. Để tăng năng lực đảm bảo an toàn thông tin, phải phòng bệnh hơn chữa bệnh

Việt Nam và nhiều quốc gia khác trên thế giới đang đẩy mạnh quá trình chuyển đổi số trong bối cảnh cuộc cách mạng công nghiệp lần thứ Tư (CMCN 4.0). Do đó, việc phát triển năng lực quốc gia về an toàn, an ninh mạng được xem như một điều kiện tiên quyết để xây dựng chính phủ điện tử, kinh tế số, phục vụ hoạt động của nhà nước, người dân và doanh nghiệp.

Trong bối cảnh đó, Hội thảo - triển lãm quốc tế Ngày An toàn thông tin Việt Nam năm 2019 với chủ đề "Nâng tầm An toàn, An ninh mạng quốc gia trong kỷ nguyên số" (Enhancing national cybersecurity in the digital era) sẽ được tổ chức vào ngày 29/11/2019 tại Khách sạn Melia Hà Nội.

Hội thảo - triển lãm quốc tế Ngày An toàn thông tin Việt Nam là sự kiện thường niên được tổ chức bởi Hiệp hội An toàn thông tin Việt Nam (VNISA), Cục An toàn thông tin (Bộ TT&TT) và Bộ Tư lệnh Tác chiến không gian mạng (Bộ Quốc phòng).

Đây là diễn đàn quan trọng cấp quốc gia và cũng là sự kiện nổi bật nhất về an toàn, an ninh mạng tại Việt Nam trong năm 2019.

Nội dung Hội thảo sẽ tập trung phân tích tầm nhìn, định hướng của chính phủ về tăng cường bảo đảm an toàn, an ninh mạng tại Việt Nam; chính sách, thực trạng, nhu cầu ứng dụng và phát triển công nghệ an toàn thông tin (ATTT) và giải pháp nâng cao thứ hạng về an toàn, an ninh mạng của Việt Nam.

Chương trình Hội thảo gồm phiên Toàn thể vào buổi sáng và 2 phiên Chuyên đề vào buổi chiều với gần 30 bài phát biểu, tham luận của lãnh đạo các cơ quan quản lý nhà nước trong lĩnh vực an toàn, an ninh mạng, các nhà quản lý, chuyên gia cao cấp về ATTT của các công ty lớn trong và ngoài nước.

Phiên toàn thể buổi sáng sẽ có sự tham dự và phát biểu của lãnh đạo cao cấp Liên minh Viễn thông quốc tế (ITU) và lãnh đạo cơ quan an toàn, an ninh thông chính phủ Phần Lan, với chủ đề về An toàn, an ninh mạng trong phát triển quốc gia số.

Bên cạnh đó là phiên toạ đàm với chủ đề "Nâng cao năng lực ATTT Việt Nam: Chính sách, giải pháp và kinh nghiệm quốc tế", dưới sự chủ trì của Lãnh đạo cục ATTT.

Phiên thứ 3 với chủ đề An toàn, an ninh mạng cho hệ thống thông tin trọng yếu Quốc gia sẽ có sự xuất hiện của công ty An ninh mạng Viettel, Amazon Web Services và Huawei với những báo cáo quan trọng về tình hình an ninh mạng.

Bên lề Hội thảo sẽ là khu vực triển lãm và khu trình diễn công nghệ, nơi giới thiệu giải pháp, sản phẩm của các tập đoàn, doanh nghiệp hàng đầu về CNTT, ATTT trong và ngoài nước.

Đáng chú ý khi sự kiện Ngày An toàn thông tin năm nay sẽ có sự hiện diện của lãnh đạo Chính phủ tại lễ bấm nút khai trương Hệ thống Giám sát An toàn thông tin phục vụ Chính phủ điện tử do Bộ TT&TT triển khai.

Theo Thứ trưởng Bộ TT&TT Nguyễn Thành Hưng, có sự liên hệ nhất định giữa ngành y và lĩnh vực an toàn, an ninh mạng. Ở những nước nghèo, khi mà điều kiện còn thiếu thốn, người ta chỉ quan tâm đến việc điều trị bệnh. Đó là vấn đề đang xảy ra tại ngành y. Điều tương tự cũng diễn ra với lĩnh vực an ninh mạng khi mà nhiều nước chỉ quan tâm đến việc ứng cứu các sự cố.

"Nếu nhìn vào góc độ kinh tế, ban đầu lựa chọn trên khá phù hợp vì không phải bỏ ra quá nhiều tiền. Tuy nhiên hậu quả mà nó đem lại cũng rất lớn", Thứ trưởng Nguyễn Thành Hưng nói.

Theo Thứ trưởng Nguyễn Thành Hưng, những nước phát triển rất quan tâm đến vấn đề y tế dự phòng. Cái khó của việc phát triển y tế dự phòng là cơ quan quản lý phải quan tâm đến một diện rất rộng toàn xã hội, thế nhưng lợi ích đem lại của nó rất lâu dài. Để làm được điều này, nhận thức của xã hội, người dân và chính phủ là vô cùng quan trọng.

Thứ trưởng Nguyễn Thành Hưng cho rằng, cần phải thay đổi nhận thức về vấn đề "phòng bệnh hơn chữa bệnh" ngay trong chính lĩnh vực an toàn thông tin. Bộ TT&TT mong muốn tăng cường công tác "phòng bệnh" và phát triển đội ngũ "bác sĩ" nội cũng như "thuốc" nội trong lĩnh vực an toàn thông tin.

Việc tổ chức sự kiện ngày An toàn thông tin sẽ giúp nâng cao nhận thức của chính phủ, người dân và toàn thể xã hội trong việc phát triển năng lực "y tế dự phòng" của an toàn thông tin, từ đó giải quyết khâu "phòng bệnh hơn chữa bệnh".

Bộ TT&TT hy vọng có thể biến nhận thức thành hành động để rồi từ đó phát triển được các lực lượng đảm bảo an toàn an ninh mạng tại Việt Nam ngang tầm với thế giới.

Link tham khảo: https://vietnamnet.vn/vn/thong-tin-truyen-thong/de-tang-nang-luc-dam-bao-an-toan-thong-tin-phai-phong-benh-hon-chua-benh-588200.html

2. Lỗ hổng trong các sản phẩm diệt virus cho phép tấn công DLL Hijacking - Cập nhật

Ngoài những cái tên như Avast, AVG, Avira, McAfee, Forcepoint, Trend Micro, Bitdefender và Check Point, Symantec Endpoint Protection hiện là sản phẩm diệt virus mới nhất bị phát hiện dính lỗ hổng này.

Symantec đã cập nhật bản vá cho lỗi CVE-2019-12758 này. Các phiên bản bị ảnh hưởng của Symantec Endpoint Protection gồm các bản từ 14.2.RU1 trở về trước.

Các nhà nghiên cứu bảo mật SafeBreach phát hiện ra lỗ hổng trong phần mềm diệt virus của McAfee cho phép kẻ tấn công vượt qua các cơ chế tự bảo vệ của phần mềm.

Lỗ hổng bảo mật có thể bị lạm dụng để tải các thư viện DLL chưa được ký và được chạy với quyền NT AUTHORITY\SYSTEM. Tuy nhiên, việc khai thác đòi hỏi kẻ tấn công phải có đặc quyền của quản trị viên.

Theo SafeBreach, các phần mềm diệt virus hiện nay chạy như một dịch vụ của Windows được thực thi với quyền "NT AUTHORITY\SYSTEM", nghĩa là có quyền cao nhất trên hệ thống.

Các nhà nghiên cứu bảo mật phát hiện ra rằng, các tiến trình bị ảnh hưởng cố gắng tải tệp từ đường dẫn C:\Windows\System32\wbem\wbemcomn.dll. Tuy nhiên không thể tìm thấy tệp do tệp đó nằm trong thư mục System32.

Cơ chế này có thể bị kẻ tấn công khai thác để tải DLL độc hại bằng cách đặt tệp của chúng vào thư mục wbem với tên gọi wbemcomn.dll.

Một thư viện không được ký số được tải bởi tiến trình phần mềm McAfee sẽ dẫn đến việc cơ chế tự bảo vệ của phần mềm diệt virus bị qua mặt, từ đó ngăn chặn người dùng, thậm chí cả quản trị viên, ghi vào các thư mục của phần mềm.

Một vấn đề khác khiến các cơ chế tự bảo vệ của phần mềm có thể bị qua mặt là phần mềm diệt virus không xác thực chữ ký số đối với tệp DLL.

SafeBreach giải thích, lỗ hổng cho phép kẻ tấn công tải và thực thi payload độc hại mỗi khi các dịch vụ được tải. Có nghĩa là một khi kẻ tấn công thả một tệp DLL độc hại, các dịch vụ sẽ tải mã độc sau mỗi lần được khởi động lại.

Lỗ hổng CVE-2019-3648 ảnh hưởng tới McAfee Total Protection (MTP), McAfee Anti-Virus Plus (AVP), và McAfee Internet Security (MIS).

McAfee đã phát hành một bản vá và cho biết chưa có thông tin về việc lỗ hổng đã bị khai thác trong các cuộc tấn công.

Vài tuần trước, SafeBreach tiết lộ các sản phẩm diệt virus của Avast, AVG và Avira cũng bị ảnh hưởng bởi các lỗ hổng DLL hijacking chiếm quyền khai thác theo cách tương tự bởi những kẻ tấn công có đặc quyền quản trị.

Theo nhận định của chuyên gia Bkav, để khai thác được lổ hổng này cần có quyền quản trị, vì vậy chúng ta không nên chạy các phần mềm không rõ nguồn gốc với quyền administrator để tránh bị khai thác bởi lỗ hổng này.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cài các phần mềm AntiVirus có bản quyền và luôn cập nhật phiên bản mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/lo-hong-trong-cac-san-pham-diet-virus-cho-phep-tan-cong-dll-hijacking-cap-nhat.12939/

3. Ứng dụng rác giá 9 triệu đồng tràn ngập Play Store Việt Nam

Play Store (hay còn được biết với tên gọi Cửa hàng Play/CH Play tại Việt Nam) là kho ứng dụng của Google tạo dựng dành cho người dùng các thiết bị như smartphone, tablet, Smart TV... chạy hệ điều hành Android. Theo số liệu của Statista, tính đến tháng 9/2019, kho ứng dụng này bao gồm 2.8 triệu ứng dụng thuộc nhiều thể loại khác nhau như Liên lạc, Giải trí, Mua sắm, Công việc...

Tuy nhiên, theo ghi nhận của chúng tôi, kho ứng dụng Play Store tại Việt Nam đang ngập tràn ứng dụng rác. Đáng quan ngại hơn, nhiều ứng dụng rác có mức giá lên đến 9 triệu đồng nhưng vẫn có lượt tải về.

Nhìn vào bảng xếp những ứng dụng trả phí được tải về nhiều nhất trên Play Store Việt Nam, toàn bộ 100 vị trí đầu tiên (từ #1 đến #100) đều là ứng dụng rác và có giá lên đến 9 triệu đồng. Điểm chung của các ứng dụng này là chúng có giao diện cực kỳ đơn giản và gần như không có bất cứ tính năng nào.

Ứng dụng trả phí đứng đầu trên kho Play Store Việt Nam hiện nay là ClickToDestroyMe. Ứng dụng này có giá 9 triệu đồng, nhưng chỉ bao gồm một ô vuông duy nhất kèm theo một con số bên trong.

Ứng dụng đứng thứ hai mang tên CachLamBanhHoi cũng có giá 9 triệu đồng, hiển thị một vài dòng hướng dẫn và hình ảnh cách làm món Bánh Hỏi.

Ứng dụng đứng thứ ba là RandomEmotion giá 9 triệu đồng, nhiệm vụ duy nhất là... hiển thị một biểu tượng cảm xúc ngẫu nhiên.

Tương tự như vậy, tất cả các ứng dụng trong Top 100 ứng dụng trả phí của Play Store Việt Nam hiện nay đều có giá 9 triệu đồng, đều vô dụng và đều là "rác". Điều đáng nói ở đây là theo số liệu thống kê từ Play Store, mỗi ứng dụng rác ở trên vẫn có hơn 100 lượt tải về, có thể đem về khoản doanh thu hàng trăm triệu đồng cho lập trình viên.

Điểm đáng chú ý ở các ứng dụng rác giá cao này là chúng đều đến từ một số nhà phát triển như Modern Hobbit, Candy Mum Mum, Times How Land, Snoop Obito Lena và Halo Xanh Green. Khi truy cập vào profile của những nhà phát triển này, tất cả những ứng dụng mà họ đưa lên Play Store đều là ứng dụng rác và có giá 9 triệu đồng.

Theo thông tin được cung cấp bởi Play Store, lập trình viên đứng đằng sau những ứng dụng này đến từ nhiều tỉnh thành khác nhau tại Việt Nam như Nghệ An, Nha Trang, Hà Nội.

Hiện vẫn chưa rõ động cơ của nhóm lập trình viên đứng đằng sau những ứng dụng rác này là gì. Tuy nhiên, việc một lượng lớn các ứng dụng như vậy lọt vào BXH trả phí của Play Store đã cho thấy khâu quản lý và kiểm duyệt lỏng lẻo của Google, tạo ra nhiều rủi ro cho người dùng Android.

Trước đó, đã nhiều lần kho ứng dụng Play Store bị phát hiện chứa chấp các ứng dụng rác, quảng cáo, thậm chí là mã độc. Gần đây nhất, một sinh viên sinh sống tại Hà Nội đã đăng tải 42 ứng dụng chứa mã độc quảng cáo lên Play Store với nhiều thủ đoạn tinh vi nhằm qua mặt đội ngũ kiểm duyệt của Google và người dùng. Một vài ứng dụng trong số đó đã được tải về đến hàng triệu lượt. Hành vi này chỉ bị "lộ tẩy" khi các chuyên gia bảo mật của hãng ESET vào cuộc.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Andoird cần cảnh giác khi download các ứng dụng trong kho Play Store để tránh bị lừa đảo mất tiền và thông tin cá nhân.

Link tham khảo: http://genk.vn/ung-dung-rac-gia-9-trieu-dong-tran-ngap-play-store-viet-nam-lap-trinh-vien-thu-loi-hang-tram-trieu-dong-20191118153430535.chn

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	Linux	CVE-2019-18807 CVE-2019-18808 CVE-2019-18683 …	Nhóm 16 lỗ hổng trên hệ điều hành Linux (Linux kernel) cho phép đối tượng tấn công khai thu thập thông tin, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá.
2	Cisco	CVE-2019-1877 CVE-2019-1980 CVE-2019-1982 ...	Nhóm 06 lỗ hổng trên một số thành phần, sản phẩm của Cisco (Cisco Enterprise Chat and Email…) cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
3	Apache	CVE-2011-3923 CVE-2019-12410 CVE-2019-12406 …	Nhóm 07 lỗ hổng trên một số thành phần của Apache (Arrow, CXF…) cho phép đối tượng tấn công khai thác lỗi bộ nhớ trong hệ thống, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE-2019-18668 CVE-2014-9013 CVE-2014-9014 …	Nhóm 05 lỗ hổng trên phần mềm Wordpress cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa, chiếm quyền điều khiển hệ thống	Đã có thông tin xác nhận và bản vá
5	Google	CVE-2011-2353 CVE-2011-2807 CVE-2011-2337 …	Nhóm 08 lỗ hổng trên một số sản phẩm của Google (Google Chrome) cho phép đối tượng tấn công tấn công từ chối dịch vụ	Chưa có thông tin xác nhận và bản vá
6	Qualcomm	CVE-2019-2302 CVE-2019-10522 CVE-2019-10505 …	Nhóm 31 lỗ hổng trên một số thành phần, sản phẩm của Qualcomm (Snapdragon Auto, Snapdragon Mobile) cho phép đối tượng tấn công có quyền kiểm soát hệ thống. 14 lỗ hổng có điểm CVSS đặc biệt nghiêm trọng 10.0 và 9.3	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	soplifan.ru
6	tydz0fqvt.ru
7	xjpakmdcfuqe.com
8	somicrososoft.ru
9	wd9szyfi.ru
10	morphed.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.