BẢN TIN NỘI BỘ

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

1. Quy định chặt chẽ hơn việc kiểm soát các thiết bị kết nối mạng tạm thời

Sự phổ biến của BYOD (thiết bị mang theo) và các thiết bị di động đang làm gia tăng các tấn công tội phạm mạng theo cấp số nhân. Theo báo cáo của TechAdvisory.org, 25% số lượng phần mềm độc hại được phát tán thông qua các thiết bị USB. Các thiết bị kết nối mạng tạm thời - hoặc các thiết bị không được kết nối với mạng liên tục (bao gồm các thiết bị USB) đang là một lỗ hổng cấp tính cho cả môi trường công nghệ thông tin (information technology - IT) và công nghệ vận hành (operational technology - OT).

Khi một thiết bị USB được cắm vào máy tính có kết nối mạng, mọi sự cố đều có thể xảy ra. Các thiết bị này có thể chứa cả mối đe dọa trên tệp và phương tiện, sử dụng thiết bị như thế này sẽ bỏ qua các lớp bảo mật của tổ chức. Trong mọi trường hợp, phần mềm độc hại có thể là thảm họa cho toàn bộ tập đoàn, đặc biệt trong các cuộc tấn công vào môi trường OT - nơi phần cứng và phần mềm được sử dụng để chạy các hệ thống kiểm soát công nghiệp có thể là một trong những điều tồi tệ nhất. Rủi ro này thường tăng lên do việc sử dụng các phương tiện di động là cách duy nhất để đưa các tệp bị nhiễm phần mềm độc hại vào các mạng OT đã được cô lập. Theo một báo cáo mới từ Fortinet, 77% các tổ chức có mội trường mạng OT đã gặp sự cố bảo mật CNTT trong năm qua và 78% trong số các tổ chức chức đó có một chút chú ý vào an ninh mạng trong môi trường OT của họ.

Ví dụ, đầu năm 2019, nhà máy sản xuất nhôm Na Uy Norsk Hydro đã mất hơn 40 triệu USD trong những tuần sau khi bị tấn công bởi mã độc tống tiền - ransomware. Cuộc tấn công đã buộc công ty ngừng hoạt động sản xuất tự động và phải chuyển sang hoạt động thủ công. Từ đó ta có thể thấy được thiệt hại vô cùng lớn mà một thiết bị cầm tay bị nhiễm mã độc trong môi trường OT có thể gây ra khi nó liên quan đến cơ sở hạ tầng quan trọng.

Mới đây, một phụ nữ đã bị Sở Mật vụ Mỹ bắt giữ tại khu nghỉ mát Mar-a-Lago của Tổng thống Trump. Cô này bị bắt khi mang theo hộ chiếu, điện thoại di động, máy tính xách tay, ổ cứng gắn ngoài và USB có chứa phần mềm độc hại vào khu nghỉ mát. Việc này nếu không được phát hiện kịp thời có thể dẫn đến việc một nhân viên Mật vụ có cắm USB độc hại vào máy tính xách tay quan trọng nào đó mà không được kiểm tra an ninh chặt chẽ.

Để khắc phục những vi phạm đã diễn ra và các nguy cơ hiện hữu, cần có những giải pháp thích hợp.

Theo Schneider Electric, một trong những chuyên gia lớn nhất thế giới về quản lý năng lượng và tự động hóa, là người dẫn đầu về an ninh mạng trong các bước của mọi quy trình và bộ phận của chuỗi cung ứng. Vào năm 2017, dòng sản phẩm an toàn Triconx đã bị tấn công bằng phần mềm độc hại có tên là “Triton” (hay “Trisisis”), với mục đích cố gắng phá hoại thiết bị an toàn (SIS-Safety Instrumented Systems) ở Trung Đông. Ông đã hóa giải thành công cuộc tấn công bằng cách tiếp cận toàn diện,

trong đó sử dụng việc tiếp cận nhiều lớp đối với an ninh mạng theo các tiêu chuẩn NIST với năm chức năng: xác định, bảo vệ, phát hiện, phản hồi và phục hồi. Từ đó đã đảm bảo an toàn cho tất cả khách hàng.

Trên thế giới, nhiều TC/DN đã đưa ra các quy định của mình đối với các thiết bị kết nối mạng tạm thời. Ví dụ, Tập đoàn điện Bắc Mỹ (NERC) đã đưa ra các tiêu chuẩn mới, như CIP-010 R4, để quản lý việc sử dụng phương tiện di động và các thiết bị khác; US-CERT (Nhóm ứng phó khẩn cấp máy tính Hoa Kỳ) cũng đã đưa ra nhiều cảnh báo về mối đe dọa của USB….

Trước tình hình này, giải pháp sử dụng các ki-ốt an ninh mạng truyền thông di động là một cách hiệu quả để ngăn chặn các cuộc tấn công và có khả năng hiển thị cũng như thể hiện sự tuân thủ quy định. Theo Oren Dvoskin, cựu chuyên gia CNTT của Không quân Israel và là giám đốc tiếp thị hiện tại của Sasa Software, bộ chỉ huy mạng của Israel khuyến nghị sử dụng các ki-ốt an ninh mạng truyền thông di động với giải giáp tái cấu trúc nội dung (content disarm and reconstruction - CDR) là lớp bảo mật cơ bản để bảo vệ cơ sở hạ tầng quan trọng. Thiết kế của các ki-ốt ngăn chặn các cuộc tấn công dựa trên truyền thông di động và công nghệ CDR tích hợp ngăn chặn các cuộc tấn công nâng cao dựa trên tệp và khó phát hiện. Hiệu quả của giải pháp CDR và các ki-ốt an ninh mạng trong các lĩnh vực thương mại được quy định đã sử dụng một cách rộng rãi ở Israel.

Ví dụ về một ki-ốt sử dụng phần mềm sao chép-ghi Sasa: Các ki-ốt được quản lý bởi trung tâm và được phân phối theo địa lý tại nhiều địa điểm. Các tệp được sao chép từ phương tiện di động sau đó được quét/vô hiệu hóa trước khi chuyển sang phương tiện đáng tin cậy hoặc sẽ được gửi an toàn vào mạng OT bằng cách sử dụng ống dữ liệu hai chiều.

Tại Singapore, các cơ quan an ninh cũng đã áp dụng các khuyến nghị này khi hợp tác với Israel. Tại Hoa Kỳ, các tổ chức thương mại đang tuân theo các khuyến nghị và tiêu chuẩn quản lý ngành năng lượng của US-CERT với các chính sách kiểm soát chặt chẽ, chẳng hạn như lệnh cấm ổ đĩa, USB của IBM.

Với các cuộc tấn công mạng được nhắm mục tiêu tấn công vào môi trường mạng OT đang gia tăng, đã đến lúc các CISO cần có một kế hoạch vững chắc về cách bảo vệ môi trường OT tránh khỏi việc bị các mã độc trên các thiết bị kết nối tạm thời xâm nhập. Các thiết bị này bao gồm: ổ USB, đĩa quang, thẻ SD, đĩa mềm cũ và thậm chí toàn bộ máy tính xách tay được các nhà cung cấp đưa vào môi trường OT.

Các thiết bị mạng tạm thời rất cần thiết cho các hoạt động hàng ngày và bảo trì các mạng bị cô lập và phải được xử lý bởi một ki-ốt an ninh mạng sử dụng công nghệ CDR trước khi chúng được đưa vào mạng. Việc chỉ quét Anti Virus là không đủ để chống lại các cuộc tấn công dựa trên phần mềm độc hại và phương tiện truyền thông tiên tiến. Việc sử dụng các ki-ốt an ninh mạng cho phép chuyển các tệp an toàn từ phương tiện vào mạng OT của các tổ chức, đồng thời cho phép thực thi chính sách, khả năng hiển thị và kiểm soát hoàn toàn bằng hệ thống báo cáo và quản lý trung tâm.

Link tham khảo: http://antoanthongtin.vn/Detail.aspx?CatID=751fd4e7-4da5-4f31-85aa-be0240fe4910&NewsID=bb9323f9-3a0e-4d6a-b007-2b7d02d278a1

2. 1,2 tỷ dữ liệu tài khoản cá nhân Amazon bị đánh cắp

Khoảng 1,2 tỷ dữ liệu tài khoản cá nhân vừa bị đánh cắp từ hệ thống của Amazon Web Services. Đây được xem như một trong những vụ rò rỉ thông tin lớn nhất mọi thời đại.

Theo SiliconAngle, các thông tin rò rỉ bao gồm nhiều cơ sở dữ liệu khác nhau. Một số dữ liệu dưới dạng các địa chỉ IP, trong khi nhiều dữ liệu khác ở dạng không thể xác định.

Sự cố trên được phát hiện bởi Bob Diachenko và Vinny Troia. Cục điều tra Liên bang Mỹ (FBI) đang vào cuộc để điều tra vụ việc này. Theo đánh giá sơ bộ, rất có thể nhiều vụ hack đã được thực hiện cùng lúc với nhau để tạo một vụ rò rỉ thông tin lớn chưa từng có.

Theo Dvir Babila - người đứng đầu bộ phận bảo mật của Cycognito, phạm vi quá lớn của sự việc khiến nhiều người đặt ra câu hỏi về thủ phạm đã đứng đằng sau. Điều này đòi hỏi đội ngũ điều tra viên phải liên kết rất nhiều tình tiết khác nhau nhờ vào sự lưu vết trên các hệ thống CNTT để tạo nên một bức tranh hoàn chỉnh.

Babila cho rằng, việc tấn công một cách thủ công nhằm lấy cắp lượng dữ liệu của hàng tỷ người cùng lúc là điều không thể. Do vậy, tin tặc nhiều khả năng sẽ sử dụng các mô hình tính toán khác nhau, kết hợp với tài nguyên được lưu trữ trên các đám mây để tấn công đánh cắp thông tin với mức độ tự động hoá nhất định.

Theo hacker Jason Kent của Cequence Security, chưa nói đến số lượng, chỉ tính riêng tính chất của loại dữ liệu thôi cũng đã đủ cho thấy mức độ nghiêm trọng của sự việc.

Thông thường, các dữ liệu đánh cắp thường là dạng dữ liệu theo một ngữ cảnh nhất định, ví dụ như dữ liệu tài chính. Tuy nhiên, các dữ liệu trong vụ đánh cắp là những thông tin được sắp xếp và có mối liên kết với nhau, do đó khi các dữ liệu này bị đánh cắp đồng thời, khả năng nguy hiểm sẽ lớn hơn nhiều.

Chia sẻ về vụ tấn công, Phó giám đốc phụ trách chiến lược và quản lý sản phẩm của Tripwire - ông Tim Erlin lưu ý rằng: “Chúng ta vẫn thường lo lắng về các dữ liệu nhạy cảm. Tuy nhiên với một thế giới kết nối, các dữ liệu có tính liên kết với nhau mới là điều đáng quan ngại nhất.”. Do vậy, vị chuyên gia của Tripwire cho rằng hiện vẫn chưa có cách nào để đo lường hết các tác động từ vụ rò rỉ thông tin này.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần đề cao cảnh giác khi sử dụng các giao dịch trên mạng, tránh lộ lọt để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/su-co-the-ky-1-2-ty-du-lieu-tai-khoan-ca-nhan-vi-danh-cap-591363.html

3. Lỗ hổng đã được vá vẫn tồn tại trong nhiều ứng dụng Android phổ biến

Những lỗ hổng nghiêm trọng đã được xử lý cách đây một năm vẫn tồn tại trong nhiều ứng dụng Android phổ biến do nhà phát triển không áp dụng bản vá cho các thư viện của bên thứ ba.

Các nhà nghiên cứu của hãng Check Point chọn lọc được ba lỗ hổng thực thi mã tùy ý nghiêm trọng đã có bản vá vào các năm 2014, 2015 và 2016 được sử dụng rộng rãi trong các thư viện của bên thứ ba.

Hãng này giải thích rằng các ứng dụng trên mobile thường phụ thuộc vào các thư viện gốc, hoặc là được lấy từ các dự án mã nguồn mở hoặc là sử dụng các đoạn code từ phần mềm mã nguồn mở. Nếu tìm thấy lỗ hổng trong các dự án mã nguồn mở, nhà phát triển có thể đưa ra một bản vá lỗi nhưng không đảm bảo liệu việc khắc phục này cũng sẽ được áp dụng cho các phần mềm khác phụ thuộc vào code của họ.

Tháng 06/2019, hãng Check Point đã thực hiện quét các ứng dụng Android hiện có trên Google Play để biết liệu chúng có sử dụng các thư viện nào dính lỗ hổng hay không.

Một trong những lỗ hổng được tìm thấy là CVE-2014-8962, một lỗi tràn bộ đệm trong định dạng file audio libFLAC (Free Lossless Audio Codec) có thể bị khai thác để thực thi mã tùy ý hoặc tấn công từ chối dịch vụ bằng cách thuyết phục người dùng mục tiêu mở một file audio FLAC tự tạo cùng với ứng dụng dùng phiên bản libFLAC có lỗ hổng.

Qua phân tích, Check Point tiết lộ rằng lỗ hổng này vẫn tồn tại trong các ứng dụng phát nhạc LiveXLive, điều khiển giọng nói Moto Voice trên các dòng điện thoại Motorola và các ứng dụng Yahoo khác. Tất cả những ứng dụng nàyđã được hàng triệu thậm chí là hàng chục triệu lượt tải về từ Google Play.

Lỗ hổng thứ hai là CVE-2015-8271 ảnh hưởng đến bộ công cụ RTMPDump trong luồng phát RTMP và có thể bị khai thác để thực thi mã tùy ý.

Lỗ hổng này nằm trong thư viện được sử dụng cho các ứng dụng Facebook, Facebook Messenger, Lenovo SHAREit, Mobile Legends: Bang Bang, Smule, JOOX Music và các ứng dụng WeChat. Ba ứng dụng đầu tiên có trên 1 tỷ lượt tải về trên Google Play, trong khi số còn lại là trên 100 triệu.

Lỗ hổng cuối cùng được các nhà nghiên cứu Check Point tìm thấy là CVE-2016-3062, ảnh hưởng đến thư viện Libav, cho phép thực thi mã từ xa và tấn công DoS thông qua các file media tự tạo. Thư viện dính lỗ hổng này được tìm thấy trong các ứng dụng AliExpress, Video MP3 Converter, Lazada, VivaVideo, Smule, JOOX Music, Retrica và TuneIn đều có trên 100 triệu lượt tải về.

Ngoài ra còn có hàng trăm ứng dụng trên Android phổ biến đã được tìm thấy bị ảnh hưởng bởi ba lỗ hổng này.

Nhà nghiên cứu Slava Makkaveev cho biết: “Dù chỉ với 3 lỗi, tất cả đều đã được khắc phục cách đây 2 năm cũng đủ khiến hàng trăm ứng dụng có nguy cơ dính lỗ hổng thực thi mã từ xa. Hãy thử tưởng tượng xem có bao nhiêu ứng dụng phổ biến

là mục tiêu của kẻ tấn công nếu chúng quét Google Play và tìm ra 100 lỗ hổng đã được nêu?"

Khuyến nghị:

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

Link tham khảo: https://whitehat.vn/threads/lo-hong-da-duoc-va-van-ton-tai-trong-nhieu-ung-dung-android-pho-bien.12978/

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	Microsoft	CVE-2019-1427 CVE-2019-1426 CVE-2019-1429 …	Nhóm 72 lỗ hổng trên phần mềm Microsoft (Microsoft Edge …) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh từ xa.	Đã có thông tin xác nhận và bản vá.
2	Android	CVE-2019-2211 CVE-2019-2207 CVE-2019-2205	Nhóm 28 lỗ hổng trên một số thành phần của hệ điều hành Android cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh từ xa, leo thang trong quyền thực thi hệ thống	Đã có thông tin xác nhận và bản vá
3	D-link	CVE-2019-18852	01 lỗ hổng trên thiết bị D-link (DIR-600,..) cho phép đối tượng tấn công thu thập thông tin tài khoản đã thiết lập sẵn trong các file cấu hình. Lổ hổng có điểm CVSS 10.0 (đặc biệt nghiêm trọng)	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE-2019-17661 CVE-2019-17234 CVE-2019-17237 …	Nhóm 11 lỗ hổng trên một số thành phần, sản phẩm của Wordpress cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ 01 lỗ hổng có điểm CVSS 9.0 (cao)	Đã có thông tin xác nhận và bản vá
5	Adobe	CVE-2019-7960 CVE-2019-8239 CVE-2019-8247	Nhóm 11 lỗ hổng trên phần mềm Adobe (Animate CC…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh.	Chưa có thông tin xác nhận và bản vá
6	Huawei	CVE-2019-5289 CVE-2019-5246 CVE-2019-5230	Nhóm 16 lỗ hổng trên một số sản phẩm của Huawei cho phép đối tượng tấn công chèn và thực thi mã lệnh từ xa, thu thập thông tin, chiếm quyền thực thi trên màn hình thiết bị.	Đã có thông tin xác nhận và bản vá

7	Asus	CVE-2019-15402 CVE-2019-15401 CVE-2019-15406	Nhóm 27 lỗ hổng trên một số sản phẩm của Asus (Asus-X00k,…) cho phép đối tượng tấn công thực thi mã lệnh tùy ý	Chưa có thông tin xác nhận và bản vá
8	Intel	CVE-2019-11135 CVE-2019-11174 CVE-2019-11170 …	Nhóm 54 lỗ hổng trên một số sản phẩm , thành phần của Intel cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ	Chưa 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	egpjjdxis.ru
5	xjpakmdcfuqe.com
6	soplifan.ru
7	xdqzpbcgrvkj.ru
8	befatd8jx.ru
9	korkrsosn.info
10	www.cityofangelsmagazine.com

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.