NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 45 (06/11/2023 – 12/11/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT SideCopy khai thác lỗ hổng trên WinRAR trong chiến dịch tấn công nhằm vào chính phủ Ấn Độ.

- **Cảnh báo:** Lỗ hổng Zero-Day - Lace Tempest khai thác lỗ hổng an toàn thông tin trên phần mềm hỗ trợ SysAid IT.

2. Điểm yếu, lỗ hổng

- **670** 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: 332** 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 SideCopy khai thác lỗ hổng trên WinRAR trong chiến dịch tấn công nhằm vào chính phủ Ấn Độ"

Nhóm APT SideCopy được phát hiện là đang sử dụng lỗ hổng an toàn thông tin trên WinRAR trong chiến dịch tấn công nhằm vào các cơ quan chính phủ của Ấn Độ nhằm phát tán mã độc trojan truy cập từ xa như AllaKore RAT, Ares RAT và Drat.

Theo ghi nhận từ công ty bảo mật, chiến dịch này hoạt động trên đa nền tảng với phiên bản của Ares RAT cho phép xâm nhập vào hệ thống Linux.

SideCopy bắt đầu hoạt động từ năm 2019 và được biết đến nhờ các chiến dịch tấn công nhằm vào Ấn Độ và Afghanistan. Hiện nhóm này được tình nghi là một nhóm con của nhóm APT Transparent Tribe (hay APT36) do có điểm chung về hạ tầng và mã độc để tấn công nhằm vào Ấn Độ.

Đầu tháng 5 năm nay, nhóm này đã được gán với một chiến dịch lừa đảo sử dụng mồi nhử liên quan tới Tổ chức Nghiên cứu và Phát triển Quốc phòng Ấn Độ (DRDO) để phát tán mã độc đánh cắp thông tin. Kể từ thời điểm đó, SideCopy cũng có liên quan tới một chuỗi tấn công lừa đảo nhằm vào lĩnh vực quốc phòng của Ấn Độ với các file đính kèm dạng ZIP để phát tán Action RAT và mã độc trojan dựa trên .NET có khả năng thực thi 18 câu lệnh khác nhau.

Trong chiến dịch mới được phát hiện này, nhóm này đã sử dụng hai chuỗi tấn công khác nhau để nhằm vào hệ điều hành Linux hoặc Windows.

Đối với Linux đối tượng tấn công sử dụng binary ELF viết bằng Golang để phát tán Ares RAT có khả năng liệt kê file, chụp ảnh màn hình và tải xuống file.

Còn trên Windows, đối tượng khai thác lỗ hổng CVE-2023-38831 nằm trên WinRAR để thực thi mã độc, dẫn tới việc triển khai AllaKore RAT, Ares RAT và hai mã độc mới là DRat và Key RAT. Mã độc DRat có khả năng đánh cắp thông tin hệ thống, lưu lại phím gõ, chụp màn hình, tải xuống file cũng như alf truy cập từ xa vào thiết bị để gửi câu lệnh, dữ liệu bị đánh cắp về máy chủ C&C.

Ấn Độ đang quyết định thay thế hệ điều hành Microsoft Windows thành MayaOS cho lĩnh vực quốc phòng và chính phủ của họ, bởi vậy việc SideCopy nhằm vào Linux không phải là một sự trùng hợp.

SideCopy đang mở rộng kho vũ khí của mình với các lỗ hổng zero-day để nhằm vào tổ chức quốc phòng tại Ấn Độ với các mã độc trojan truy cập từ xa khác nhau, đồng thời APT36 cũng mở rộng việc chia sẻ trình hỗ trợ Linux cho SideCopy nhằm triển khai Python RAT mã nguồn mở, Ares.

Nguồn:
https://thehackernews.com/2023/11/sidecopy-exploiting-winrar-flaw-in.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng Zero-Day - Lace Tempest khai thác lỗ hổng an toàn thông tin trên phần mềm hỗ trợ SysAid IT"

Nhóm tấn công Lace Tempest đã được biết đến với chiến dịch tấn công mới bằng việc khai thác lỗ hổng zero-day tồn tại trên phần mềm hỗ trợ SysAid IT.

Lace Tempest nổi tiếng với việc phát tán mã độc ransomware Cl0p, trước đây đã từng khai thác các lỗ hổng zero-day tồn tại trên MOVEit Transfer và máy chủ PaperCut.

Lỗ hổng an toàn thông tin với mã định danh CVE-2023-47245 là một lỗi đường dẫn truyền tải, sau khi bị khai thác sẽ cho phép đối tượng tấn công thực thi mã trong quá trình cài đặt tại chỗ. Hiện nay, lỗ hổng này đã được vá trong phiên bản 23.3.36 của phần mềm.

Sau khi khai thác lỗ hổng CVE-2023-47245, nhóm Lace Tempest thực thi các câu lệnh qua phần mềm SysAid để tải xuống bộ tải mã độc cho Gracewire. Sau đó, chuỗi tấn công được tiếp nối bởi các tác vụ thực hiện thủ công bởi đối tượng tấn công như leo thang đặc quyền ngang, đánh cắp dữ liệu và triển khai ransomware.

Theo SysAid, nhóm tấn công đã tải lên một file lưu trữ WAR có chứa webshell và các dữ liệu độc hại khác vào thư mục gốc của dịch vụ web SysAid Tomcat. Ngoài vai trò làm backdoor cho thiết bị nhiễm mã độc, webshell này còn được sử dụng để tải xuống một tập lệnh PowerShell được thiết kế để tải xuống mã độc Gracewire.

Sau đó, nhóm Lace Tempest triển khai thêm một tập lệnh PowerShell thứ hai được sử dụng để xóa dấu vết của lỗ hổng sau khi khai thác payload độc hại. Điểm đặc trưng trong chuỗi tấn công này là việc sử dụng MeshCentral Agent cùng với PowerShell để tải và thực thi Cobalt Strike, đây là một framework hậu khai thác hợp pháp.

Các đơn vị đang sử dụng SysAid cần cập nhật bản vá sớm nhất có thể để hạn chế nguy cơ bị tấn công ransomware và kiểm tra môi trường làm việc để phát hiện kịp thời các dấu hiệu bị khai thác bởi lỗ hổng này. Thông báo này được đưa ra sau khi FBI cảnh báo về các đối tượng tấn công mạng đang nhằm mục tiêu tấn công vào các nhà cung cấp phần mềm trung gian và lợi dụng các công cụ hợp pháp để xâm nhập vào hệ thống thông tin của các tổ chức, doanh nghiệp.

Nếu người dùng bị lừa gọi đến số điện thoại do các đối tượng tấn công cung cấp và cài đặt một công cụ quản lý hợp pháp qua đường dẫn gửi từ email, nhóm đối tượng này có thể lợi dụng công cụ quản lý hợp pháp đó để thực hiện các tác vụ độc hại như xâm nhập vào các file cục bộ, ổ đĩa được chia sẻ qua mạng, đánh cắp dữ liệu cá nhân và tống tiền các tổ chức, doanh nghiệp.

Nguồn: https://thehackernews.com/2023/11/zero-day-alert-lace-tempest-exploits.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 **670** lỗ hổng, trong đó có 320 lỗ hổng mức Cao, 200 lỗ hổng mức Trung bình, 04 lỗ hổng mức Thấp và 146 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 06 lỗ hổng trong Linux, Nhóm 08 lỗ hổng trong Microsoft, Nhóm 10 lỗ hổng trong Google, Nhóm 189 lỗ hổng trong Wordpress, Nhóm 04 lỗ hổng trong Apache, Nhóm 33 lỗ hổng trong Samsung, Nhóm 08 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-2023-1194, CVE-2023-1476,...

- Microsoft: CVE-2023-36014, CVE-2023-36034,...

- Google: CVE-2023-32837, CVE-2023-32832,...

- Wordpress: CVE-2023-34171, CVE-2023-5454,...

- Apache: CVE-2023-47248, CVE-2023-46851,...

- Samsung: CVE-2023-43531, CVE-2023-42536,...

- IBM: CVE-2023-43018, CVE-2023-46176,...

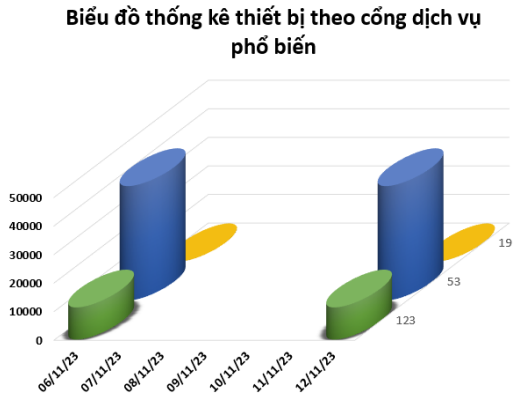
Thông tin điểm yếu, lỗ hổng

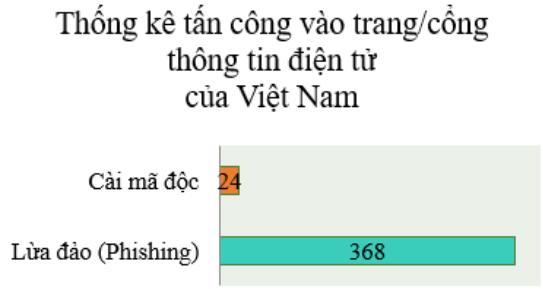
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-1194 CVE-2023-1476 CVE-2023-5090 …	Nhóm 06 lỗ hổng trong Linux cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép	Đã có thông tin xác nhận và bản vá
2	Microsoft	CVE-2023-36014 CVE-2023-36034 CVE-2023-36024 …	Nhóm 08 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Google	CVE-2023-32837 CVE-2023-32832 CVE-2023-5996 …	Nhóm 10 lỗ hổng trong Google cho phép đối tượng tấn công leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-34171 CVE-2023-5454 CVE-2022-45357 …	Nhóm 189 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗi XSS, khai thác lỗi CSRF, thực hiện SQL Injection, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép	Chưa có thông tin xác nhận và bản vá
5	Apache	CVE-2023-47248 CVE-2023-46851 CVE-2023-46819 …	Nhóm 04 lỗ hổng trong Apache cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	Samsung	CVE-2023-42531 CVE-2023-42536 CVE-2023-42537 …	Nhóm 33 lỗ hổng trong Samsung 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
7	IBM	CVE-2023-43018 CVE-2023-46176 CVE-2023-42027 …	Nhóm 08 lỗ hổng trong IBM phép đối tượng tấn công khai thác lỗi SSRF, 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

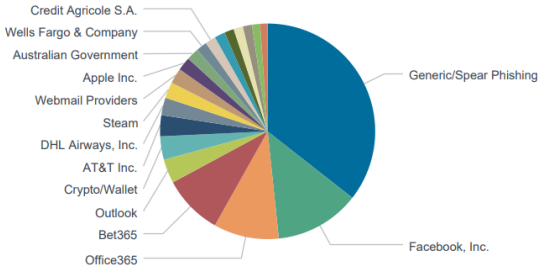
Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tán tấn công DRDoS. Trong tuần có **51.390**, (giảm so với tuần trước **55.896**) thiết bị có khả năng bị huy động và trở thành nguồn tấn công DRDoS. Các thiết bị này đang mở sử dụng các dịch vụ NTP (123), DNS (53), 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 **392** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 368 trường hợp tấn công lừa đảo (Phishing), 24 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: 13478 IP	hzmksreiuojy.ru: 229 IP
disorderstatus.ru: 4541 IP	xjpakmdcfuqe.biz: 207 IP
atomictrivia.ru: 2057 IP	xjpakmdcfuqe.com: 82 IP
amnsreiuojy.ru: 787 IP	xjpakmdcfuqe.ru: 48 IP
restlesz.su: 330 IP	xjpakmdcfuqe.in: 31 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **332** 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	pwsk88.com businesseventskp.top pwsk11.com tiki5688.shop	Website giả mạo sàn TMĐT Tiki
2	globalsellingads.com	Website giả mạo sàn TMĐT Amazon
3	vieclamlazada.vn	Website giả mạo sàn TMĐT Lazada
4	ebaayshopping.site	Website giả mạo Ebay
5	vib-tindung.online	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
6	dich-vu-the-vvip-vpb.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
7	vnpt99.com	Website giả mạo VNPT- Tập đoàn Bưu chính Viễn thông Việt Nam

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