BẢN TIN NỘI BỘ

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

1. 50000 máy chủ MS-SQL và PHPMYADMIN bị lây nhiễm mã độc Rootkit

Các nhà nghiên cứu an ninh mạng tại Guardicore Labs hôm nay đã công bố một báo cáo chi tiết về chiến dịch tấn công mã hóa các máy chủ Windows MS-SQL và PHPMyAdmin trên toàn thế giới.

Chiến dịch này được gọi với cái tên Nansh0u, cuộc tấn công bằng mã độc này được cho là do nhóm hacker APT-style đến từ Trung Quốc thực hiện. 50000 máy chủ đã lây nhiễm và bị cài đặt vào nhân Kernel một loại mã độc rootkit

Chiến dịch bắt đầu vào 26 tháng 2. Nhưng đến tháng 4 mới phát hiện bản đầu tiên. Cùng với đó là khoảng 20 phiên bản khác nhau của mã độc này được lưu trữ trên các máy chủ cung cấp dịch vụ lưu trữ

Tấn công Brute-forcing này có thể truy cập công khai vào các máy chủ MS-SQL, PHPMyAdmin bằng 1 trình quét cổng đơn giản.

Sau khi chiếm quyền quản trị, attacker sẽ thực thi một chuỗi các câu lệnh MS-SQL trên hệ thống và tải về mã độc từ máy chủ lưu trữ từ xa và chạy nó với các đặc quyền cao nhất của hệ thống.

Sau khi thâm nhập hệ thống, tận dụng lỗ hổng leo thang đặc quyền CVE-2014-4113 để có được các đặc quyền cao nhất của hệ thống.

“Sử dụng đặc quyền Windows này sẽ cái đặt mã độc vào quy trình Winlogon. Mã độc sẽ tạo thành 1 quy trình mới kế thừa các đặc quyền của hệ thống Winlogon, cung cấp các đặc quyền tương đương”

Cổng PAYLOAD sau đó cài đặt một mã độc khai thác tiền điện tử trên các máy chủ bị xâm nhập để khai thác tiền điện tử TurtleCoin

Bên cạnh đó, mã độc cũng tự bảo vệ quá trình của nó khỏi bị chấm dứt bằng cách sử dụng rootkit chế độ nhân, được kí điện tử để duy trì - “chúng tôi tìm thấy trong trình điều khiển có chứng chỉ được cấp bởi công ty công nghệ Hàng Châu Hootian”

Các nhà nghiên cứu cũng đã cung cấp 1 danh sách đầy đủ các tập lệnh dựa trên PowerShell miễn phí mà nhờ vào đó các quản trị viên có thể sử dụng để kiểm tra xem hệ thống của mình có bị nhiễm mã độc này ko.

Vì cuộc tấn công lợi dụng cơ chế mật khẩu yếu của MS-SQL và PHPMyAdmin nên các quản trị viên được khuyến cáo nâng cao độ mạnh và sự phức tạp cho mật khẩu của họ.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị cần đề cao cảnh giác, đặt mật khẩu mạnh và đổi mật khẩu theo định kỳ để đảm bảo an toàn thông tin. Kiểm tra các tập lệnh PowerShell để kiểm tra việc lây nhiễm.

Link tham khảo: https://securitybox.vn/7805/50000-may-chu-ms-sql-va-phpmyadmin-bi-lay-nhiem-ma-doc-rootkit/

2. Windows tồn tại lỗi cho phép vượt qua màn hình khóa trong các phiên Remote Desktop

Chi tiết về lỗ hổng mới chưa được vá trong Microsoft Windows Remote Desktop Protocol (RDP) vừa được công bố. Lỗ hổng này, CVE-2019-9510, có thể cho phép kẻ tấn công phía máy khách vượt qua màn hình khóa trong các phiên remote desktop (RD).

Được phát hiện bởi Joe Tammariello của Đại học Carnegie Mellon (SEI), lỗ hổng tồn tại khi tính năng Microsoft Windows Remote Desktop yêu cầu máy khách xác thực bằng Network Level Authentication (NLA), một tính năng mà gần đây Microsoft đề xuất để chống lại lỗ hổng BlueKeep RDP.

Theo Will Dormann, một nhà phân tích lỗ hổng tại CERT/CC, nếu một sự cố mạng kích hoạt ngắt kết nối RDP tạm thời trong khi máy khách đã được kết nối với máy chủ nhưng màn hình đăng nhập bị khóa, thì "khi kết nối lại, phiên RDP sẽ khôi phục trạng thái mở khóa, bất kể hệ thống từ xa như thế nào".

CERT mô tả kịch bản tấn công như sau:

• Người dùng mục tiêu kết nối với hệ thống Windows 10 hoặc Server 2019 thông qua RDS.

• Người dùng khóa phiên làm việc từ xa và không chú ý đến thiết bị nữa.

• Tại thời điểm này, kẻ tấn công có quyền truy cập vào thiết bị máy khách có thể làm gián đoạn kết nối mạng và có quyền truy cập vào hệ thống từ xa mà không cần bất kỳ thông tin xác thực.

Điều này có nghĩa là việc khai thác rất đơn giản, vì kẻ tấn công chỉ cần làm gián đoạn kết nối mạng của hệ thống mục tiêu.

Tuy nhiên, vì kẻ tấn công cần có truy cập vật lý vào một hệ thống mục tiêu như vậy (tức là, một phiên hoạt động với màn hình bị khóa), bản thân kịch bản hạn chế khả năng tấn công ở mức độ lớn hơn.

Tammariello đã thông báo cho Microsoft về lỗ hổng này vào ngày 19 tháng 4, nhưng được phản hồi rằng "hành vi không đáp ứng tiêu chí về an ninh của Microsoft", có nghĩa là gã khổng lồ công nghệ không có kế hoạch khắc phục sự cố.

Tuy nhiên, người dùng có thể tự bảo vệ mình trước khả năng bị khai thác qua lỗ hổng này bằng cách khóa hệ thống cục bộ thay vì hệ thống từ xa và ngắt kết nối các phiên remote desktop thay vì chỉ khóa chúng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị viên cần tắt chức năng Remote Desktop trên các hệ điều hành để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/windows-ton-tai-loi-cho-phep-vuot-qua-man-hinh-khoa-trong-cac-phien-remote-desktop.12333/

3. Cảnh báo việc đặt mật khẩu "có cũng như không" của điện thoại

Dù bạn có tin hay không, "1234" và "0000" là 2 trong số những mật khẩu điện thoại "tệ hại" nhất mà mọi người dùng để bảo vệ cho thiết bị của mình.

Chuyên gia an ninh mạng Tarah Wheeler gần đây đã chia sẻ 1 danh sách những mã PIN phổ biến nhất được người dùng điện thoại di động sử dụng dựa trên dữ liệu mà Học viện SANS - một trong những tổ chức bảo mật lớn nhất thế giới.

Đây là các mật khẩu dễ bị tấn công nhất. Và nếu mật khẩu thiết bị của bạn nằm trong số này, hãy thay đổi ngay lập tức.

Theo Wheeler, có đến 26% các điện thoại di động bị bẻ khóa với các mật khẩu loại này. Như vậy, cứ 4 người dùng thì sẽ có 1 người dễ dàng bị bị hacker bẻ khoá thiết bị:

1234
1111
0000
1212
7777
1004
2000
4444
2222
6969
9999
3333
5555
6666
1122
1313
8888
4321
2001
1010

Tốt hơn hết bạn nên đổi sang sử dụng mật khẩu 6 số thay vì chỉ 4 số hoặc các phương thức bảo mật sinh trắc học như Face ID hoặc Touch ID sẽ an toàn hơn.

Cách đổi mật khẩu trên thiết bị di động

Thiết bị dùng hệ điều hành iOS:

Vào Settings (Cài đặt), rồi vào một trong số các tùy chọn sau, tùy theo model thiết bị: Face ID & Passcode, Touch ID & Passcode, hoặc Passcode. Bật chế độ Passcode On hoặc Change Passcode. Chế độ mật khẩu 6 số dài hơn 4 số sẽ an toàn hơn.

Thiết bị dùng hệ điều hành Android:

Mở Settings (Cài đặt) trên thiết bị, nhấn vào mục Security & location, Security (Bảo mật) hoặc Màn hình khóa hay Sinh trắc học và Bảo mật. Tại đây bạn có thể chọn các hình thức bảo mật khác nhau.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng điện thoại cần đặt mật khẩu mạnh để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/top-20-mat-khau-co-cung-nhu-khong-so-xem-ban-co-nam-trong-so-nay-538910.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	Synacor	CVE-2015-7609 CVE-2018-14013 CVE-2018-14425 CVE-2018-15131 ...	Nhóm 11 lỗ hổng dự trên một số sản phẩm của Synacor (ZxChat, Zimbra, ..) cho phép kẻ tấn công lấy thông tin từ các tài khoản thông qua lỗ hổng XML	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2019-4139 CVE-2019-4184 CVE-2019-4138 CVE-2019-4137 …..	Nhóm 04 lỗ hổng dựa trên một số sản phẩm của IBM (APM API Connect, QRadar SIEM, Cognos Analytics,...) cho phép kẻ tấn công nhúng các đoạn mã JavaScript để lấy thông tin, giải mã (do sử dụng giải thuật mã hóa yếu), thu thập thông tin nhạy cảm.	Đã có thông tin xác nhận và bản vá
3	Qualcomm	CVE-2019-5930 CVE-2019-5931 CVE-2019-5933 CVE-2019-5934 ……..	Nhóm 31 lỗ hổng dựa trên một số sản phẩm của Qualcomm có phép kẻ tấn công truy cập trái phép vào hệ thống gây tràn bộ đệm, lỗi truy cập.	Đã có thông tin xác nhận và bản vá.
4	Linux	CVE-2019-12454 CVE-2019-12456 CVE-2019-12378 ……	Nhóm 09 lỗ hổng trên nhân của Linux cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá.
5	Abobe	CVE-2019-7018 CVE-2019-7019 CVE-2019-7020 CVE-2019-7025 …..	Nhóm 78 lỗ hổng trên một số sản phẩm của Adobe (bridge, flash Player, Acrobat) cho phép khai thác lỗi tràn bộ đệm, lỗ hổng trong việc truyền tải đường dẫn hay xử lý siêu liên kết không an toàn.	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	5fuvz5pe.ru
6	xjpakmdcfuqe.com
7	0juwrq36.ru
8	kukutrustnet777.info
9	plpanaifheaighai.com
10	iri914a7.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.