BẢN TIN NỘI BỘ

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

1. TeamViewer bị tin tặc APT41 của Trung Quốc xâm nhập, cho phép truy cập và cài backdoor lên hệ thống

Phần mềm điều khiển từ xa nổi tiếng TeamViewer đã bị hack từ nhiều năm trước và một số máy tính người dùng đã bị tin tặc kiểm soát và cài đặt các cửa hậu để đánh cắp dữ liệu.

Hiện tại, TeamViewer vẫn chưa thừa nhận rằng máy chủ đã bị tấn công. Ngược lại, các nhà phát triển cho biết người dùng bị tấn công chủ yếu bằng cách rò rỉ ID và mật khẩu từ xa. Tuy nhiên, điều gây sốc là công ty bảo mật FireEye đã một lần nữa tiết lộ rằng TeamViewer đã bị hack. Kẻ tấn công có thể điều khiển tất cả các máy tính đăng nhập vào phần mềm và vận hành nó tùy ý.

Mới đây, kiến trúc sư an ninh hàng đầu đến từ công ty bảo mật hàng đầu FireEye, đã viết trên Twitter rằng TeamViewer đã bị hack và rò rỉ mật khẩu tài khoản của người dùng. Nhóm tin tặc này là APT41. Fire Eye cho biết trên Twitter rằng tin tặc có thể truy cập nó trên bất kỳ máy tính nào đã cài đặt TeamViewer.

Từ những bức ảnh được phát hành bởi FireEye, đây sẽ là một bài thuyết trình được trình bày tại hội nghị bảo mật do Fire Eye tổ chức và hãng này không tiết lộ chi tiết cụ thể. Tuy nhiên, công ty bảo mật này là một nhóm nghiên cứu bảo mật nổi tiếng trong ngành, vì vậy độ tin cậy của tin tức được công bố là 100%, số liệu cụ thể về nạn nhân bị ảnh hưởng và phương thức khai thác của nhóm tin tặc không được tiết lộ.

Theo hình ảnh được tiết lộ bởi FireEye thì cuộc tấn công này diễn ra vào năm 2017-2018. Báo cáo tiết lộ TeamViewer đã bị hack vào năm 2016 khi một số lượng lớn người dùng bị tấn công và đánh cắp thông tin tài chính chỉ trong 24 giờ.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và người quản trị cần tuân thủ các chính sách an toàn thông tin đã ban hành, không sử dụng TeamViewer để tránh nguy cơ cho hệ thống.

Link tham khảo: https://whitehat.vn/threads/teamviewer-bi-tin-tac-apt41-cua-trung-quoc-xam-nhap-cho-phep-truy-cap-va-cai-backoor-len-he-thong.12814/

2. Apple gửi dữ liệu duyệt web trên iPhone cho công ty TQ

Cụ thể, trình duyệt Safari trên iPhone bị tố là "tội đồ" trong trường hợp này. Safari được tích hợp cơ chế kiểm soát an ninh giúp ngăn chặn các hành vi độc hại như lừa đảo phishing.

Trên Safari, gói công cụ giúp bảo vệ người dùng này có tên Fraudulent Website Warning. Để tính năng có thể hoạt động chuẩn xác, Safari cần thu thập và gửi dữ liệu tới Google Safe Browsing.

Sở dĩ làm thế là bởi Safari cần so sánh các đường liên kết với danh sách đen của Google Safe Browsing, từ đó xác định trang web có an toàn hay không.

Tuy nhiên, ngoài việc gửi thông tin tới Google, Apple còn gửi dữ liệu tương tự tới Tencent, cái tên gắn liền với chế độ kiểm duyệt và có liên quan mật thiết với chính phủ Bắc Kinh. Hiện chưa rõ gói thông tin Safari gửi cho Tencent gồm những gì.

Người dùng iPhone có thể tắt tính năng Fraudulent Website Warning trong phần Settings > Safari > Privacy & security > Fraudulent Website Warning. Tuy nhiên, làm vậy cũng sẽ tắt luôn việc đối sánh đường link với kho dữ liệu của Google.

Apple chưa từng công bố việc hãng này có quan hệ hợp tác với Tencent. Tính năng Fraudulent Website Warning được bật tự động trên tất cả iPhone và iPad chạy hệ điều hành iOS 13.

Điều này có nghĩa dữ liệu duyệt web trên iPhone được bí mật gửi tới Google và Tencent.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/apple-gui-du-lieu-duyet-web-tren-iphone-cho-cong-ty-tq-577326.html

3. Triển khai đánh giá bảo mật trang web miễn phí

Công ty cổ phần An ninh mạng Việt Nam (VSEC) chính thức triển khai chương trình "Đánh giá bảo mật website miễn phí" tới tất cả doanh nghiệp đang hoạt động tại thị trường Việt Nam.

Theo thông tin từ Bộ Thông tin và Truyền thông, 6 tháng đầu năm 2019 tại Việt Nam xảy ra 3.159 vụ tấn công mạng vào các hệ thống thông tin, trong đó có 968 cuộc tấn công thay đổi giao diện (Deface), 635 cuộc tấn công cài cắm mã độc (Malware), 1.556 cuộc tấn công lừa đảo (Phishing).

Tuy hình thức tấn công thông qua các lỗ hổng đơn giản nhưng gây ra những thiệt hại lớn tới doanh nghiệp như hệ thống bị tê liệt, bị xóa dữ liệu, thời gian khôi phục lâu... Nguy hiểm hơn, các tin tặc sẽ tiến hành khai thác một cách âm thầm và lấy cắp nhiều thông tin nhạy cảm như: danh sách khách hàng, danh sách nhân viên, tài liệu dự án...

Với kỳ vọng nâng cao nhận thức và bảo mật an toàn thông tin mạng khi sử dụng website của doanh nghiệp Việt, VSEC phát động chương trình "Đánh giá website miễn phí" cho đối tượng hướng tới là các doanh nghiệp đang hoạt động tại Việt Nam.

Theo đó, bằng công nghệ rà soát bảo mật và giám sát website toàn diện, VSEC sẽ tiến hành rà soát website để phát hiện lỗ hổng bảo mật tiềm ẩn nguy cơ bị tấn công, từ đó các chuyên gia của VSEC sẽ đưa ra các cảnh báo về nguy cơ tấn công website và đề xuất giải pháp. Ngoài ra, VSEC cũng sẽ có chia sẻ và hướng dẫn các kỹ năng cần thiết về bảo mật và bảo vệ website dựa trên tình hình thực tế của từng doanh nghiệp.

Chương trình đánh giá website miễn phí sẽ bắt đầu diễn ra từ ngày 15.10 đến 31.12.2019.

Link tham khảo: https://thanhnien.vn/cong-nghe/trien-khai-danh-gia-bao-mat-trang-web-mien-phi-1136883.html

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	Adobe	CVE-2019-8073 CVE-2019-8074 CVE-2019-8072 CVE-2019-8075	Nhóm 04 lỗ hổng trên một số sản phẩm, thành phần của Adobe (Coldfusion, Flash Player ...) cho phép đối tượng tấn công thu thập thông tin trái phép, thực thi mã lệnh từ xa. 02 lỗ hổng có điểm đặc biệt nghiêm trọng là 10.0	Đã có thông tin xác nhận và bản vá.
2	Linux	CVE-2019-16994 CVE-2019-16995 CVE-2019-17054 …	Nhóm 09 lỗ hổng trên hệ điều hành Linux (linux_kernel) cho phép đối tượng tấn công thực thi mã lệnh tùy ý, thu thập thông tin, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	Dlink	CVE-2019-16920	Nhóm 01 lỗ hổng trên một số sản phẩm của thiết bị Dlink (DIR-655C, DIR-652, DIR-886L…) cho phép đối tượng tấn công thực thi mã lệnh từ xa, có được quyền truy cập hệ thống. Lỗ hổng có điểm đặc biệt nghiêm trọng là 10.0	Đã có thông tin xác nhận và bản vá
4	Android	CVE-2019-9259 CVE-2019-9266 CVE-2019-9301 …	Nhóm 257 lỗ hổng trên một số sản phẩm của Android (Android -10Android ID:A-112610994...) cho phép đối tượng tấn công thu thập thông tin trái phép, thực thi mã lệnh từ xa, làm tràn bộ đệm, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
5	Cisco	CVE-2019-12713 CVE-2019-12678 CVE-2019-12698 …	Nhóm có 43 lỗ hổng trên một số sản phẩm của Cisco (Cisco Adaptive Security Appliance Softwere, Firepower Threat Defense Software) cho phép đối tượng thực hiện tấn công	Chưa có thông tin xác nhận và bản vá

			XSS, tấn công tấn công từ chối dịch vụ, thực thi mã lệnh từ xa, thu thập thông tin trái phép	
6	Wordpress	CVE-2019-16931	Nhóm có 01 lỗ hổng trên một số sản phẩm, thành phần của Wordpress cho phép đối tượng tấn công thực thi mã lệnh tùy ý , tấn công qua XSS	Chưa có thông tin xác nhận và bản vá
7	Firefox	CVE-2019-11736 CVE-2019-11737 CVE-2019-11741	Nhóm có 20 lỗ hổng trên một số sản phẩm, thành phần của Firefox (Firefox<69, Firefox ESR<68.1…) cho phép đối tượng tấn công thực thi mã lệnh tùy ý, đánh cắp mật khẩu và xóa dữ liệu đã sử dụng của người dùng, tấn công UXSS. Có một số lỗ hổng mức nghiêm trọng cao (9.3 và 7.5)	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	ld3t8xao8.ru
6	xjpakmdcfuqe.com
7	xdqzpbcgrvkj.ru
8	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
9	cp.x1yuqjh9.ru
10	yrwyzgopwjug.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.