TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

NCSC VN
National Cyber Security Center

CẢNH BÁO TUẦN

SỐ 09 (28/02/2022 – 06/03/2022)

Thông tin liên hệ: Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 – ais.@mic.gov.vn

Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp.Hà Nội

NỘI DUNG TUẦN

"NỖ LỰC ĐỂ KHÔNG GIAN MẠNG VIỆT NAM LUÔN AN TOÀN, LÀNH MẠNH"

TIN CẢNH BÁO

- **Cảnh báo:** Lỗ hổng bảo mật mới trong Linux Kernel cgroups cho phép đối tượng tấn công leo thang đặc quyền

- **Chiến dịch tấn công APT:** Phần mềm độc hại Daxin được sử dụng trong các cuộc tấn công APT nhằm mục tiêu vào chính phủ nhiều quốc gia

ĐIỂM YẾU, LỖ HỔNG

- **375** lỗ hổng được công bố và cập nhật.

- **07** lỗ hổng, nhóm lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam.

SỐ LIỆU, THỐNG KÊ

- Tấn công DRDoS
- Tấn công Web
- Tấn công lừa đảo người dùng Việt Nam

Hot News!

Tài liệu lưu trữ:

Chuyên mục **Báo cáo định kỳ** tại địa chỉ:

https://service.khonggianmang.vn

TIN CẢNH BÁO

Cảnh báo: Lỗ hổng bảo mật mới trong Linux Kernel cgroups cho phép đối tượng tấn công leo thang đặc quyền

Gần đây, các chuyên gia bảo mật đã phát hiện một lỗ hổng có mức ảnh hưởng Cao trong Linux kernel (đã có bản vá) có khả năng bị khai thác để thoát khỏi container nhằm thực thi các lệnh tùy ý trên container host.

Lỗ hổng CVE-2022-0492 (điểm CVSS: 7,0) cho phép đối tượng tấn công leo thang đặc quyền trong cgroups v1 release_agent, một tập lệnh được thực thi sau khi kết thúc bất kỳ quá trình nào trong cgroup. Lỗi này là hậu quả của việc thiếu xác minh khi kiểm tra đặc quyền quản trị trong quá trình thiết lập tệp release_agent, khiến cho nguy cơ bị khai thác cao.

Thông thường, một lỗ hổng leo thang đặc quyền chỉ có thể được khai thác bởi tài khoản người dùng root, tuy nhiên chạy với quyền root không phải lúc nào cũng có toàn quyền kiểm soát máy: Có một vùng (grey area) giữa người dùng root và các đặc quyền đầy đủ bao gồm các quyền sử dụng, namespaces và containers, trong những trường hợp này, tài khoản root không có toàn quyền kiểm soát máy.

Mặc dù containers chạy với AppArmor hoặc SELinux nên sẽ được bảo vệ khỏi lỗ hổng này, nhưng cơ quan tổ chức được khuyến nghị cài đặt các bản vá vì thực tế nó có thể bị lợi dụng để khai thác bởi các tiến trình độc hại khác trong máy chủ để leo thang đặc quyền.

Nguồn: https://thehackernews.com/2022/03/new-linux-kernel-cgroups-vulnerability.html?m=1

Phần mềm độc hại Daxin được sử dụng trong các cuộc tấn công APT nhằm mục tiêu vào chính phủ nhiều quốc gia

Gần đây, các chuyên gia bảo mật phát hiện một công cụ gián điệp đã được triển khai trong chiến dịch tấn công kéo dài của một nhóm đối tượng tấn công APT của Trung Quốc kể từ năm 2013, nhằm mục tiêu vào chính phủ nhiều quốc gia.

Phần mềm độc hại này có tên là Daxin, cho phép đối tượng tấn công thực hiện nhiều hoạt động độc hại, thu thập thông tin. Daxin là một backdoor rootkit rất tinh vi với chức năng điều khiển và kiểm soát phức tạp. Phần mềm này có thể hoạt động mà không tạo ra lưu lượng truy cập đáng ngờ nào để không bị phát hiện, bên cạnh đó còn có khả năng chuyển tiếp các lệnh qua mạng các máy tính bị nhiễm, từ đó cho phép đối tượng tấn công truy cập định kỳ vào máy tính bị xâm nhập trong thời gian dài.

Theo các nhà nghiên cứu, Daxin là phần mềm độc hại tiên tiến, được sử dụng bởi nhóm tấn công của Trung Quốc. Qua khả năng của nó và bản chất các cuộc tấn công đã triển khai, Daxin dường như được tối ưu hóa để sử dụng chống lại các mục tiêu cao, cho phép tấn công sâu vào hệ thống mạng của mục tiêu và lấy dữ liệu mà không gây nghi ngờ.

Nguồn: https://thehackernews.com/2022/03/china-linked-daxin-malware-targeted.html

Nguy cơ tấn công mạng từ điểm yếu, lỗ hổng

Trong tuần, các tổ chức quốc tế đã công bố và cập nhật ít nhất 375 lỗ hổng, trong đó có 03 lỗ hổng mức cao, 23 lỗ hổng mức trung bình, 06 lỗ hổng mức thấp và 343 lỗ hổng chưa đánh giá. Trong đó có ít nhất 30 lỗ hổng cho phép chèn và thực thi mã lệnh.

Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 07 lỗ hổng/nhóm lỗ hổng trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam: Nhóm 10 lỗ hổng trong Linux kernel, Nhóm 07 lỗ hổng trong sản phẩm của HP, Nhóm 06 lỗ hổng trong sản phẩm của IBM, Nhóm 06 lỗ hổng trong Liferay Portal, Nhóm 05 lỗ hổng trong thiết bị D-Link, Nhóm 04 lỗ hổng trong các sản phẩm của Aruba, Nhóm 04 lỗ hổng trong phần mềm Vmware. Thông tin chi tiết về một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

Một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam:

- Linux: CVE-2022-0492, CVE-2021-3609,...

- HP: CVE-2022-23953, CVE-2022-23958,...

- IBM: CVE-2021-38993, CVE-2021-38955,...

- Liferay: CVE-2021-38265, CVE-2021-38267,...

- D-Link: CVE-2021-46381, CVE-2022-25106,...

- Aruba: CVE-2021-41000, CVE-2021-41001,...

- Vmware: CVE-2022-22947, CVE-2022-22946,...

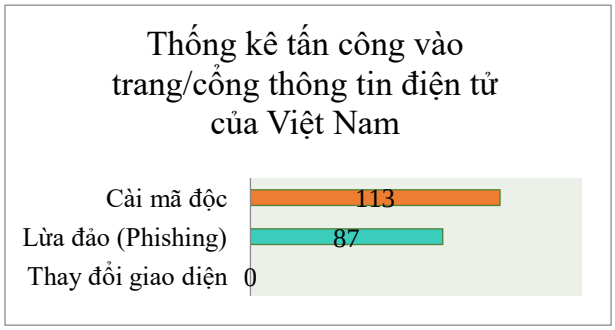
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2022-0492 CVE-2021-3609 CVE-2021-3428 …	Nhóm 10 lỗ hổng trong Linux kernel cho phép đối tượng tấn công leo thang đặc quyền, gây bất thường cho hệ thống, tấn công từ chối dịch vụ, thu thập thông tin.	Đã có thông tin xác nhận và bản vá
2	HP	CVE-2022-23953 CVE-2022-23958 CVE-2022-23957 …	Nhóm 07 lỗ hổng trong sản phẩm của HP (PC) cho phép đối tượng tấn công thực thi mã từ xa, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	IBM	CVE-2021-38993 CVE-2021-38955 CVE-2022-22350 …	Nhóm 06 lỗ hổng trong sản phẩm của IBM (VIOS, AIX,…) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá
4	Liferay	CVE-2021-38265 CVE-2021-38267 CVE-2022-25146 …	Nhóm 06 lỗ hổng trong Liferay Portal cho phép đối tượng tấn công thu thập thông tin, tấn công XSS, CSRF, thực hiện các hành động trái phép, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
5	D-Link	CVE-2021-46381 CVE-2022-25106 CVE-2021-46353 …	Nhóm 05 lỗ hổng trong thiết bị D-Link (DAP-1620, DIR-859,…) cho phép đối tượng tấn công thu thập thông tin, tấn công path traversal, từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá. Một số sản phẩm lỗi thời không được hỗ trợ bản vá
6	Aruba	CVE-2021-41000 CVE-2021-41001 CVE-2021-41003 …	Nhóm 04 lỗ hổng trong các sản phẩm của Aruba (CX 6200F Switch Series,…) cho phép đối tượng tấn công thực thi mã từ xa, tấn công command injection, path traversal.	Đã có thông tin xác nhận và bản vá
7	Vmware	CVE-2022-22947 CVE-2022-22946 CVE-2022-22943 …	Nhóm 04 lỗ hổng trong phần mềm Vmware (spring cloud gateway,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công stored-XSS	Đã có thông tin xác nhận và bản vá

Thống kê nguy cơ, các cuộc tấn công tại Việt Nam

Tấn công DRDoS

Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **74,883** (tăng so với tuần trước **73,335**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), Chargen (19). Dưới đây là biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến trong tuần.

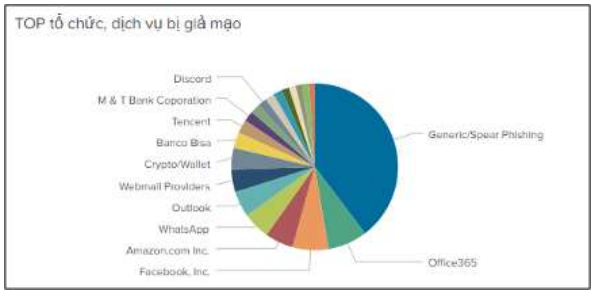


Tấn công Phishing

Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử .v.v… Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và tính phí) như các mạng xã hội, Paypment, Apple, Paypal ..v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để đánh cắp tài khoản.

Tấn công Web

Trong tuần, có 200 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 0 trường hợp tấn công thay đổi giao diện, 87 trường hợp tấn công lừa đảo (Phishing), 113 trường hợp tấn công cài cắm mã độc.



Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

differentia.ru	xjpakmdcfuqe.ru
disorderstatus.ru	xjpakmdcfuqe.in
atomictrivia.ru	amnsreiuojy.ru
xjpakmdcfuqe.biz	bsxqyi.info
xjpakmdcfuqe.com	restlesz.su

New

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 122 phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam thông báo về Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) qua hệ thống tại địa chỉ https://canhbao.khonggianmang.vn. Qua kiểm tra, phân tích có nhiều trường hợp lừa đảo giả mạo website của ngân hàng, lừa đảo liên quan đến COVID…

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	https://tikivip.com	Giả mạo website sàn TMĐT Tiki
2	https://lazadavn.net	Giả mạo website sàn TMĐT Lazada
3	https://vipmomo77.com https://kkoi.me	Web lừa đảo cờ bạc qua ví điện tử Momo

Khuyến nghị đối với các cơ quan, đơn vị

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin cảnh báo** Quý đơn vị cần thường xuyên cập nhật thông tin (như các chiến dịch tấn công của các nhóm APT, thông tin IoC kèm theo từng chiến dịch, điểm yếu lỗ hổng đang bị lợi dụng để khai thác,…), rà soát trên các hệ thống thống thông tin để phát hiện và ngăn chặn, xử lý kịp thời.

***

2. Đối với các điểm yếu, lỗ hổng trong phần **Nguy cơ tấn công mạng từ điểm yếu lỗ hổng**, Quý đơn vị cần lưu ý theo dõi và cập nhật bản vá cho các lỗ hổng liên quan đến sản phẩm đang sử dụng. Ngoài ra, những đơn vị đã có tài khoản trên "Hệ thống Cảnh báo điểm yếu và rà soát lỗ hổng bảo mật tự động" tại địa chỉ https://service.khonggianmang.vn, quản trị viên có thể thêm các sản phẩm đang sử dụng để giám sát và nhận cảnh báo ngay khi có lỗ hổng mới phát sinh.

***

3. Đối với các nguy cơ về tấn công từ chối dịch vụ, tấn công web trong phần **Thống kê nguy cơ, các cuộc tấn công tại Việt Nam**, Quý đơn vị cần rà soát, hạn chế tối đa việc mở các cổng dịch vụ có thể bị lợi dụng để thực hiện tấn công từ chối dịch vụ; thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và xử lý nguy cơ tấn công.

***

4. Đối với các IP/tên miền được đề cập trong mục **Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam**, Quý đơn vị cần kiểm tra và xử lý các thiết bị trong toàn bộ hệ thống mạng nếu có dấu hiệu kết nối đến các tên miền độc hại mà Cục ATTT đã chia sẻ.

***

Thông tin liên hệ:

Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 - ais@mic.gov.vn

Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội