BẢN TIN NỘI BỘ

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

1. Nhân viên sơ suất mật khẩu khiến dữ liệu bị rò rỉ suốt hai năm

Cụ thể, tài khoản của một quản trị viên đã bị xâm phạm do không thay đổi mật khẩu trong suốt hai năm, tạo điều kiện cho tin tặc xâm nhập hệ thống và một số máy trạm, thiết lập cửa hậu và thu thập dữ liệu của hệ thống.

Nhóm ứng phó sự cố của Kaspersky đã theo dõi, nghiên cứu và chặn đứng cuộc tấn công mạng nhắm vào một tổ chức khách hàng. Cuộc tấn công diễn ra từ năm 2017 - 2019, gây ra vụ rò rỉ dữ liệu lớn.

Theo các chuyên gia của Kaspersky, dù là doanh nghiệp lớn hay nhỏ đều có nguy cơ bị tấn công mạng bất kể việc sở hữu năng lực công nghệ hiện đại hay trình độ đội ngũ chuyên gia bảo mật thông tin chất lượng cao. Lý do của các cuộc tấn công mạng đơn giản xuất phát từ chính yếu tố con người.

Sự cố vừa được xử lý bởi các chuyên gia Kaspersky một lần nữa chứng minh rằng sự thiếu trách nhiệm cơ bản từ nhân viên cũng có thể dẫn đến một cuộc tấn công mạng, gây thiệt hại đáng kể cho tổ chức.

Một doanh nghiệp lớn đã tìm đến các nhà nghiên cứu của Kaspersky sau khi phát hiện những quy trình đáng ngờ trong hệ thống mạng công ty. Nghiên cứu sau đó phát hiện ra rằng hệ thống đã bị xâm nhập thông qua tài khoản quản trị viên cục bộ (adm_Ivan), được sử dụng để tải một tập tin độc hại.

Các tập tin được tải bao gồm một thư viện mã độc cũng như các trình tải xuống và một cửa hậu. Các mã độc này bị ẩn trong hệ thống thông qua biến thể của các phím tắt trên màn hình nền, menu và thanh tác vụ. Sau đó, thông qua việc nhấp vào phím tắt, một tệp độc hại sẽ khởi chạy trước tệp thực thi ban đầu của ứng dụng, cho phép tin tặc che giấu hoạt động đáng ngờ trước sự giám sát của các hệ thống bảo mật.

Cách thức sử dụng cửa hậu để cấp quyền truy cập đầy đủ vào hệ thống đã thu hút sự quan tâm đặc biệt từ các nhà nghiên cứu. Phân tích sâu hơn cho thấy tin tặc đã xây dựng nhiều lệnh khác nhau và tìm kiếm các tệp bằng cách sử dụng từ khóa và tiện ích mở rộng. Tin tặc cũng theo dõi dữ liệu từ các tệp đã tải xuống trước đó.

Đáng chú ý cửa hậu được thiết kế riêng cho cuộc tấn công này và không ghi nhận trường hợp tương tự trong hơn một năm qua. Phân tích bổ sung cũng cho phép tổ chức tìm hiểu cách các hệ thống bị xâm phạm và các phím tắt được biến đổi thành tệp độc hại.

Trong thời gian dài, tin tặc đã xâm phạm có chọn lọc những hệ thống liên quan, thu thập dữ liệu và sau đó xóa dấu vết. Đây là một quá trình mà tổ chức cùng với các nhà nghiên cứu đang theo dõi và kiểm soát. Tuy nhiên, tin tặc đã quyết định lây nhiễm tất cả các hệ thống trên hệ thống mạng nhằm thu được một điểm truy cập thay thế. Hành động này đã khiến tổ chức phải chặn ngay cuộc tấn công đang diễn ra.

Ông Pavel Kargapoltsev, chuyên gia bảo mật của Kaspersky cho biết: “Cuộc tấn công này đã chứng minh rằng sự hợp tác trong ngành bảo mật là cực kỳ quan trọng, giúp thu thập được những thông tin có giá trị, ngăn chặn những cuộc tấn công

tương tự trong tương lai và tiếp tục cuộc chiến chống tội phạm mạng hiệu quả hơn. Khi tin tặc ngày càng sáng tạo hơn trong chiến thuật và kỹ thuật tấn công, chúng tôi cần mở rộng phạm vi hợp tác để phát hiện các mối đe dọa ngay từ giai đoạn đầu, cũng như bảo vệ người dùng và tổ chức hiệu quả hơn."

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị và người dùng cần tuân thủ các quy định về đổi mật khẩu để đảm bảo an toàn thông tin.

Link tham khảo: http://antoanthongtin.vn/hacker-malware/nhan-vien-so-suat-mat-khau-khien-du-lieu-bi-ro-ri-suot-hai-nam-105812

2. Bộ An ninh Nội địa Mỹ đưa cảnh báo nguy cơ từ trình duyệt Windows

Lỗ hổng zero-day của trình duyệt IE trong Microsoft tiềm ẩn nguy cơ khôn lường khiến Bộ An ninh Nội địa Mỹ phải đưa ra cảnh báo mất an toàn.

Trong bản tin tuần này, Cơ quan An ninh Hạ tầng và An ninh mạng (CISA) thuộc Bộ An ninh Nội địa Mỹ cảnh báo kẻ tấn công có thể kiểm soát thiết bị Windows qua lỗ hổng chưa được vá trong trình duyệt IE.

Thực tế, IE không còn là trình duyệt mặc định trong Windows và bị thay thế bởi Microsoft Edge. Tuy nhiên, việc nó được tích hợp sẵn trong hệ điều hành sẽ gây nguy hiểm cho người dùng.

CISA nói kẻ xấu có thể khai thác lỗ hổng này từ xa và thực tế tin tặc đã nhiều lần tấn công nạn nhân qua con đường này.

CISA khuyến cáo người dùng chuyển sang trình duyệt khác trong lúc chờ Microsoft phát hành miếng vá.

Cũng cần biết rằng ngay cả khi sử dụng trình duyệt khác, máy tính Windows vẫn tiềm ẩn nguy cơ vì có nhiều ứng dụng được phát triển trên lõi IE.

Microsoft đã biết lỗ hổng này nhưng chưa thể phát triển bản vá lỗi đầy đủ. Hãng này không cho biết khi nào sẽ có miếng vá bảo mật như vậy. Tuy nhiên, nhiều khả năng nó sẽ được phát hành vào ngày 11/2 tới đây.

Khuyến nghị: Người dùng sử dụng các trình duyệt khác và cập nhật bản vá mới nhất của IE khi Microsoft phát hành để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/bo-an-ninh-noi-dia-my-dua-canh-bao-nguy-co-tu-trinh-duyet-windows-611004.html

3. Israel ra mắt mạng xã hội an ninh mạng đầu tiên trên thế giới

Mạng xã hội đang có tác động ngày càng sâu rộng đối với mọi mặt của đời sống, trong đó có cả lĩnh vực bảo mật - an ninh mạng. Tổng cục Điện tử Quốc gia Israel (INCD) mới đây đã cho ra mắt nền tảng mạng xã hội an ninh mạng đầu tiên trên thế giới, được thiết kế để tạo điều kiện cho các chuyên gia bảo mật, nhân viên IT và cả người dùng phổ thông dễ dàng chia sẻ thông tin liên quan đến các cuộc tấn công mạng, nâng cao kiến thức bảo mật cũng như kêu gọi sự hộ trợ nhằm bảo vệ các công ty, tổ chức, cá nhân trước bất kỳ tác nhân độc hại nào.

"Cybernet là "mạng xã hội an ninh mạng đầu tiên trên thế giới", là nơi chia sẻ các báo cáo tấn công mạng một cách an toàn và đáng tin cậy để đối phó với mọi mối đe dọa từ khi chúng manh nha xuất hiện", đại diện INCD cho biết.

Cybernet được phát triển từ sự phối hợp giữa INCD với các công ty và tổ chức hàng đầu của Israel, cũng như cộng đồng mạng trong nước và quốc tế. Dù mới ra mắt nhưng nền tảng mạng xã hội này hiện có sự góp mặt của hơn 1.000 chuyên gia an ninh mạng, các nhà phân tích, nhà nghiên cứu và quản lý bảo mật thông tin. Nó được xây dựng giống như một mạng xã hội bình thường, nơi mỗi người dùng đều sở hữu một hồ sơ cá nhân "chính chủ" và có thể đăng thông tin, thậm chí ẩn danh.

Người dùng cũng có thể nhận thông tin nhanh về các cuộc tấn công mạng đã và đang diễn ra gần mình và ở Israel nói chung. Thông tin được chia sẻ cũng giúp các thành viên kiểm tra xem liệu cuộc tấn công có thể ảnh hưởng đến tổ chức của họ hay không, và cần làm gì để ngăn chặn nó càng sớm càng tốt.

Ngoài ra Cybernet cũng cho phép người dùng truy cập vào các báo cáo và cảnh báo, nhận thông tin cập nhật về các sự kiện bảo mật lớn trên thế giới, tham dự các nhóm thảo luận và trò chuyện nội bộ, xem báo cáo xử lý vi phạm an ninh mạng của tổ chức và hơn thế nữa. Những báo cáo bảo mật quan trọng sẽ được chuyển đến trung tâm ứng phó sự cố máy tính khẩn cấp của INCD, và từ đó được gửi đến các công ty liên quan.

Với hiện trạng tình hình an ninh mạng toàn cầu đang có những diễn biến ngày càng phức tạp, những nền tảng như Cybernet sẽ đóng vai trò cực kỳ hữu dụng, cần được nhân rộng trên toàn thế giới.

Link tham khảo: https://quantrimang.com/israel-ra-mat-mang-xa-hoi-an-ninh-mang-dau-tien-tren-the-gioi-169233

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	Cisco	CVE 2019 15979 CVE 2019 15984 CVE 2019 15975 …	Nhóm 13 lỗ hổng trên một số thành phần, sản phẩm của Cisco (Cisco Data Center Network Manager,...) cho phép đối tượng tấn công chèn và thực thi mã từ xa. 10 lỗ hổng có điểm CVSS đặc biệt nghiêm trọng (9.0, 10.0)	Đã có thông tin xác nhận và bản vá.
2	Android	CVE 2019 9468 CVE 2020 0002 CVE 2019 9469 …	Nhóm 15 lỗ hổng trên hệ điều hành Android (Android kernel Android ID: A 144168326, Android 9,…) cho phép đối tượng tấn công tấn công chèn và thực thi mã tùy ý. 01 lỗ hổng có điểm CVSS nghiêm trọng 9,3	Đã có thông tin xác nhận và bản vá
3	Wordpress	CVE 2019 20361 CVE 2019 20360 CVE 2020 6166 …	Nhóm 14 lỗ hổng trên một số thành phần của phần mềm Wordpress (Minimal Coming Soon & maintenance, WordPress plugin,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
4	Gitlab	CVE 2019 19088 CVE 2019 19628 CVE 2019 19260 …	Nhóm 21 lỗ hổng trên một số thành phần của Gitlab (Gitlab Enterprise Edition, Community and Enterprise Edition,...) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
5	Chrome	CVE 2019 13765 CVE 2019 5844 CVE 2019 13766 …	Nhóm 07 lỗ hổng trên hệ điều hành Chrome (trước version 73.0.3683.75) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
6	Samsung	CVE 2012 3810 CVE 2012 3808	Nhóm 04 lỗ hổng trên sản phẩm của Samsung (Samsung	Đã có thông tin

		CVE 2012 3806	Kies) cho phép đối tượng tấn công thực thi mã tùy ý, tấn công từ chối dịch vụ.	xác nhận và bản vá
7	Linux	CVE 2019 19332	01 lỗ hổng trên hệ điều hành Linux (Linux kernel) cho phép đối tượng tấn công có thể tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
8	Apache	CVE 2019 20343 CVE 2020 1925	Nhóm 02 lỗ hổng trên phần mềm Apache (Apache Olingo, MojoHaus Exec Maven) cho phép đối tượng tấn công thực thi mã tùy ý.	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	xjpakmdcfuqe.biz
5	xjpakmdcfuqe.com
6	and30.blabladomdom.com
7	xjpakmdcfuqe.in
8	amnsreiuojy.ru
9	ovrz52z140.ru
10	hzmksreiuojy.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.