BẢN TIN NỘI BỘ

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

1. Apple vô tình 'mở cửa' cho tin tặc đánh cắp dữ liệu người dùng

Apple đã "quên" không vá một lỗi trong hệ điều hành iOS khiến người dùng với bản cập nhật iOS 12.4 mới nhất có thể bẻ khóa điện thoại (jailbreak), nhưng cũng khiến họ dễ bị tấn công.

Lỗi này được các nhà nghiên cứu bảo mật phát hiện vào cuối tuần qua. Trước đây, nó đã từng được các nhà phân tích của Google phát hiện và Apple vá lại trong bản iOS 12.3. Nhưng một quá trình chuyển đổi gần đây sang bản iOS 12.4 phát hành vào tháng 7, lỗ hổng này đã xuất hiện trở lại.

Trang Motherboard dẫn lời các nhà nghiên cứu giấu tên cho biết, lỗ hổng bảo mật trên iOS 12.4 làm giảm đáng kể rào cản đối với các tin tặc tìm cách đánh cắp dữ liệu của người dùng.

'Do 12.4 là phiên bản iOS mới nhất hiện có và là phiên bản duy nhất mà Apple cho phép nâng cấp lên, trong vài ngày tới (cho đến bản 12.4.1 phát hành), tất cả các thiết bị đang chạy phiên bản hệ điều hành này (hoặc bất kỳ phiên bản iOS 11.x và 12 .x dưới 12.3) sẽ dễ bị bẻ khóa - điều đó có nghĩa là điện thoại iPhone cũng dễ bị tổn thương,' Jonathan Levin, một nhà nghiên cứu bảo mật nói với Motherboard.

Về mặt lý thuyết, các tin tặc có đủ trình độ để có thể khai thác lỗ hổng này trong Safari hoặc, 'tạo ra một phần mềm gián điệp hoàn hảo.'

Mã độc khai thác lỗ hổng cũng có thể được nhúng vào một ứng dụng, điều này sẽ khiến bất cứ ai tải mã độc này bị hack hoặc kết hợp với một cuộc tấn công trình duyệt.

Có thể sẽ mất vài ngày trước khi Apple phát hành iOS 12.4.1 để sửa bản vá bịt trở lại lỗ hổng nguy hiểm này.

Khuyến nghị:

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

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/apple-vo-tinh-mo-cua-cho-tin-tac-danh-cap-du-lieu-nguoi-dung-560776.html

2. Phần lớn cuộc tấn công Job attack trên Microsoft SQL server nhắm vào Châu Á

Microsoft SQL Server được các công ty trên thế giới sử dụng nhằm quản lý cơ sở dữ liệu. Với mức độ phổ biến như vậy, cùng với việc không có cơ chế bảo vệ đủ mạnh, Microsoft SQL Server trở thành mục tiêu của những kẻ tấn công với nhiều mục đích khác nhau.

Một trong những cuộc tấn công phổ biến nhất trên Microsoft SQL Server là tấn công dựa trên các Job độc hại. Dù đã xuất hiện được một thời gian, nhưng các kẻ tấn công vẫn tận dụng hình thức này để truy cập vào các máy trạm thông qua mật khẩu quản trị yếu.

Theo số liệu được thống kê, Việt Nam là nước có số lượng cuộc tấn công nhiều nhất, chiếm 16%. Tiếp theo đó là Nga với 12%, Ấn Độ là 7%, Thổ Nhĩ Kỳ và Brazil ở mức 5%.

Theo Kaspersky, các cuộc tấn công Microsoft SQL Server thường lớn và không có mục tiêu cụ thể. Các kẻ tấn công quét các mạng con (sub-network) để tìm kiếm các máy chủ có mật khẩu yếu.

Sau khi kiểm tra từ xa để xác định cài đặt SQL Server, kẻ tấn công sẽ brute force mật khẩu để truy cập vào hệ thống.

Bước tiếp theo là sửa cấu hình máy chủ để truy cập vào dòng lệnh, cho phép kẻ tấn công ngấm ngầm đưa phần mềm độc hại vào hệ thống đích thông qua các Job của SQL Server.

Job biểu thị một chuỗi các lệnh bởi SQL Server và có thể bao gồm nhiều hành động khác nhau, một số trong đó có thể bị tận dụng để thực thi mã hoặc các hoạt động độc hại khác.

Ví dụ, các kẻ tấn công có thể cài đặt Job có nhiệm vụ download mã độc bằng tiện ích ftp.exe tiêu chuẩn, tải phần mềm độc hại từ nguồn từ xa bằng JavaScript hoặc viết và thực thi phần mềm độc hại trên hệ thống.

Phân tích về các payload của các cuộc tấn công vào MS SQL Server thông qua Job độc hại cho thấy hầu hết là các mã độc đào tiền ảo hoặc backdoor truy cập từ xa. Một số payload khác có nhiệm vụ lấy mật khẩu hoặc leo thang đặc quyền.

Để an toàn, quản trị viên nên cân nhắc việc sử dụng mật khẩu mạnh cho các tài khoản SQL Server. Kiểm tra Agent SQL Server cho các Job của bên thứ ba cũng có thể giúp phát hiện các xâm nhập có thể xảy ra.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị cần tuân thủ việc đặt mật khẩu mạnh và đổi mật khẩu theo định kỳ để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/phan-lon-cuoc-tan-cong-job-attack-tren-microsoft-sql-server-nham-vao-chau-a.12611/

3. Hacker mạo danh doanh nghiệp chuyển phát để lừa phát tán email chứa mã độc

Theo nhận định của chuyên gia Công ty CyRadar, sử dụng email để phát tán mã độc là hình thức không còn mới tập trung vào sự thiếu cảnh giác của người dùng. Sự thiếu cảnh giác này được tạo ra nhờ nội dung có tính thuyết phục và gây tò mò cho người dùng.

Mới đây, qua hệ thống giám sát SOC của CyRadar, việc hacker tấn công một khách hàng của CyRadar là doanh nghiệp chuyển phát thông qua hình thức phát tán email cài mã độc đã bị phát hiện. Một lượng lớn email độc hại đã được gửi đến nhân viên của doanh nghiệp này với nội dung gây khá nhiều sự tò mò.

Khi người dùng thực hiện tải, giải nén và mở tệp tin có chứa mã độc, mã độc sẽ được thực thi lây nhiễm trên máy nạn nhân.

Chuyên gia Đỗ Quang Thắng của CyRadar phân tích, về hành vi mã độc thực hiện nhiều thao tác nguy hiểm như ăn cắp thông tin người dùng, tạo cổng sau cho kẻ tấn công nhằm chiếm quyền điều khiển máy tiếp tục lây nhiễm sâu vào bên trong hệ thống.

Mã độc được kết nối đến máy chủ độc hại. Thay vì đăng ký tên miền, hacker sử dụng DNS miễn phí nhằm linh hoạt trong việc thay đổi tên miền, cũng là để qua mặt một số biện pháp bảo vệ. Tùy thuộc vào lệnh trả về mã độc sẽ thực hiện những hành vi độc hại khác nhau.

Để tránh trở thành nạn nhân của thư rác độc hại, chuyên gia CyRadar khuyến nghị, người dùng không nhấp vào liên kết trong email, văn bản, tin nhắn hoặc bài đăng trên mạng xã hội nếu chúng đến từ những người hoặc tổ chức mà bạn không biết, hoặc có địa chỉ đáng ngờ. Người dùng cũng nên kiểm tra lại kỹ các thông tin, tổ chức doanh nghiệp.

Đối với đội ngũ CNTT và hệ thống doanh nghiệp cần có những biện pháp chặt chẽ trong việc giám sát, phát hiện trong những trường hợp này vì nó có thể xảy ra bất cứ lúc nào. Đồng thời nâng cao nhận thức cho người dùng qua truyền thông hoặc các khóa đào tạo nhận thức...

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng không nhấp vào liên kết trong email, văn bản, tin nhắn hoặc bài đăng trên mạng xã hội nếu chúng đến từ những người hoặc tổ chức mà bạn không biết, hoặc có địa chỉ đáng ngờ, cần kiểm tra kỹ các thông tin trước của người gửi trước khi nhấn vào liên kết.

Link tham khảo: https://ictnews.vn/cntt/bao-mat/hacker-mao-danh-doanh-nghiep-chuyen-phat-de-lua-phat-tan-email-chua-ma-doc-188941.ict

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-2019-1151 CVE-2019-1144 CVE-2019-1181 ...	Nhóm 88 lỗ hổng trên sản phẩm, ứng dụng của Microsoft (Remote Desktop Service, Office, Windows 10, Azure Active Directory, Defender, DHCP Client, Microsoft Edge) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh, tấn công leo thang, Một số lỗ hổng nghiêm trọng (CVE-2019-1181, CVE-2019-1182) đã được Cục ATTT cảnh báo trong văn bản cảnh báo số 751/CATTT-NCSC	Đã có thông tin xác nhận và bản vá.
2	Atlassian	CVE-2019-11581 CVE-2019-15053 CVE-2018-20826 CVE-2019-8448 …..	Nhóm 05 lỗ hổng trong một số sản phẩm của Atlassian (Jira, Confluence Server, Jira Server and Data Center, …) cho phép đối tượng tấn công thiết lập Reporter, khai thác lỗi XSS, chèn và thực thi mã lệnh. Lỗ hổng CVE-2019-11581 đã được Cục ATTTT cảnh báo trực tiếp đến tổ chức đang public máy chủ Jira trên Internet trong văn bản số 705/CATTT-NCSC	Đã có thông tin xác nhận và bản vá.
3	Wordpress	CVE-2019-14948 CVE-2017-18515 CVE-2016-10889	Nhóm 136 lỗ hổng trong nhiều plugin(newstatpress,wpstatistics,events-manager, FV Flowplayer Video Player, nextgen-gallery, subscriber, wpgoogle-map-plugin,...) củaWordpress cho phép đối tượngtấn công thự chiện khai thác lỗi SQL Injection,	Đã có thông tin xác nhận và bản vá

4	Huawei	CVE-2019-5223 CVE-2019-5299 CVE-2019-5280	Nhóm 03 lỗ hổng trên một số sản phẩm của Huawei(PCManager, Huawei CloudLink Phone, Huawei mobile phones Hima) cho phép đối tượng tấn công chèn và thực thi mã lệnh, tấn công nghe lén	Đã có thông tin xác nhận và bản vá
5	Adobe	CVE-2019-8062 CVE-2019-7870 CVE-2019-8063	Nhóm 09 lỗ hổng trên một số sản phẩm của Adobe (Adobe Experience Manager, Adobe Premiere Pro CC, AdobePrelude CC, Creative Cloud Desktop Application) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh, tấn công leo thang	Đã có thông tin xác nhận và bản vá
6	Bluetooth	CVE-2019-9506	Lỗ hổng trong tất cả thiết bị hỗ trợ kết nối Bluetooth BR/EDR trong quá trình thiết lập khóa mật mã cho phép đối tượng tấn công lấy dò đoán khóa mã hóa để giải mã dữ liệu trao đổi từ đó có thể thu thập thông tin và tấn công leo thang.	Đã có thông tin xác nhận và bản vá
7	HTTP/2	CVE-2019-9512 CVE-2019-9513 CVE-2019-9511 ...	Nhóm 09 Lỗ hổng trong việc thực thi HTTP/2 cho phép thực hiện nhiều h.nh thức tấn công từ chối dịch vụ. Lỗ hổng này có thể được khai thác trên diện rộng để thực hiện tấn công từ chối dịch vụ quy mô lớn Ảnh hưởng tới nhiều ứng dụng, máy chủ tham khảo chi tiết tại: https://vuls.cert.org/confluence/pages/viewpage.action?pageId=56393752	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	kn0ugjov.ru
5	soplifan.ru
6	xjpakmdcfuqe.com
7	xdqzpbcgrvkj.ru
8	75ulqnwb.ru
9	www.cityofangelsmagazine.com
10	somicrososoft.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.