BẢN TIN NỘI BỘ

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

1. Xuất hiện cách thức hack thẻ tín dụng mới của người dùng

Gần đây, nhiều công ty lớn trên thế giới bị tấn công bởi một hình thức hack thẻ tín dụng của khách hàng hoàn toàn mới, nhằm đánh cắp thông tin tải khoản ngân hàng của khách hàng từ các trang web.

Chính quyền liên bang Mỹ đã đưa ra một cảnh báo cho người mua sắm liên quan đến thông tin thẻ tín dụng. Các thiết bị giấu kín nhằm thực hiện hành vi tội phạm (thường gắn với máy bơm trạm xăng tự động và cây ATM) sở hữu công nghệ ngày càng cao.

"Thật khó để đưa ra những con số chính xác xung quanh vấn đề này. Nhưng một điều chúng tôi biết chắc chắn là hàng trăm triệu thẻ tín dụng trên khắp thế giới đã bị đánh cắp thông tin trong suốt hai năm qua", Herb Stapleton - Trưởng bộ phận không gian mạng của FBI chia sẻ với CNBC.

Loại hình tấn công hoàn toàn mới này được gọi là e-skinkle hoặc Magecart. Tội phạm mạng có thể giành được quyền truy cập vào thông tin cá nhân và thẻ tín dụng của người dùng. Chúng có thể xâm nhập trực tiếp vào máy chủ trang web hoặc đột nhập vào một máy chủ lớn có chức năng hỗ trợ nhiều trang web mua sắm trực tuyến khác, từ đó theo dõi khách hàng của trang web mua sắm này mà không ai có thể nhận biết được.

Vì vậy, các chuyên gia khuyến cáo người tiêu dùng cần nắm rõ những điều dưới đây để bảo vệ chính mình khi mua sắm trực tuyến:

a. Luôn mua sắm bằng thẻ tín dụng thay vì thẻ ghi nợ trực tuyến

Ông Pargman, Giám đốc cấp cao về xử lý tội phạm mạng tại Binary Defense cho biết, việc sử dụng thẻ tín dụng sẽ làm giảm bớt sự bất tiện nếu thẻ của người dùng bị xâm phạm. Người dùng thẻ tín dụng thường phải chịu trách nhiệm pháp lý nếu có hành vi lừa đảo xảy ra. Ngoài ra, việc nhận lại tiền đối với thẻ ghi nợ của người dùng có thể mất rất nhiều thời gian.

b. Xem xét việc sử dụng thẻ tín dụng ảo

Không phải tất cả các ngân hàng đều cung cấp thẻ tín dụng ảo nhưng nếu có thể, người dùng nên trang bị cho mình loại thẻ này. Thẻ tín dụng ảo sở hữu số thẻ tín dụng được sử dụng cho các giao dịch cụ thể và cho một cá nhân cụ thể. Nếu con số này bị tấn công hoặc sử dụng sai mục đích đăng ký, mọi khoản thanh toán sẽ bị từ chối.

c. Theo dõi thẻ để phát hiện bất kỳ hoạt động bất thường nào và báo cáo ngay lập tức cho ngân hàng

Các chuyên gia của FBI cho biết, loại hình tấn công thông tin ngân hàng e-skimming đã xuất hiện khá lâu, tuy nhiên, hiện nay, loại tội phạm này luôn luôn đổi hình thức tấn công thông qua việc chia sẻ các phần mềm độc hại với công nghệ ngày càng tinh vi hơn.

Khuyến nghị: Người dùng cần kiểm tra kỹ khi thanh toán bằng thẻ tín dụng qua các trang web thanh toán trực tuyến để tránh bị lộ thông tin dẫn đến mất tài sản.

Link tham khảo: http://antoanthongtin.vn/an-toan-thong-tin/xuat-hien-cach-thuc-hack-the-tin-dung-moi-cua-nguoi-dung-105849

2. Chiếm quyền điều khiển web bằng mã độc giả mạo thông tin virus Corona

Lợi dụng sự quan tâm về dịch cúm Corona, tin tặc phát đi những đường link chứa mã ngụy trang dưới dạng tin về virus Corona. Những mã độc này sau đó được sử dụng đề chiếm quyền điều khiển web.

Hồi đầu tháng 2, hãng bảo mật Kaspersky từng đưa ra cảnh báo về việc các mã độc đang được tin tặc ngụy trang dưới dạng tài liệu liên quan đến virus Corona.

Theo đó, người dùng nhận được các thông tin gắn đường link chứa mã khai thác ngụy trang dưới dạng thông tin về virus Corona. Tên của tệp thể hiện nội dung hướng dẫn cách bảo vệ mọi người khỏi virus, cập nhật về các mối nguy hại, và thậm chí là quy trình phát hiện virus. Tuy nhiên, tất cả thông tin đều không đúng sự thật.

Những thông tin mới nhất cho thấy, các mã độc này được kẻ xấu phát tán nhằm mục đích chiếm quyền điều khiển website mà nạn nhân đang sở hữu. Thông tin này vừa được cảnh báo bởi Công ty CP An ninh mạng Việt Nam.

Đơn vị này đã phát đi cảnh báo về lỗ hổng bảo mật Cross-site request forgery (CSRF) trên plugin Code Snippets của nền tảng Wordpress. Nguy cơ từ lỗ hổng này là nó sẽ giúp tin tặc chiếm quyền quản trị website để thực hiện các mã lệnh từ xa. Với lỗ hổng này, tin tặc có thể điều khiển máy chủ và triển khai các hoạt động trái phép gây ảnh hưởng cho doanh nghiệp.

Lỗ hổng CSRF được phát hiện vào đầu tháng 2/2020 và được gắn mã CVE-2020-8417. Đây là một loại mã định danh các lỗ hổng bảo mật được phát hiện trong các sản phẩm công nghệ phổ biến trên thế giới và được cung cấp bởi MITRE - một đơn vị được bảo trợ bởi Cơ quan An ninh nội địa Mỹ.

Để khai thác lỗ hổng này, tin tặc sẽ tạo đường link chứa mã khai thác và lừa người quản trị truy cập đường link đó. Một trong các cách thức mà kẻ xấu sử dụng là thông qua chính các tập tin có nội dung hướng dẫn cách bảo vệ mọi người khỏi virus Corona.

Khi người quản trị truy cập vào đường link này lúc đang đăng nhập vào Wordpress, một tài khoản quản trị xấu sẽ được thêm vào hệ thống quản trị website mà người dùng không được thông báo. Từ đây, tin tặc thực hiện xóa quyền quản trị của nạn nhân, thêm vào đó chúng cũng tiến hành việc thay đổi toàn bộ thông tin website.

Sau khi đã thu được tài khoản này, tin tặc sẽ thực thi mã lệnh từ xa (RCE) qua chức năng chỉnh sửa mã nguồn của Wordpress nhằm chiếm quyền điều khiển máy chủ. Qua đó, tin tặc có thể thực hiện những cuộc tấn công gián điệp đối với các thiết bị và máy chủ thuộc cùng mạng nội bộ với máy chủ bị tấn công. Theo các chuyên gia, Code Snippets trước phiên bản 2.14.0 đều bị ảnh hưởng.

WordPress là một mã nguồn mở bằng ngôn ngữ PHP để hỗ trợ xây dựng và phát triển website. Đây là nền tảng phổ biến vì dễ sử dụng, nhiều tính năng hữu ích mà nổi bật là Code Snippets - tính năng mở rộng rất tiện ích trên Wordpress giúp chèn

trực tiếp các đoạn mã vào các tập tin giao diện. Hiện nay, trên thế giới, ước tính có hơn 60% website sử dụng CMS là Wordpress. Trong đó có khoảng 200.000 website cài đặt Code Snippets.

Khuyến nghị: Người quản trị và người dùng cần kiểm tra trước khi truy cập những đường link lạ. Bên cạnh đó, cần cập nhật ngay phiên bản plugin Code Snippets mới nhất để khắc phục lỗ hổng này.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/chiem-quyen-dieu-khien-web-bang-ma-doc-nguy-trang-thong-tin-virus-corona-615569.html

3. Lỗ hổng trên Dell SupportAssist cho phép thực thi mã với các đặc quyền cao

Một nhà nghiên cứu đã phát hiện ra một lỗ hổng DLL hijacking trong Dell SupportAssist, cho phép thực thi mã với các đặc quyền cao. Khai thác lỗ hổng chỉ yêu cầu quyền thấp.

Dell đã tiết lộ rằng, Dell SupportAssist cho PC doanh nghiệp và gia đình đều bị ảnh hưởng bởi lỗ hổng đường dẫn tìm kiếm không được kiểm soát, cho phép người dùng có đặc quyền thấp thực thi mã tùy ý với quyền nâng cao bằng cách tác động để các tệp nhị phân SupportAssist tải các tệp DLL tùy ý.

Lỗ hổng CVE-2020-5316 được đánh giá ở mức độ nghiêm trọng cao, đã được Dell phát hành bản vá SupportAssist cho PC doanh nghiệp phiên bản 2.1.4 và SupportAssist cho PC gia đình phiên bản 3.4.1.

Eran Shimony – nhà nghiên cứu phát hiện ra lỗ hổng bảo mật này – cho biết Dell mất 3 tháng để phát hành các bản vá, nhanh hơn so với thời gian vá hầu hết các lỗ hổng khác mà ông đã báo cáo với Dell.

Những loại lỗ hổng này có thể mang lại giá trị đối với các kẻ tấn công bởi phần mềm này đã được cài đặt sẵn trên hàng triệu PC Dell. Mục đích của Dell SupportAssist là cho phép người dùng kiểm tra tình trạng thiết bị. Việc kiểm tra phần mềm và phần cứng được thực hiện bởi công cụ yêu cầu các đặc quyền nâng cao, bởi vậy một số thành phần của chúng phải chạy với đặc quyền hệ thống.

Một số lỗ hổng leo thang đặc quyền đã được tìm thấy trong Dell SupportAssist trong vài năm qua, nhưng các lỗ hổng liên quan đến DLL hijacking có thể yêu cầu các đặc quyền nâng cao để khai thác, và các nhà cung cấp phần mềm thường nói rằng chúng có rủi ro thấp.

DLL hijacking liên quan đến việc đưa tệp DLL độc hại vào một vị trí trên hệ thống, từ đó ứng dụng mục tiêu sẽ tải tệp độc hại trước các thành phần hợp pháp.

Nếu một ứng dụng không tìm thấy tệp DLL trong thư mục hiện tại hoặc các thư mục hệ thống, nó sẽ cố gắng xác định vị trí tệp trong biến môi trường của hệ thống PATH. Kẻ tấn công với đặc quyền quản trị có thể viết đường dẫn riêng tới biến này, do đó đảm bảo rằng tệp sẽ được tải khi phần mềm mục tiêu được thực thi.

Với trường hợp lỗ hổng CVE-2020-5316, Shimony đã phát hiện ra Dell SupportAssist cố tải DLL từ thư mục mà ngay cả người dùng có đặc quyền không phải quản trị viên cũng có thể sao chép tệp.

Do vậy, hacker, dưới vai trò là một người dùng có đặc quyền thấp, có thể tạo một DLL và lừa để Dell SupportAssist tải DLL này, từ đó giành quyền thực thi mã bên trong phần mềm chạy với các đặc quyền NT AUTHORITY\System. "Điều này xảy ra bởi bạn có thể viết một code entry trong hàm DLLMain (DLL độc hại). Đoạn mã này sẽ chạy ở cấp đặc quyền của NT AUTHORITY\System', Dell cho biết.

Khuyến nghị: Người dùng sản phẩm Dell cần cập nhật phiên bản mới nhất của SupportAssist để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/lo-hong-tren-dell-supportassist-cho-phep-thuc-thi-ma-voi-cac-dac-quyen-cao.13226/

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	Wordpress	CVE 2013 2009 CVE 2015 2062 CVE 2015 1394 …	Nhóm 10 lỗ hổng trên phần mềm Wordpress (Strong Testimonials plugin,...) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công XSS, tấn công CSRF.	Đã có thông tin xác nhận và bản vá.
2	Qualcomm	CVE 2019 14051 CVE 2019 14046 CVE 2019 14044 …	Nhóm 16 lỗ hổng trên thiết bị Qualcomm (Snapdragon Industrial IOT in MDM9206, MDM9607, Snapdragon Auto, Snapdragon Compute…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, làm tràn bộ đệm. 01 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
3	Cisco	CVE 2020 3111 CVE 2020 3110 CVE 2013 2683 …	Nhóm 19 lỗ hổng trên sản phẩm của Cisco (Cisco Discovery Protocol, Cisco Linksys E4200 1.0.05 Build 7,…) cho phép đối tượng tấn công tấn công chèn và thực thi mã tùy ý, truy cập trái phép vào hệ thống với quyền root, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
4	Apache	CVE 2019 12426	01 lỗ hổng trên phần mềm Apache (Apache OFBiz) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
5	D-link	CVE 2013 7055 CVE 2013 7052 CVE 2013 7051 …	Nhóm 06 lỗ hổng trên sản phẩm của D link (D Link DIR 100 4.03B07, DIR865L v1.03…) cho phép đối tượng tấn công thu thập thông tin, thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá

6	Gitlab	CVE 2020 7978 CVE 2020 7966 CVE 2020 7968 …	Nhóm 14 lỗ hổng trên một số thành phần của Gitlab (GitLab EE 12.4, GitLab EE 10.1, GitLab EE 8.0, GitLab EE 12.6…) cho phép đối tượng tấn công thu thập thông tin, tấn công XSS, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
7	Android	CVE 2019 11516 CVE 2014 7224	Nhóm 02 lỗ hổng trên hệ điều hành Android (Android prior to 4.4.0) cho phép đối tượng tấn công chèn và thực thi mã từ xa.	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	xjpakmdcfuqe.biz
5	www.cityofangelsmagazine.com
6	amnsreiuojy.ru
7	xjpakmdcfuqe.biz
8	ydbnsrt.me
9	somicrososoft.ru
10	cp.yvgp6yj6.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.