NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 33 (14/8/2023 – 20/8/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT29 sử dụng ứng dụng nhắn tin Zulip để che giấu máy chủ C&C trong chiến dịch tấn công lừa đảo (Phishing).

- **Cảnh báo:** Chiến dịch LABRAT sử dụng lỗ hổng trong GitLab để tấn công Cryptojacking và Proxyjacking.

2. Điểm yếu, lỗ hổng

- **632** 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: 314** 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

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT29 sử dụng ứng dụng nhắn tin Zulip để che giấu máy chủ C&C trong chiến dịch tấn công lừa đảo (Phishing)"

Một chiến dịch tấn công đang diễn ra nhằm vào đại sứ quán của các quốc gia thuộc NATO có dấu hiệu liên kết tới đối tượng tấn công tại Nga.

Chiến dịch tấn công Phishing sử dụng văn bản PDF với nội dung ngoại giao được sử dụng để lây nhiễm mã độc Duke, có liên kết tới nhóm APT29 (hay còn được biết đến với tên gọi BlueBravo, Cloaked Ursa, Cozy Bear, Iron Hemlock, Midnight Blizzard và The Dukes)

Theo chuyên gia bảo mật, đối tượng tấn công sử dụng ứng dụng Zulip làm máy chủ C&C để hoạt động, nhằm giảm thiểu nguy cơ bị phát hiện thông qua việc ẩn mình sau các lưu lượng web hợp pháp. Chuỗi lây nhiễm được mô tả như sau: file PDF được nhúng code JavaScript thực thi một quy trình đa giai đoạn để cài vào một backdoor duy trì trên mạng lưới bị xâm nhập.

Việc sử dụng chủ đề này của APT29 đã từng được ghi lại trong chiến dịch tấn công giả danh đại sứ quan Na Uy trước đó nhằm truyền đi payload DLL có khả năng kết nối tới máy chủ từ xa để tải xuống thêm payload bổ trợ.

Domain "bahamas.gov[.]bs" được sử dụng trong cả hai bộ xâm nhập càng góp phần củng cố sự liên kết giữa 2 chiến dịch này.

Nếu người dùng mở lên file PDF, một dropper HTML độc hại với tên "Invitation_Farewell_DE_EMB" được khởi chạy để thực thi JavaScript tải xuống file ZIP, file này chứa HTML Application (HTA) được thiết kế để triển khai mã độc Duke.

Máy chủ C&C sử dụng API của Zulip gửi đi các thông tin của nạn nhân tới một phòng chat tạo bởi đối tượng tấn công (toyy.zulipchat[.]com) đồng thời cũng là chỉ huy từ xa các máy chủ bị xâm nhập

Ngoài ra, một file PDF khác còn được tìm thấy và được nghi là dùng để thăm dò hoặc phục vụ mục đích thử nghiệm của nhóm APT29.

Mục tiêu chính của nhóm tấn công APT29 là nhằm vào chính phủ, các bên có hợp đồng với chính phủ, tổ chức chính trị, viện nghiên cứu và các ngành công nghiệp quan trọng tại Mỹ và Châu Âu.

Diễn biến này được công bố khi một công ty bảo mật đưa ra cảnh báo về hình thức tấn công Phisihing nhằm vào các tổ chức thuộc Ukraine sử dụng bộ tool hậu khai thác mã nguồn mở - Merlin. Hoạt động này đang được theo dõi dưới mã UAC-0154.

Một số mã độc còn bao gồm NETD nhằm đảm bảo duy trì, DROPBEAR để thiết lập kết nối từ xa, STL để thu thập dữ liệu từ hệ thống vệ tinh Starlink, DEBLIND để trích xuất dữ liệu và mã độc Mirai botnet. Ngoài ra, trong chiến dịch tấn công còn sử dụng dịch vụ ẩn TOR để truy cập thiết bị trên mạng LAN thông qua Internet.

Nguồn: https://thehackernews.com/2023/08/russian-hackers-use-zulip-chat-app-for.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Chiến dịch LABRAT sử dụng lỗ hổng trong GitLab để tấn công Cryptojacking và Proxyjacking"

Gần đây, chiến dịch tấn công mạng LABRAT đã bị phát hiện với động cơ tài chính, bằng cách khai thác lỗ hổng Nghiêm trọng tồn tại trên GitLab trong chiến dịch tấn công Cryptojacking và Proxyjacking.

Theo chuyên gia bảo mật, đối tượng tấn công sử dụng Signature - Based, phần mềm độc hại đa nền tảng, công cụ C&C vượt qua tường lửa và rootkit dựa trên kernel để che giấu sự hiện diện của mình. Đối với máy chủ C&C, đối tượng tấn công lạm dụng dịch vụ của TryCloudflare để che giấu đi máy chủ.

Hình thức tấn công Proxyjacking cho phép đối tượng tấn công thuê một máy chủ bị xâm nhập trên mạng proxy, từ đó kiếm được tiền từ băng thông không sử dụng. Cryptojacking là hình thức tấn công cho phép đối tượng sử dụng các tài nguyên hệ thống để phục vụ tác vụ đào tiền ảo.

Một điểm đáng chú ý của chiến dịch là việc sử dụng các tệp nhị phân được viết bằng Go và .NET để tránh bị phát hiện, kết hợp thêm khả năng cung cấp truy cập backdoor của LABRAT. Qua đó mở ra hướng đi cho các cuộc tấn công tiếp theo, đánh cắp dữ liệu và thực hiện tấn công ransomware.

Chuỗi tấn công bắt đầu bằng việc khai thác lỗ hổng CVE-2021-22205 (Điểm CVSS: 10) cho phép đối tượng tấn công thực thi mã từ xa đã và đang được sử dụng để triển khai bộ đào tiền ảo. Khi xâm nhập thành công, một tệp script dropper shell sẽ được tải về từ máy chủ C&C nhằm thiết lập tính liên tục, thực hiện leo thang đặc quyền và tải thêm các tệp nhị phân bổ trợ từ kho dữ liệu riêng tư của GitLab.

Trong chiến dịch LABRAT, đối tượng tấn công đã sử dụng dịch vụ TryCloudflare để điều hướng kết nối tới một web server chứa tệp script shell độc hại. TryCloudflare là một công cụ miễn phí dùng để tạo một Cloudflare Tunnel mà không yêu cầu thêm trang web vào DNS của Cloudflare. Nó khởi chạy một tiến trình tạo ra các subdomain ngẫu nhiên trên trycloudflare.com, qua đó công khai tài nguyên chưa sử dụng lên mạng internet công khai.

Sự phát triển này làm gia tăng việc lạm dụng dịch vụ Clouflare để triển khai các kênh liên lạc kín từ máy chủ bị xâm nhập và quyền truy cập chính tới mạng của nạn nhân.

Trong biến thể thứ hai của cuộc tấn công, đối tượng tấn công đã sử dụng máy chủ Solr thay vì TryCloudflare để tải xuống một bản khai thác cho PwnKit (CVE-2021-4034) từ kho dữ liệu GitLab nhằm leo thang đặc quyền.

Một số payload tải xuống bởi script dropper gồm có tiện ích mã nguồn Global Socker để tạo kết nối từ xa, cùng với các tệp nhị phân thực hiện Cryptojacking, Proxyjacking thông qua dịch vụ IPRoyal và ProxyLite. Quá trình đào tiền ảo được che giấu bởi rookit trên kernel với tên "hiding-cryptominers-linux-rootkit".

Ngoài ra, còn có một tệp thực thi dựa trên ngôn ngữ lập trình Go, được thiết kế để duy trì kết nối và tắt tiến trình hoặc phiên bản cũ hơn của chính nó, nhằm tối ưu hóa việc sử dụng tài nguyên của thiết bị cho việc khai thác tiền ảo.

Nguồn: https://thehackernews.com/2023/08/new-labrat-campaign-exploits-gitlab.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 **632** lỗ hổng, trong đó có 120 lỗ hổng mức Cao, 113 lỗ hổng mức Trung bình, 04 lỗ hổng mức Thấp và 395 lỗ hổng chưa đánh giá. Trong đó có ít nhất 113 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 18 lỗ hổng trong Apple, Nhóm 05 lỗ hổng trong Linux, Nhóm 62 lỗ hổng trong Google, Nhóm 81 lỗ hổng trong Wordpress, Nhóm 56 lỗ hổng trong Intel, Nhóm 02 lỗ hổng trong Apache, Nhóm 06 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:

- Apple: CVE-2022-48503, CVE-2023-28918,...

- Linux : CVE-2023-40283, CVE-2023-4385,...

- Google: CVE-2023-21273, CVE-2023-21229,...

- Wordpress: CVE-2023-3452, CVE-2023-4293,...

- Intel: CVE-2023-25775, CVE-2023-29887,...

- Apache: CVE-2023-40272, CVE-2023-40037

- IBM: CVE-2023-35009, CVE-2023-35893,...

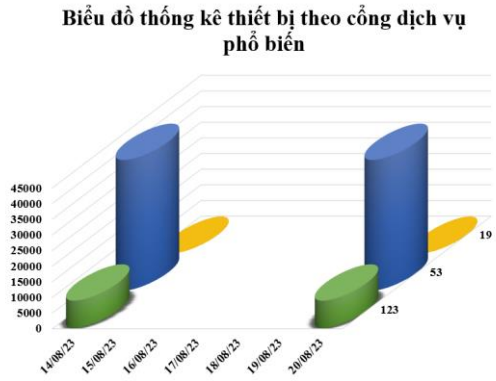
Thông tin điểm yếu, lỗ hổng

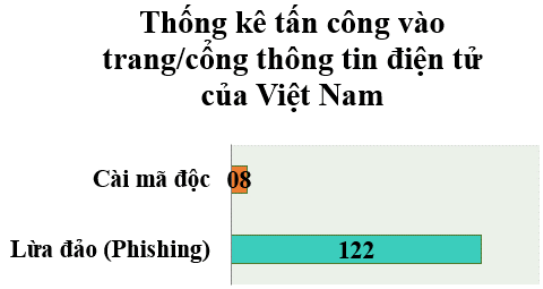
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Apple	CVE-2022-48503 CVE-2023-28198 CVE-2023-32358 …	Nhóm 18 lỗ hổng trong Apple cho phép đối tượng tấn công thực hiện leo thang đặc quyền, thực thi mã từ xa, thực hiện Spoofing, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-40283 CVE-2023-4385 CVE-2023-4387 …	Nhóm 05 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Google	CVE-2023-21273 CVE-2023-21229 CVE-2023-21231	Nhóm 62 lỗ hổng trong Google cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-3452 CVE-2023-4293 CVE-2023-3958 …	Nhóm 81 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền, thực thi mã từ xa, thực hiện tấn công XSS, thực hiện tấn công CSRF, thực hiện tấn công SQL Injecton.	Đã có thông tin xác nhận và bản vá
5	Intel	CVE-2023-25775 CVE-2022-29887 CVE-2023-27515 …	Nhóm 56 lỗ hổng trong Intel cho phép đối tượng tấn công thực hiện leo thang đặc quyền, khai thác lỗ hổng XSS, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
6	Apache	CVE-2023-40272 CVE-2023-40037	Nhóm 02 lỗ hổng trong Apache 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
7	IBM	CVE-2023-35009 CVE-2023-35893 CVE-2023-35011 …	Nhóm 06 lỗ hổng trong IBM phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá

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

Tấn công DRDoS

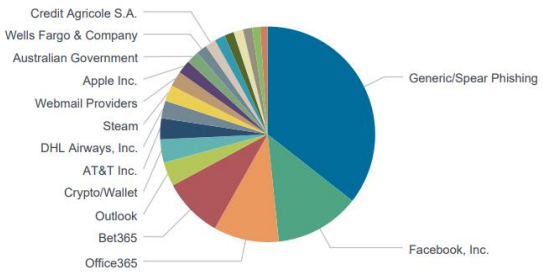
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **49.587**, (giảm so với tuần trước **50.652**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), 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 130 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 122 trường hợp tấn công lừa đảo (Phishing), 08 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: 8887 IP	xjpakmdcfuqe.ru: 45 IP
disorderstatus.ru: 2971 IP	xjpakmdcfuqe.in: 44 IP
atomictrivia.ru: 1398 IP	restlesz.su: 214 IP
xjpakmdcfuqe.biz: 171 IP	amnsreiuojy.ru: 238 IP
xjpakmdcfuqe.com: 52 IP	hzmksreiuojy.ru: 48 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **314** 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	mkg283868.com	Website giả mạo sàn TMĐT Lazada
2	skdg511.com shopeelive.site	Website giả mạo sàn TMĐT Shopee
3	dhte11.com	Website giả mạo sàn TMĐT Tiki
4	ama-zon-sc.cc	Website giả mạo Amazon
5	internetcapquang.com.vn tongdaitruyenhinhcap68h.online trungtam-truyenhinhcap.online dichvutruyenhinh.info	Website giả mạo SCTV

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