NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 12 (18/03/2024 – 24/03/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Chiến dịch tấn công của nhóm tấn công APT Earth Krahang gây ảnh hưởng tới 70 tổ chức tại 23 quốc gia.

- **Cảnh báo:** Hình thức tấn công LoopDoS đe dọa đến hàng ngàn thiết bị.

2. Điểm yếu, lỗ hổng

- **782** 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.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Tấn công lừa đảo người dùng Việt Nam: 320** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

4. Tài liệu lưu trữ

Chuyên mục **Cảnh báo tuần** tại địa chỉ:

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Chiến dịch tấn công: Chiến dịch tấn công của nhóm tấn công APT Earth Krahang gây ảnh hưởng tới 70 tổ chức tại 23 quốc gia."

Một chiến dịch tấn công mạng được thực hiện bởi nhóm APT Trung Quốc, có tên là "Earth Krahang", đã xâm nhập vào 70 tổ chức và nhắm tới ít nhất 116 tổ chức trên 45 quốc gia, trong đó có cả Việt Nam. Chiến dịch tấn công này bắt đầu từ đầu năm 2022 và chủ yếu nhằm vào các tổ chức chính phủ, đặc biệt là tại khu vực Đông Nam Á. Cụ thể, nhóm này đã tấn công 48 tổ chức chính phủ, trong đó có 10 Bộ Ngoại Giao.

Nhóm APT Earth Krahang sử dụng các công cụ mã nguồn mở để tìm kiếm các máy chủ công cộng có lỗ hổng bảo mật như CVE-2023-32315 (có trên Openfire) hoặc CVE-2022-21587 (có trên Oracle Web Apps). Sau đó, nhóm này tận dụng hai lỗ hổng trên để triển khai webshell, giúp họ xâm nhập vào hệ thống một cách trái phép và duy trì kết nối trong hệ thống đã bị tấn công.

Ngoài ra, nhóm tấn công cũng sử dụng spear-phishing làm phương tiện để tiếp cận hệ thống, với nội dung của email liên quan đến các vấn đề chính trị toàn cầu nhằm đánh lừa người dùng mở tệp đính kèm hoặc nhấp vào liên kết độc hại. Khi đã xâm nhập thành công, nhóm Earth Krahang sẽ sử dụng hạ tầng của tổ chức bị tấn công để lưu trữ các phần mềm độc hại, làm trung gian cho lưu lượng tấn công và sử dụng các tài khoản email chính phủ để tiếp tục tấn công các cơ quan chính phủ khác thông qua spear-phishing.

Các tệp đính kèm độc hại trong email được sử dụng để cài đặt backdoor trên thiết bị của người dùng. Cơ quan bảo mật đã phát hiện ra rằng nhóm Earth Krahang còn sử dụng các tài khoản email Outlook để thử mật khẩu trên Exchange, cũng như sử dụng script Python để trích xuất email từ các máy chủ thư Zimbra.

Nhóm Earth Krahang đã thiết lập máy chủ VPN trên các máy chủ bị xâm nhập bằng phần mềm SoftEtherVPN để kết nối với các hệ thống bị ảnh hưởng khác, điều này giúp họ dễ dàng chuyển đổi giữa các thiết bị. Sau đó, nhóm này sẽ triển khai các mã độc và công cụ như Cobalt Strike, RESHELL và XDealer để thực thi mã từ xa và thu thập dữ liệu. Mã độc backdoor XDealer phức tạp hơn so với hai mã độc còn lại vì nó ảnh hưởng đến cả hệ điều hành Linux và Windows, có khả năng ghi lại các thao tác gõ phím, chụp ảnh màn hình và chặn bắt các dữ liệu sao chép từ clipboard.

Phía cơ quan bảo mật cũng phát hiện ra một điểm chung giữa Earth Krahang và một nhóm APT Trung Quốc khác là Earth Lusca, dựa vào việc sử dụng chung các máy chủ C&C. Hiện cả hai nhóm đều bị tình nghi là một phần của một lực lượng gián điệp không gian mạng chuyên nghiệp được thành lập bởi chính phủ.Trước đó, mã độc RESHELL đã được nhóm APT Gallium sử dụng, trong khi XDealer đã được sử dụng bởi nhóm APT Luoyu.

Nguồn: https://www.bleepingcomputer.com/news/security/chinese-earth-krahang-hackers-breach-70-orgs-in-23-countries/

Tin tức An toàn thông tin

"Cảnh báo: Hình thức tấn công LoopDoS đe dọa đến hàng ngàn thiết bị."

Một loại tấn công từ chối dịch vụ mới được phát hiện, đang gây ảnh hưởng đến hàng ngàn thiết bị thông qua giao thức UDP, gọi là Loop DoS. Cách hoạt động của hình thức tấn công này là ghép đôi các máy chủ của giao thức UDP để chúng liên tục trao đổi dữ liệu với nhau.

Bản chất của giao thức UDP là "không-kết nối" vì nó không có khả năng xác thực địa chỉ IP nguồn, dẫn đến việc dễ bị tác động bởi hình thức tấn công giả mạo IP (IP Spoofing). Đối tượng tấn công thường sử dụng kỹ thuật này để gửi các gói tin UDP chứa địa chỉ IP của nạn nhân tới các máy chủ đích, khiến chúng phản hồi lại nạn nhân và tạo ra cuộc tấn công từ chối dịch vụ ánh xạ (Reflected DoS).

Trong nghiên cứu mới nhất về giao thức UDP, các chuyên gia phát hiện ra rằng một số dịch vụ như DNS, NTP, TFTP, Active Users, Daytime, Echo, Chargen, QOTD và Time đều có thể bị lợi dụng để tạo ra một vòng lặp tấn công DoS tự tồn tại. Cụ thể, hình thức tấn công này xảy ra khi hai máy chủ cùng chạy trên phiên bản của giao thức mà các đối tượng tấn công đang khai thác.

Đối tượng tấn công giả mạo địa chỉ IP của một máy chủ (SV1) và kết nối tới máy chủ còn lại (SV2), khiến máy chủ SV2 phản hồi thông báo lỗi về cho SV1. Sau đó, SV1 gửi lại thông báo lỗi tới SV2, tạo ra một vòng lặp gửi thông báo lỗi giữa hai máy chủ, làm cạn tài nguyên của chúng và gây gián đoạn dịch vụ.

Theo điều tra, khoảng 300.000 hệ thống và mạng lưới có thể bị khai thác để thực hiện tấn công Loop DoS. Hiện không có bằng chứng nào cho thấy tấn công này đã được sử dụng trong thực tế, nhưng các chuyên gia vẫn cảnh báo về nguy cơ của nó. Nhiều sản phẩm từ các nhà sản xuất như Broadcom, Cisco, Honeywell, Microsoft, MikroTik và Zyxel có thể bị ảnh hưởng. Đối tượng tấn công chỉ cần một hệ thống có khả năng giả mạo để thực hiện tấn công, vì vậy các quản trị viên cần chủ động lọc các luồng dữ liệu giả mạo để bảo vệ hệ thống.

Nguồn: https://thehackernews.com/2024/03/new-loop-dos-attack-impacts-hundreds-of.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 **782** lỗ hổng, trong đó có 224 lỗ hổng mức Cao, 273 lỗ hổng mức Trung bình, 29 lỗ hổng mức Thấp và 256 lỗ hổng chưa đánh giá. Trong đó có ít nhất 122 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 25 lỗ hổng trong Linux, Nhóm 07 lỗ hổng trong Google, Nhóm 56 lỗ hổng trong Adobe, Nhóm 05 lỗ hổng trong Microsoft, Nhóm 13 lỗ hổng trong Mozilla, Nhóm 03 lỗ hổng trong Github, Nhóm 10 lỗ hổng trong IBM. 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-2023-52609, CVE-2023-52610,...

- Google: CVE-2024-2625, CVE-2024-2626,...

- Adobe: CVE-2024-20761,...

- Microsoft: CVE-2024-29059,...

- Mozilla: CVE-2023-5388, CVE-2024-2605,...

- Github: CVE-2024-2443, CVE-2024-2469,...

- IBM: CVE-2024-22352, CVE-2023-45177,...

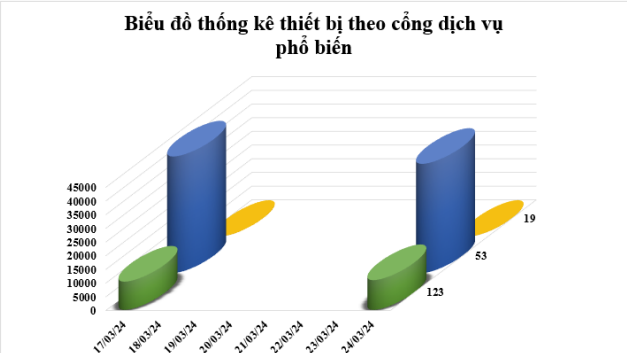
Thông tin điểm yếu, lỗ hổng

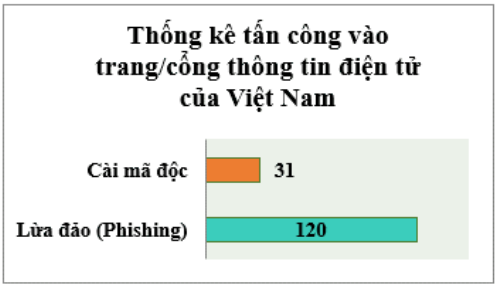
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-52609 CVE-2023-52610 CVE-2023-52611 ...	Nhóm 25 lỗ hổng trong Linux cho phép tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Google	CVE-2024-2625 CVE-2024-2626 CVE-2024-2627 ...	Nhóm 07 lỗ hổng trong Google cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Adobe	CVE-2024-20761 CVE-2024-20752 CVE-2024-20755 ...	Nhóm 56 lỗ hổng trong Adobe cho phép đối tượng tấn công, khai thác lỗi XSS, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Microsoft	CVE-2024-29059 CVE-2024-28916 CVE-2024-26247 ...	Nhóm 05 lỗ hổng trong Microsoft cho phép đối tượng tấn công leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
5	Mozilla	CVE-2023-5388 CVE-2024-2605 CVE-2024-2606 ...	Nhóm 13 lỗ hổng trong Mozilla cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Github	CVE-2024-2443 CVE-2024-2469 CVE-2024-1908	Nhóm 03 lỗ hổng trong Github cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2024-22352 CVE-2023-45177 CVE-2022-32751 ...	Nhóm 10 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

Thống kê nguy cơ, các cuộc tấn công mạng vào 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 **50.788** (giảm so với tuần trước **52.933**) 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.



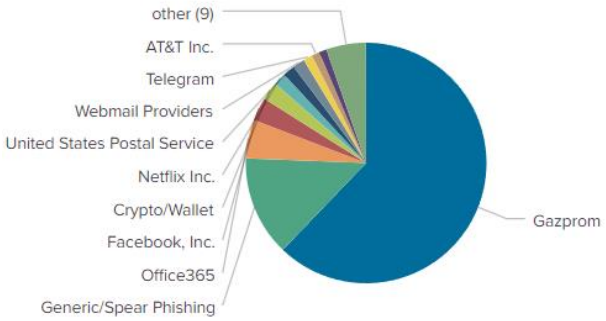


Tấn công Web

Trong tuần, có **151** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 120 trường hợp tấn công lừa đảo (Phishing), 31 trường hợp tấn công cài cắm mã độc.

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, Payment, 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.



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

differentia.ru: 1923 IP	hzmksreiuojy.ru: 42 IP
disorderstatus.ru: 988 IP	xjpakmdcfuqe.biz: 22 IP
atomictrivia.ru: 518 IP	xjpakmdcfuqe.com: 23 IP
amnsreiuojy.ru: 124 IP	xjpakmdcfuqe.ru: 16 IP
restlesz.su: 89 IP	xjpakmdcfuqe.in: 13 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **320** phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam phản ánh 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, các trang thương mại điện tử…

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

STT	Website lừa đảo	Ghi chú
1	vib[.]truc-tuyen-cham-socthekhachhang[.]com cskh-vib[.]ho-tro-tin-dung-ca-nhan[.]com dich-vu-xvip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
2	www[.]taikhoanvps[.]com[.]vn motaikhoanchungkhoanvps[.]com	Website giả mạo Công ty chứng khoán VPS
3	shinhan[.]ho-tro-tin-dung-ca-nhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
4	eufk55[.]com tikimall[.]org	Website giả mạo sàn TMĐT Tiki
5	vn78223p[.]com vn86414s[.]com s33788[.]com/ vn667755s[.]com/login	Website giả mạo sàn TMĐT Shopee
6	apple[.]support-find-my-iphone[.]com/s113h	Website giả mạo Apple
7	tpbank[.]chamsocthekhachang-truc-tuyen[.]com/	Website giả mạo Ngân hàng TMCP Tiên Phong
8	nganhangsaison[.]org/	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
9	policeonline[.]club/	Website giả mạo Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC)
10	dichvucong[.]cvgov[.]com	Website giả mạo Dịch vụ công Quốc Gia

NCSC VN
National Cyber Security Center

Khuyến nghị đối với các cơ quan, đơn vị

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

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin tức an toàn thông tin,** 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 thông tin để phát hiện và ngăn chặn, xử lý kịp thời.

***

2. Đối với các điểm yếu, lỗ hổng trong phần **Lỗ hổng bảo mật**, 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. Bên cạnh đó, 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.

***

4. Đối với các website giả mạo thống kê tại mục **Tấn công lừa đảo người dùng Việt Nam**, Quý đơn vị cần chú ý quan tâm không truy cập vào các trang web được nêu để tránh nguy cơ bị tấn công lừa đảo, nâng cao nhận thức bản thân và tuyên truyền cho bạn bè, người thân và những người xung quanh tránh việc trở thành nạn nhân của những cuộc tấn công lừa đảo này.

024.3209.1616
ncsc@ais.gov.vn
https://khonggianmang.vn/
https://www.facebook.com/govSOC
Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội