BẢN TIN NỘI BỘ

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

1. Microsoft gấp rút tung ra cập nhật bảo mật cho Windows XP, Server 2003

Nếu bạn vẫn đang sử dụng bản sao Windows XP hoặc Windows Server 2003 trên các hệ thống được kết nối mạng (và cả Windows 7, Windows Server 2008 và 2008 R2), hãy chú ý! Microsoft sẽ đưa ra một bản vá khẩn cấp cho các hệ điều hành nêu trên nhằm ngăn chặn một lỗ hổng có thể tạo điều kiện cho kẻ gian exploit hệ thống từ xa thông qua dịch vụ RDP, hoàn toàn có thể dẫn đến một kịch bản tồi tệ như Wannacry 2 năm trước.

Lỗ hổng này hiện có định danh CVE-2019-0708. Phương thức exploit lỗ hổng khá đơn giản, kẻ tấn công sẽ chỉ cần gửi một yêu cầu được tạo đặc biệt tới các hệ thống mục tiêu Remote Desktop Service thông qua RDP, qua đó thực thi mã từ xa trên hệ thống. Nguy hiểm hơn, quá trình exploit có thể lan truyền từ máy tính này sang máy tính khác một cách nhanh chóng, từ đó khiến toàn bộ hệ thống sụp đổ bởi nó có thể lây lan mà không cần sự can thiệp của người dùng.

Trong một báo cáo mới nhất, Microsoft lưu ý rằng vấn đề không nằm ở giao thức RDP mà là do chính dịch vụ này:

"Bản thân Remote Desktop Protocol (RDP) hoàn toàn không dễ bị tấn công. Chúng tôi nhận định rằng lỗ hổng này là một dạng xác thực trước và không yêu cầu tương tác người dùng. Nói cách khác, lỗ hổng bảo mật này có thể xếp vào loại "wormable", nghĩa là mọi phần mềm độc hại trong tương lai đều có thể khai thác này và lan truyền từ máy tính này sang máy tính khác theo cách tương tự như cái cách mà phần mềm độc hại WannaCry lan rộng trên toàn cầu vào năm 2017 trước kia".

May mắn thay, lỗ hổng này hoàn toàn không ảnh hưởng đến Windows 8.1 hoặc Windows 10. Tuy nhiên để bảo đảm an toàn, chắc chắn Microsoft sẽ tung ra một bản cập nhật bảo mật bổ sung cho 2 hệ điều hành trên.

Quay trở lại với trường hợp của những hệ điều hành cũ hơn đã nêu ở đầu bài viết, bạn có thể tìm bản vá cho Windows XP và Windows Server 2003 tại đây. Các hệ điều hành khác đang được vá thông qua chu kỳ Patch Tuesday thông thường.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng sử dụng hệ điều hành Windows XP và Windows Server 2003 cần cập nhật ngay các bản vá nêu trên, ngoài ra cần sớm nâng cấp hệ điều hành mới có cập nhật bản quyền và hỗ trợ từ nhà cung cấp để đảm bảo an toàn thông tin.

Link tham khảo: https://quantrimang.com/cap-nhat-bao-mat-cho-windows-xp-server-2003-163731

2. Phát hiện biến thể mới của mã độc tống tiền Dharma

Kể từ khi được phát hiện lần đầu vào năm 2016, mã độc Dharma đã không ngừng phát triển và liên tục "đòi tiền chuộc" từ người dùng internet trên toàn thế giới. Hiện tại, mã độc này đang có biến thể nguy hiểm mới.

Các chuyên gia bảo mật của Trend Micro đã phát hiện hình thái tấn công mới từ loại mã độc này: ngụy trang như một phần mềm an toàn để người dùng tải về máy, sau đó mới phát tán mã độc tống tiền. Cụ thể, mã độc sử dụng giao diện cài đặt của phần mềm diệt virus ESET, đây được xem như là cách "tung hỏa mù" của mã độc khiến nạn nhân mất cảnh giác.

Mã độc được các tin tặc phân tán trên mạng thông qua hình thức spam email có đính kèm Dharma lưu trữ dưới dạng nhị phân, mỗi email kèm theo mật khẩu riêng, trong đó sẽ có định dạng file là Defender.exe và có máy chủ đặt tại server của hacker link[.]fivetier[.]com.

Mật khẩu để mở tập độc hại đính kèm trong email spam cộng thêm cách tiếp cận được thiết kế khiến nạn nhân tò mò mở file và vô tình điều đó đã làm lây nhiễm mã độc Dharma trên máy của họ.

Mỗi khi file Defender.exe được nạn nhân bấm vào, nó sẽ hiển thị bằng giao diện cài đặt cũ của phần mềm diệt virus ESET dưới tên là Defender_nt32_othy.exe , và song song là một file taskhost.exe được thêm vào C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\ - đây chính là lúc Dharma khởi chạy và bắt đầu tiến trình mã hóa dữ liệu của nạn nhân cho mục đích tống tiền.

Phần mềm diệt virus ESET do mã độc Dharma ngụy trang sẽ tiến cài hành cài đặt tự động khi được kích hoạt trong thư mục đã giải nén, trong lúc sự chú ý tập trung vào việc cài đặt thì mã độc Dharma sẽ mã hóa các nội dung một cách âm thầm mà nạn nhân không hề hay biết.

Theo như báo cáo từ các chuyên gia bảo mật Trend Micro về mã độc Dharma, "Các mã độc này vẫn sẽ mã hóa file dữ liệu thậm chí không cần phải bắt đầu tiến trình cài đặt, mã độc gây hại này chạy trên một phiên bản khác với cài đặt phần mềm, vì vậy chúng gần như chẳng liên quan gì nhau".

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng không mở, cài đặt các chương trình lạ được gửi kèm mật khẩu hoặc làm giả giao diện của chương trình diệt Virus ESET như trên. Không click vào những email không rõ nguồn gốc hoặc có vẻ đáng nghi ngờ, thường xuyên sao lưu các dữ liệu trên máy tính, luôn cập nhật phần mềm diệt virus phiên bản mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/phat-hien-bien-the-moi-cua-ma-doc-tong-tien-dharma-1081939.html

3. Phát hiện phương thức lừa tiền tinh vi nhắm vào các ứng viên tìm việc

Các chuyên gia của Kaspersky Lab đã phát hiện một loạt email spam tinh vi được gửi đến người dùng, bao gồm thư mời làm việc giả mạo có địa chỉ người nhận đến từ những tập đoàn lớn, và do đó thu hút rất nhiều sự quan tâm từ các ứng viên tiềm năng.

Tuy nhiên, trên thực tế, những email này lại đến từ những kẻ lừa đảo với mục đích cài đặt phần mềm độc hại lên thiết bị của người dùng.

Mối đe dọa từ email rác thường bị đánh giá thấp, tuy nhiên chúng có thể phát tán phần mềm độc hại dựa vào sự tương tác với con người như lừa dối hoặc thao túng tâm lý người dùng.

Báo cáo Spam and Phishing Q1 2019 của Kaspersky Lab cho thấy, người nhận email spam đã được mời làm những vị trí hấp dẫn trong các công ty lớn.

Họ được mời tham gia hệ thống tìm kiếm việc làm miễn phí bằng cách cài đặt ứng dụng đặc biệt vào thiết bị của họ. Để quá trình cài đặt trông đáng tin cậy hơn, những kẻ tấn công đã thêm một cửa sổ mang dòng chữ "Bảo vệ khỏi Tấn công từ chối dịch vụ DDoS (DDoS Protection)" và một tin nhắn giả thông báo người dùng đang được chuyển hướng đến trang web của một trong những công ty tuyển dụng lớn nhất.

Trên thực tế, các nạn nhân đã được chuyển hướng đến một trang lưu trữ đám mây, từ đây họ sẽ tải xuống chương trình độc hại trông giống như một file word. Chức năng của nó là tải về máy nạn nhân Trojan ngân hàng khét tiếng có tên Gozi - một trong những phần mềm độc hại được sử dụng phổ biến nhất để đánh cắp tiền. Kaspersky Lab phát hiện ra nó chính là Trojan-Banker.Win32.Gozi.bqr

Để tránh trở thành nạn nhân của thư rác độc hại, Kaspersky khuyến cáo người dùng nên kiểm tra địa chỉ web bạn được chuyển hướng đến, hoặc địa chỉ liên kết và email của người gửi trước khi nhấp vào, và đảm bảo rằng liên kết đó không bị ẩn (hyperlink) bằng một liên kết khác.

Tuyệt đối 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. Hãy chắc chắn rằng chúng hợp pháp và bắt đầu với "https" khi bạn được yêu cầu cung cấp bất kỳ thông tin cá nhân hoặc tài chính nào.

Nếu không chắc chắn rằng trang web hiện tại là có thật và an toàn, tuyệt đối nhập thông tin cá nhân của bạn.

Ngoài ra, người dùng nên kiểm tra trang web chính thức của công ty về các vị trí đang tuyển dụng và gọi điện thoại để đảm bảo rằng bạn đã nhận lời mời chính thức từ công ty. Xem xét cẩn thận lời mời nhận việc của bạn: kiểm tra kỹ tên công ty, chức danh và mô tả công việc.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng không click 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 nghị ngờ, luôn kiểm tra địa chỉ web bạn được chuyển hướng đến để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/phat-hien-phuong-thuc-lua-tien-tinh-vi-nham-vao-cac-ung-vien-tim-viec-532389.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-2018-1990 CVE-2018-2001 CVE-2018-1790 CVE-2018-2008 CVE-2019-4208 ...	Nhóm 09 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	Cisco	CVE-2018-15388 CVE-2019-1687 CVE-2019-1694 CVE-2019-1697 CVE-2019-1706 …..	Nhóm 43 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.	Đã có thông tin xác nhận và bản vá
3	Linux	CVE-2019-9791 CVE-2019-9792 CVE-2019-9794 CVE-2019-9795 ……..	Nhóm 07 lỗ hổng dựa trên một số sản phẩm của Mozilla (Thunderbird…) cho phép kẻ tấn công có quyền truy cập và thực thi vào hệ thống qua nhiều giao thức khác nhau gây ra thiếu dữ liệu.	Đã có thông tin xác nhận và bản vá.
4	Qualcomm	CVE-2017-18279 CVE-2017-18156 CVE-2017-18157 CVE-2017-18274 ……	Nhóm 10 lỗ hổng trên một số sản phẩm của Qualcomm (SmallCell SoC, Snapdragon Mobile, Snapdragon Wea) lỗi thiếu sự kiểm tra độ dài bộ đệm khi copy có thể gây tràn bộ đệm.	Đã có thông tin xác nhận và bản vá.
5	Google	CVE-2018-6243 CVE-2019-2044 CVE-2019-2045 CVE-2019-2046 …….	Nhóm 12 lỗ hổng trên 1 số sản phẩm của Google lỗi thiếu sự kiểm tra tham số lượng tham số đầu vào, gây ra từ chối dịch vụ, tràn bộ nhớ	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	43trfdsds.com
2	strikotunrev.top
3	d3s1.me
4	io90s8dudi.xyz
5	tesivisi11.top
6	laopre.at
7	babushkabenmen.net
8	strikotunrev.top
9	dnshkjashsdk3d11144d.ru
10	pupuiolili.top

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.