NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 50 (11/12/2023 – 17/12/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Lazarus Group khai thác các lỗ hổng Log4j để triển khai trojan truy cập từ xa.

- **Cảnh báo:** Mã độc NKAbuse sử dụng blockchain NKN để tấn công DDoS.

2. Điểm yếu, lỗ hổng

- **975** 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: 302** 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://service.khonggianmang.vn

https://khonggianmang.vn

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Lazarus Group khai thác các lỗ hổng Log4j để triển khai trojan truy cập từ xa"

Nhóm APT Lazarus Group, có liên quan đến Triều Tiên, đang thực hiện một chiến dịch tấn công toàn cầu khai thác lỗ hổng bảo mật trong Log4j để triển khai trojan truy cập từ xa (RAT) lên các hệ thống bị ảnh hưởng.

Chiến dịch tấn công này được theo dõi dưới tên Operation Blacksmith và nổi bật với việc sử dụng ba loại mã độc DLang khác nhau bao gồm: NineRAT, DLRAT, và BottomLoader. Mặc dù phương thức tấn công trong chiến dịch này có nhiều thay đổi nhưng phát hiện ra nhiều điểm tương đồng với cách thức hoạt động của nhóm Andariel, một nhóm con thuộc Lazarus Group.

Chuỗi tấn công bằng NineRAT bắt đầu bằng việc khai thác lỗ hổng Log4Shell (CVE-2021-44228) trên các máy chủ công cộng của VMWare Horizon, nhằm triển khai NineRAT đến các hệ thống mục tiêu. Các ngành công nghiệp như sản xuất, nông nghiệp, và bảo mật vật lý đã phải đối mặt với ảnh hưởng của chiến dịch này, đặc biệt là khi ứng dụng vẫn sử dụng các phiên bản thư viện Log4j có lỗ hổng sau 2 năm từ khi công bố.

Mã độc NineRAT được phát triển từ tháng 5/2022 và lần đầu được triển khai vào tháng 03/2023 trong chiến dịch nhằm vào tổ chức nông nghiệp tại Nam Mỹ và trong một chiến dịch khác vào tháng 09/2023 nhằm vào đơn vị sản xuất tại Châu u. Mã độc này sử dụng các dịch vụ nhắn tin hợp pháp như Telegram để liên lạc với máy chủ C&C, nhằm giữ cho việc tấn công của chúng trở nên khó phát hiện.

NineRAT đóng vai trò quan trọng trong chiến dịch tấn công của Lazarus Group, là điểm tương tác chính với hệ thống bị ảnh hưởng. Mã độc này cung cấp cho nhóm tấn công Lazarus khả năng thực hiện nhiều hoạt động như thu thập thông tin, tải lên và tải xuống file, thậm chí cả khả năng tự nâng cấp và gỡ bỏ. Điều này tạo ra một môi trường linh hoạt cho Lazarus Group và hỗ trợ nhóm thích ứng với các mục tiêu cụ thể.

Nguồn: https://thehackernews.com/2023/12/lazarus-group-using-log4j-exploits-to.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Lazarus Group khai thác các lỗ hổng Log4j để triển khai trojan truy cập từ xa"

Chuyên gia bảo mật nhận định rằng sau khi mã độc NineRAT được kích hoạt trên thiết bị người dùng, nó sẽ nhận lệnh từ kênh C&C trên Telegram để ghi lại thông tin về thiết bị bị nhiễm mã độc. Việc phân tích dấu vân tay số mà mã độc để lại cho thấy rằng dữ liệu thu thập bởi Lazarus có thể được chia sẻ với các nhóm APT khác và được lưu trữ trong nhiều kho dữ liệu khác nhau. Sau giai đoạn trinh sát, chiến dịch Operation Blacksmith sử dụng bộ công cụ proxy HazyLoad để khai thác lỗ hổng bảo mật nghiêm trọng trong JetBrains TeamCity (CVE-2023-42793, điểm CSS: 9,8). Bộ công cụ này được tải và thực thi bởi mã độc BottomLoader.

Qua quan sát, có thể nhận thấy chiến dịch Operation Blacksmith tiếp tục phát tán mã độc DLRAT để vừa làm bộ tải vừa làm RAT. Mục tiêu của DLRAT là thực hiện trinh sát hệ thống, triển khai mã độc và thực thi các lệnh từ máy chủ C&C đến hệ thống bị tấn công. DLRAT được biết đến là một mã độc phát triển theo xu hướng của Lazarus, sử dụng ngôn ngữ và framework hiếm gặp, cùng với mã độc có tính module nhằm tránh bị phát hiện.

Việc sử dụng nhiều bộ công cụ có cùng vai trò backdoor mang lại cho Lazarus Group các phương án dự phòng, giúp duy trì việc truy nhập cao trong trường hợp một công cụ bị phát hiện. Không bất ngờ khi nhóm Andariel khai thác lỗ hổng Log4Shell vì trước đó, họ đã sử dụng lỗ hổng này để lan truyền mã độc EarlyRAT.

Thông tin chi tiết về chiến dịch này được tiết lộ sau khi nhóm Kimsuky, cũng thuộc Lazarus Group sử dụng phiên bản Autolt của mã độc Amadey và RftRAT trong một cuộc tấn công spear-phishing, sử dụng file đính kèm độc hại và đường dẫn độc hại nhằm vượt qua các giải pháp bảo mật. Bên cạnh đó, sau khi phát hiện chiến dịch lừa đảo liên quan đến Konni, nhóm này đã sử dụng các tệp thực thi giả mạo thành các tệp Word để lan truyền mã độc backdoor có chức năng nhận lệnh và thực thi mã độc dưới dạng XML.

Nguồn:
https://thehackernews.com/2023/12/lazarus-group-using-log4j-exploits-to.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Mã độc NKAbuse sử dụng blockchain NKN để tấn công DDoS"

Một mã độc mới đa nền tảng có tên NKAbuse vừa bị phát hiện khi sử dụng giao thức kết nối mạng phi tập trung P2P với NKN (viết tắt cho New Kind of Network) làm kênh liên lạc cho mã độc. Công nghệ trao đổi dữ liệu giữa các thiết bị ngang hàng của NKN đã bị lợi dụng để tạo ra một thiết bị cấy ghép mạnh mẽ có khả năng làm tràn và làm backdoor.

Mạng NKN có hơn 62,000 điểm kết nối trên mạng lưới blockchain và được mô tả như một mạng lưới phần mềm trên Internet, cho phép người dùng chia sẻ băng thông mạng dư thừa, đồng thời, được nhận token như một phần thưởng. NKN được tạo ra như một lớp bổ sung cho hệ thống Internet bao gồm một phần blockchain đặc biệt được tích hợp lên trên ngăn xếp giao thức TCP/IP đã có sẵn.

Mã độc NKAbuse lợi dụng công nghệ blockchain để thực hiện tấn công từ chối dịch vụ (DDoS) và hoạt động như một phần cấy ghép trên các hệ thống bị nhiễm mã độc. Được viết bằng ngôn ngữ lập trình Go, NKAbuse có khả năng giao tiếp với bot chủ và thực thi các câu lệnh, chủ yếu tập trung vào các hệ thống sử dụng Linux, kể cả các thiết bị IoT ở Colombia, Mexico và Việt Nam.

Nguồn:https://thehackernews.com/2023/12/new-nkabuse-malware-exploits-nkn.html?&web_view=true

Hiện vẫn chưa xác định rõ mức độ ảnh hưởng của chiến dịch tấn công này. Tuy nhiên, đã phát hiện lỗ hổng bảo mật tồn tại trong Apache Struts (CVE-2017-5637, Điểm CVSS: 10.0) được sử dụng trong suốt 6 năm để xâm nhập vào hệ thống của một công ty tài chính. Khi lỗ hổng này bị khai thác, mã độc sẽ tải xuống một đoạn mã shell script từ máy chủ từ xa và kiểm tra phiên bản hệ điều hành. Máy chủ từ xa lưu trữ 8 phiên bản mã độc NKAbuse khác nhau (i386, arm64, arm, amd64, mips, mipsel, mips64, và mips64el) tương ứng với các cấu trúc CPU, nhưng mã độc này không tự phát tán mà chỉ có thể lây nhiễm thông qua một lỗ hổng bảo mật.

Để duy trì sự tồn tại sau mỗi lần khởi động, NKAbuse sử dụng cron jobs và yêu cầu quyền root bằng cách kiểm tra user ID. Nếu ID là 0, mã độc sẽ thêm vào crontab để chạy mỗi lần khởi động. NKAbuse cũng có tính năng backdoor, gửi thông điệp định kỳ cho bot chủ, bao gồm thông tin hệ thống, chụp ảnh màn hình, thực hiện tác vụ lên file và thực thi câu lệnh hệ thống.

Chuyên gia bảo mật nhận định rằng mã độc được thiết kế đặc biệt để tích hợp vào botnet và có khả năng hoạt động như một backdoor trên một số thiết bị cụ thể. Ngoài ra, việc sử dụng công nghệ blockchain không chỉ đảm bảo sự an toàn và ẩn danh mà còn duy trì sự phát triển bền vững của botnet trong thời gian dài mà không cần bộ điều khiển trung tâm có thể định dạng được.

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 **975** lỗ hổng, trong đó có 344 lỗ hổng mức Cao, 502 lỗ hổng mức Trung bình, 17 lỗ hổng mức Thấp và 112 lỗ hổng chưa đánh giá. Trong đó có ít nhất 248 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 34 lỗ hổng trong Google, Nhóm 35 lỗ hổng trong Microsoft, Nhóm 33 lỗ hổng trong Apple, Nhóm 78 lỗ hổng trong Wordpress, Nhóm 16 lỗ hổng trong Dell, Nhóm 214 lỗ hổng trong Adobe, Nhóm 14 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:

- Google: CVE-2023-48423,...

- Microsoft: CVE-2023-35624,...

- Apple: CVE-2023-40446, CVE-2023-42910,...

- Wordpress: CVE-2023-5756,...

- Dell: CVE-2023-48660, CVE-2023-48662,...

- Adobe: CVE-2023-48632,...

- IBM: CVE-2023-45166, CVE-2023-45170,...

Thông tin điểm yếu, lỗ hổng

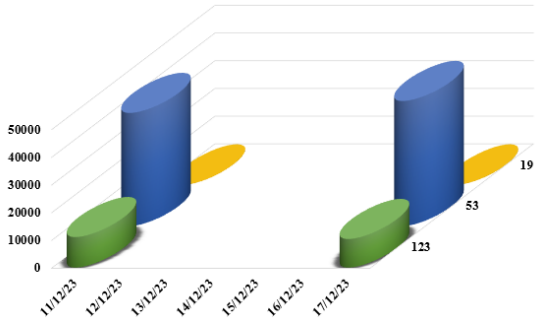
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-48423 CVE-2023-45866 CVE-2023-48398 …	Nhóm 34 lỗ hổng trong Google cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
2	Microsoft	CVE-2023-35624 CVE-2023-35621 CVE-2023-36010 …	Nhóm 35 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền, thực thi mã từ xa, khai thác lỗ hổng XSS.	Đã có thông tin xác nhận và bản vá
3	Apple	CVE-2023-40446 CVE-2023-42910 CVE-2023-42882 …	Nhóm 33 lỗ hổng trong Apple cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-5756 CVE-2023-6035 CVE-2023-48771 …	Nhóm 78 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực thi mã từ xa, thực hiện SQL Injection, khai thác lỗ hổng XSS, khai thác lỗ hổng CSRF.	Chưa có thông tin xác nhận và bản vá
5	Dell	CVE-2023-48660 CVE-2023-48662 CVE-2023-48663 …	Nhóm 16 lỗ hổng trong Dell cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, khai thác lỗ hổng CSRF.	Đã có thông tin xác nhận và bản vá
6	Adobe	CVE-2023-48632 CVE-2023-48633 CVE-2023-48634 …	Nhóm 214 lỗ hổng trong Adobe cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ, khai thác lỗ hổng XSS.	Đã có thông tin xác nhận và bản vá
7	IBM	CVE-2023-45166 CVE-2023-45170 CVE-2023-45174 …	Nhóm 14 lỗ hổng trong IBM phép đối tượng tấn công leo thang đặc quyền, 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

Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

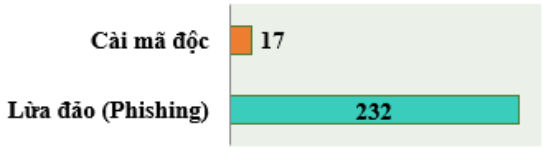
Tấn công DRDoS

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 **55.537**, (tăng so với tuần trước **51.921**) 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.

Biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến

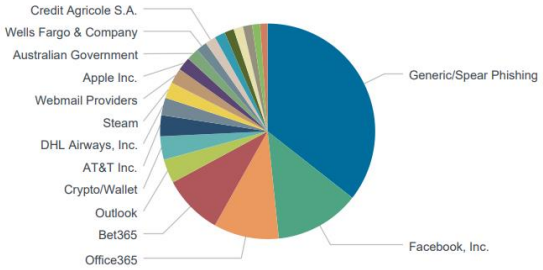


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **249** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 232 trường hợp tấn công lừa đảo (Phishing), 17 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: 13390 IP	hzmksreiuojy.ru: 208 IP
disorderstatus.ru: 4539 IP	xjpakmdcfuqe.biz: 211 IP
atomictrivia.ru: 2068 IP	xjpakmdcfuqe.com: 73 IP
amnsreiuojy.ru: 856 IP	xjpakmdcfuqe.ru: 50 IP
restlesz.su: 343 IP	xjpakmdcfuqe.in: 30 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **302** 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	vxvw55.com	Website giả mạo sàn TMĐT Tiki
2	xskttd5d.com	Website giả mạo Công ty Cổ phần Viễn thông FPT
3	vib.khach-hang-the-tructuyen.online vib.khach-hang-the-tructuyen.com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
4	veitgov.cc	Website giả mạo Dịch vụ công Quốc Gia
5	tindungshb.com	Ngân hàng TMCP Sài Gòn – Hà Nội

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 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