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

1. Google chặn lừa đảo thông qua trình duyệt web nhúng

Theo Engadget, các framework trình duyệt nhúng cho phép các nhà phát triển có thể tích hợp các trình duyệt web như Chromium vào ứng dụng của họ. Nó giúp người dùng cuối đăng nhập trực tiếp vào tài khoản Google, Facebook hoặc Twitter mà không cần phải chuyển sang phiên bản trình duyệt đầy đủ.

Tuy nhiên người dùng sẽ có những rủi ro lừa đảo liên quan đến trải nghiệm đăng nhập liền mạch này. Một cuộc tấn công lừa đảo trung gian có thể chặn thông tin liên lạc thời gian thực giữa người dùng và các nhà cung cấp như Google vì Google không thể phân biệt giữa một đăng nhập hợp pháp qua trình duyệt thông thường và đăng nhập trong các trình duyệt nhúng. Giải pháp Google đối với kiểu tấn công trung gian này là hãng sẽ chặn quá trình đăng nhập với các framework trình duyệt nhúng, bắt đầu từ tháng 6 tới.

Bên cạnh chính sách mới, Google cũng đã triển khai nhiều biện pháp bảo mật hơn xung quanh quá trình đăng nhập trong những tháng gần đây nhằm nỗ lực bảo vệ thông tin chi tiết của người dùng. Chẳng hạn, vào cuối năm 2018, hãng đã đưa ra một tính năng đánh giá rủi ro và đòi hỏi có JavaScript để có thể đăng nhập vào tài khoản.

Google khuyên các nhà phát triển nên chuyển sang xác thực OAuth dựa trên trình duyệt để hiển thị URL của trang web đang truy cập nhằm giúp họ tránh các cuộc tấn công lừa đảo. Ứng dụng sẽ gửi người dùng đến Chrome, Safari, Firefox…để nhập mật khẩu của họ với thông tin xác thực cần thiết.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị viên cần kiểm tra kỹ càng trước khi đăng nhập vào các tài khoản Google, Facebook hoặc Twitter trên trình duyệt nhúng để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/google-chan-lua-dao-thong-qua-trinh-duyet-web-nhung-1073189.html

2. Hacker tấn công Microsoft, đánh cắp nhiều thông tin

Các dịch vụ e-mail này bao gồm @outlook.com, @hotmail.com, và @msn.com. Vụ tấn công xảy ra từ đầu năm, hacker đã tiếp cận nhiều thông tin người dùng, Microsoft cho biết.

Cụ thể, các thông tin lọt vào tay tin tặc gồm địa chỉ e-mail, tên thư mục, tiêu đề e-mail, tên các địa chỉ e-mail mà người dùng liên lạc. Tuy nhiên, nội dung e-mail và file đính kèm không lộ ra ngoài, Microsoft xác nhận.

Truy cập trái phép diễn ra trong khoảng thời gian từ 1/1 – 28/3 vừa qua. Microsoft không tiết lộ chi tiết về việc tin tặc đã làm thế nào để xâm nhập vào hệ thống của hãng này bằng tài khoản nhân viên.

Hãng phần mềm cho biết đã ngay lập tức vô hiệu hóa tài khoản nhân viên nói trên.

Microsoft cảnh báo hoạt động lừa đảo sử dụng các tài khoản e-mail bị lộ ngày càng gia tăng, đồng thời khuyến cáo khách hàng đổi e-mail ngay lập tức. Microsoft cũng nói rõ rằng đây chỉ là biện pháp đề phòng bởi trên thực tế mật khẩu e-mail người dùng không bị lộ ra ngoài.

Chưa rõ bao nhiêu khách hàng sử dụng dịch vụ e-mail của Microsoft bị ảnh hưởng nhưng ít nhất một số người dùng tại châu Âu nằm trong số này.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần đổi mật khẩu tài khoản email theo định kỳ để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/hacker-tan-cong-microsoft-danh-cap-nhieu-thong-tin-523646.html

3. Việt Nam thành lập Liên minh Xử lý mã độc và phòng, chống tấn công mạng

Tại Hội thảo và Triển lãm quốc tế về an toàn, an ninh mạng Việt Nam 2019 (Vietnam Security Summit 2019), dưới sự bảo trợ của Bộ TT&TT, Cục An toàn thông tin và Hiệp hội An toàn thông tin Việt Nam (VNISA) cùng với 5 thành viên sáng lập đã công bố ra mắt Liên minh xử lý mã độc và phòng chống tấn công mạng.

Liên minh này là sáng kiến của Cục An toàn thông tin (Bộ TT&TT) cùng Hiệp hội An toàn thông tin Việt Nam. Liên minh xử lý mã độc và phòng chống tấn công mạng được thành lập nhằm đoàn kết, tập hợp lực lượng, từ đó tăng cường hợp tác, chia sẻ thông tin phục vụ công tác đảm bảo an toàn thông tin quốc gia và cộng đồng người dùng Internet tại Việt Nam.

Liên minh hoạt động dưới sự bảo trợ, dẫn dắt của Bộ Thông tin và Truyền thông. Trung tâm Giám sát an toàn không gian mạng quốc gia (Cục ATTT) và Hiệp hội An toàn thông tin Việt Nam nắm vai trò chủ trì liên minh.Thiết lập bộ phận hỗ trợ tiếp nhận và xử lý kịp thời các vướng mắc, tra soát, khiếu nại phát sinh nếu có trong qúa trình thực hiện.

Thành viên sáng lập Liên minh bao gồm: Công ty an ninh mạng Viettel, Trung tâm An toàn thông tin VNPT, Trung tâm An ninh mạng FPT, Công ty cổ phần BKAV và Công ty TNHH An ninh an toàn thông tin CMC.

Tại buổi ra mắt, các thành viên trong liên minh đã cùng nhau thống nhất thỏa thuận hợp tác với 4 mục tiêu.

1. Thúc đẩy hợp tác toàn diện giữa cơ quan nhà nước, Hiệp hội và doanh nghiệp nhằm cung cấp, phát triển những sản phẩm, dịch vụ hỗ trợ cho cộng đồng, xã hội.

2. Tăng cường mối quan hệ tin cậy, gắn kết, chia sẻ giữa các doanh nghiệp lớn đang làm về an toàn thông tin tại Việt Nam, nhằm huy động và gắn kết sức mạnh của doanh nghiệp trong công tác đảm bảo an toàn, an ninh mạng.

3. Cùng nhau bảo vệ tài sản của cơ quan, tổ chức và người dân Việt Nam trước các nguy cơ tấn công mạng.

4. Giảm tỉ lệ lây nhiễm mã độc tại Việt Nam, góp phần đưa Việt Nam trở thành quốc gia có môi trường mạng an toàn, tin cậy.

Link tham khảo: https://vietnamnet.vn/vn/thong-tin-truyen-thong/viet-nam-thanh-lap-lien-minh-xu-ly-ma-doc-va-phong-chong-tan-cong-mang-524000.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	IBM	CVE-2019-4155 CVE-2019-4013 CVE-2018-1994 CVE-2018-1903 CVE-2018-1885 ...	Nhóm 16 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (API Connect, DB2 Linux/ Windows, Rational Engineering Lifecycle Manage, IBM SDK, WebSphere Application Server...) cho phép đối tượng tấn công thực hiện thu thập thông tin, khai thác các lỗi tràn bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	Microsoft	CVE-2019-0592 CVE-2019-0609 CVE-2019-0739 CVE-2019-0771 CVE-2019-0861 ...	Nhóm 140 lỗ hổng trên nhiều sản phẩm của Microsoft (.NET Framework, Microsoft Edge, Exchange Server, Internet Explorer, Office Access Connectivity Engine, SharePoint) cho phép đối tượng tấn công thực hiện thu thập thông tin nhạy cảm trên hệ thống, thực thi mã lệnh và tấn công leo thang.	Đã có thông tin xác nhận và bản vá
3	Apache	CVE-2019-0211 CVE-2019-0229 CVE-2019-0215 CVE-2019-0217 CVE-2019-0199 …..	Nhóm 06 lỗ hổng trong một số sản phẩm của Apache (JMeter, Solr, Qpid Broker-J, Apache Traffic Server) cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn và thực thi mã lệnh trong phạm vi của ứng dụng.	Chưa có thông tin xác nhận và bản vá.
4	Cisco	CVE-2019-1827 CVE-2019-1828 …	Nhóm 02 lỗ hổng trên một số sản phẩm của Cisco (các dòng switch Nexus, NX-OS, FXOS Software,) cho phép truy cập và thông tin nhạy cảm lưu trữ trên hệ thống, chèn và thực thi mã lệnh để chiếm quyền kiểm soát thiết bị.	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	e1jlp5ii1.ru
6	xjpakmdcfuqe.com
7	6kbj7ea9.ru
8	xtyr0xg4w.ru
9	kukutrustnet777.info
10	plpanaifheaighai.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.