NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 17 (24/04/2023 – 30/04/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Alloy Taurus sử dụng PingPull và một backdoor mới nhằm mục tiêu vào người dùng hệ điều hành Linux.

- **Cảnh báo:** Lỗ hổng bảo mật tồn tại trong các sản phẩm của TP-Link, Apache và Oracle.

2. Điểm yếu, lỗ hổng

- **604** 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: 233** 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

"Nhóm tấn công APT Alloy Taurus sử dụng PingPull và một backdoor mới nhằm mục tiêu vào người dùng hệ điều hành Linux"

Nhóm tấn công APT Alloy Taurus của Trung Quốc đã tung ra một biến thể mới của phần mềm độc hại PingPull để nhằm mục tiêu vào hệ điều hành Linux. Biến thể phần mềm độc hại này đang được sử dụng cùng với một backdoor khác, được biết đến với tên gọi là Sword203 trong một chiến dịch nhằm vào Nam Phi và Nepal.

Phần mềm độc hại PingPull

Biến thể mới của phần mềm độc hại PingPull là một tệp .ELF, điều này đang bị cảnh báo bởi 3 trong số 62 nhà cung cấp các phần mềm phòng chống vi-rút. Khi được thực thi, biến thể phần mềm độc hại sử dụng thư viện OpenSSL và yêu cầu HTTP POST để tương tác với các máy chủ C&C. Biến thể này cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. Trong các nghiên cứu gần đây cho thấy rằng trình xử lý lệnh được sử dụng trong phần mềm độc hại này trùng khớp với China Chopper - một web shell được sử dụng trong các cuộc tấn công chống lại các máy chủ của Microsoft Exchange.

Sword2033 backdoor

Sword2033 cũng là một tệp .ELF được phát hiện lần đầu tiên vào tháng 7 năm 2022. Tương tự như biến thể PingPull, Sword2033 được thiết kế để kết nối với cổng 8443 qua HTTPS. Biến thể này cho phép đối tượng tấn công thực thi mã độc và tải xuống các tệp từ hệ thống bị ảnh hưởng. Alloy Taurus thường tận dụng các sản phẩm hợp pháp, chẳng hạn như SoftEther VPN để vượt tránh bị phát hiện và duy trì sự bền bỉ trên hệ thống bị tấn công.

Alloy Taurus vẫn là mối đe đối với các tổ chức viễn thông, tài chính và chính phủ trên khắp Đông Nam Á, Châu Âu và Châu Phi. Việc phát hiện ra biến thể PingPull mới và việc sử dụng backdoor Sword2033 cho thấy nhóm này đang tích cực hoạt động để khởi động nhiều chiến dịch tấn công mạng trong thời gian sắp tới.

Để tránh nguy cơ bị tấn công mạng các cơ quan, tổ chức cần tăng cường kiểm tra, rà soát và sẵn sàng các phương án xử lý kịp thời khi có dấu hiệu bị cài cắm, tấn công mạng.

Nguồn: https://cyware.com/news/alloy-taurus-apt-spotted-using-pingpull-and-a-new-backdoor-to-target-linux-users-30399251

Tin tức An toàn thông tin

"Cảnh báo: Lỗ hổng bảo mật tồn tại trong các sản phẩm của TP-Link, Apache và Oracle"

Gần đây, các nhà nghiên cứu đã phát hiện ra 03 lỗ hổng bảo mật mới tồn tại trong các sản phẩm của TP-Link, Apache và Oracle.

03 lỗ hổng bảo mật mới:

- Lỗ hổng Command Injection trong TP-Link Archer AX-21 với mã khai thác CVE-2023-1389 (Điểm CVSS: 8,8). Lỗ hổng CVE-2023-1389 cho phép đối tượng tấn công thực thi mã từ xa, gây ảnh hưởng đến bộ định tuyến TP-Link Archer AX-21. Lỗ hổng này đã được các đối tượng tấn công liên quan đến botnet Mirai sử dụng kể từ ngày 11/04/2023.

- Lỗ hổng Deserialization of Untrusted Data trong Apache Log4j2 với mã khai thác CVE-2021-45046 (Điểm CVSS: 9,0). Lỗ hổng CVE-2021-45046 cho phép đối tượng tấn công thực thi mã từ xa, ảnh hưởng đến thư viện ghi nhật ký Apache Log4j2 được phát hiện vào tháng 12/2021. Hiện tại vẫn chưa rõ lỗ hổng này đang được sử dụng với mục đích nào trong thực tế, tuy nhiên các nghiên cứu gần đây đã phát hiện dấu hiệu tích cực khai thác 74 địa chỉ IP thông qua lỗ hổng CVE-2021-45046 trong 30 ngày qua. Đồng thời, các đánh giá này cũng nhắc đến cả lỗ hổng bảo mật Log4Shell (CVE-2021-44228).

- Lỗ hổng bảo mật chưa được xác định trong Oracle WebLogic Server với mã khai thác CVE-2023-21839 (điểm CVSS: 7,5) . Lỗ hổng bảo mật ở mức Cao trong Oracle WebLogic Server phiên bản 12.2.1.3.0, 12.2.1.4.0 và 14.1.1.0.0 cho phép các đối tượng tấn công không cần xác thực có quyền truy cập mạng thông qua T3 và IIOP, để xâm nhập máy chủ Oracle WebLogic nhằm thu thập thông tin dữ liệu nhạy cảm, truy cập và thực hiện các hành động trái phép trái phép. Lỗ hổng này đã được cập nhật bản vá vào tháng 01/2023.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, tổ chức cần thực hiện kiểm tra, rà soát và xử lý hệ thống bị ảnh hưởng. Tăng cường giám sát và sẵn sàng các phương án xử lý khi phát hiện có dấu hiệu bị cài cắm, khai thác, tấn công mạng.

Nguồn: https://thehackernews.com/2023/05/active-exploitation-of-tp-link-apache.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 **604** lỗ hổng, trong đó có 50 lỗ hổng mức Cao, 52 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 502 lỗ hổng chưa đánh giá. Trong đó có ít nhất 57 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 03 lỗ hổng trong Microsoft, Nhóm 13 lỗ hổng trong Linux, 01 lỗ hổng trong Google, Nhóm 21 lỗ hổng trong Wordpress, Nhóm 04 lỗ hổng trong VMware, Nhóm 05 lỗ hổng trong Solarwinds, Nhóm 17 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:

- *Microsoft: CVE-2023-21712, CVE-2023-29334,...*
- *Linux: CVE-2023-1998, CVE-2023-2006,...*
- *Google: CVE-2023-30845.*
- *Wordpress: CVE-2023-0276, CVE-2023-0418,...*
- *Vmware: CVE-2023-20869, CVE-2023-20870,...*
- *Solarwinds: CVE-2023-23837, CVE-2023-23838,...*
- *IBM: CVE-2023-27556, CVE-2023-27557,...*

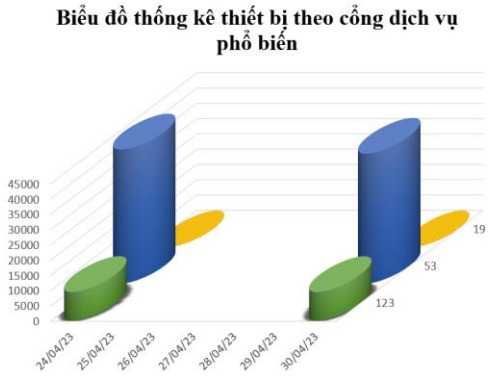
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-21712 CVE-2023-29334 CVE-2023-30846 …	Nhóm 03 lỗ hổng trong Microsoft (Edge,…) cho phép đối tượng tấn công thực thi mã từ xa, rò rỉ thông tin dữ liệu, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-1998 CVE-2023-2006 CVE-2023-2007 …	Nhóm 13 lỗ hổng trong Linux (kernel, DPT I2O) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, thực thi mã tùy ý, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2023-30845	01 lỗ hổng trong Google (ESPv2) 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
4	Wordpress	CVE-2023-0276 CVE-2023-0388 CVE-2023-0418 …	Nhóm 21 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công CSRF, tấn công XSS, SQL injection, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	VMware	CVE-2023-20869 CVE-2023-20870 CVE-2023-20871 …	Nhóm 04 lỗ hổng trong VMware (fusion,...) cho phép đối tượng tấn công thực hiện nâng cao các đặc quyền để có quyền truy cập root vào hệ điều hành máy chủ, thực thi lỗ hổng đọc/ghi ngoài giới hạn, lỗ hổng tràn bộ đệm.	Chưa có thông tin xác nhận và bản vá
6	Solarwinds	CVE-2023-23838 CVE-2023-23837 CVE-2023-23839 …	Nhóm 05 lỗ hổng trong Solarwinds 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-2023-27557 CVE-2023-27556 CVE-2023-27559 …	Nhóm 17 lỗ hổng trong IBM phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, chèn JavaScript tùy ý, thu thập thông tin dữ liệu nhạy cảm, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

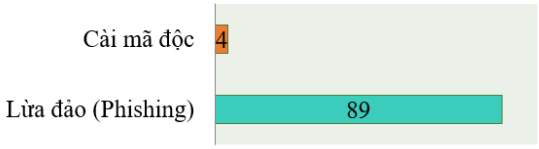
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **51,953** (giảm so với tuần trước **53,360**) 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.

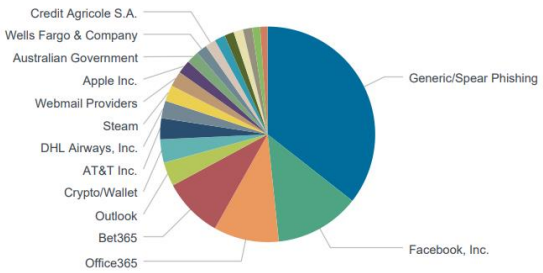


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 93 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 89 trường hợp tấn công lừa đảo (Phishing), 04 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: 12532 IP	xjpakmdcfuqe.ru:240 IP
disorderstatus.ru: 5289 IP	xjpakmdcfuqe.in:304 IP
atomictrivia.ru: 2531 IP	restlesz.su: 310 IP
xjpakmdcfuqe.biz: 411 IP	amnsreiuojy.ru: 853 IP
xjpakmdcfuqe.com: 299 IP	hzmksreiuojy.ru: 46 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **233** 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	lottefinance.vay10s.com	Website giả mạo LOTTE
2	vn268.com	Website giả mạo sàn TMĐT Tiki
3	senopaee.com	Website giả mạo sàn TMĐT Shopee
4	vp7811.com somnio-evolve.com 888b.biz hdsaison-vn.com thuongmaidientuquocte.com	Website giả mạo, lừa đảo

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