NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 19 (08/5/2023 – 14/5/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công APT của Iran tham gia cuộc tấn công nhằm vào Papercut.

- **Cảnh báo:** 9 loại ransomware từ mã nguồn Babuk nhằm vào máy chủ VMware ESXi.

2. Điểm yếu, lỗ hổng

- **890** 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: 368** 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 của Iran tham gia cuộc tấn công nhằm vào Papercut"

Gần đây, các nhà nghiên cứu bảo mật đã phát hiện ra một số nhóm APT mới có liên quan đến Iran như: Mango Sandstorm (hay còn được gọi là Mercury) và Mint Sandstorm (hay còn được biết đến với tên gọi APT35). Các nhóm này đã tham gia cuộc tấn công nhằm vào việc khai thác lỗ hổng nghiêm trọng trong phần mềm quản lý in PaperCut.

Theo các nghiên cứu của Microsoft, cả nhóm Mango Sandstorm và nhóm Mint Sandstorm đều đang tích cực khai thác lỗ hổng CVE-2023-27350 để có được quyền truy cập ban đầu. Lỗ hổng bảo mật CVE-2023-27350 (điểm CVSS: 9,8) có mức ảnh hưởng Nghiêm trọng liên quan đến bản cài đặt PaperCut MF/NG phiên bản 8.o trở lên. Lỗ hổng này cho phép các đối tượng tấn công không cần xác thực có thể thực thi mã tùy ý với các đặc quyền của hệ thống.

PaperCut là một phần mềm quản lý in với hơn 100 triệu người dùng của 70.000 doanh nghiệp bao gồm các công ty lớn, tổ chức nhà nước, giáo dục trên toàn thế giới. Điều này cho thấy nếu việc khai thác thành công lỗ hổng có thể gây ảnh hưởng rất nghiêm trọng đến hệ thống của nhiều cơ quan, tổ chức.

Sau vài tuần diễn ra cuộc tấn công Microsoft đã xác nhận có sự tham gia của nhóm tấn công Lace Tempest, đây là nhóm APT hoạt động chung với các nhóm tấn công FIN11 và TA505 có liên quan đến ransomware Clop. Ngoài ra, một số cuộc xâm nhập đã dẫn đến các cuộc tấn công ransomware LockBit.

Để giảm thiểu nguy cơ bị tấn công mạng các cơ quan, tổ chức sử dụng phần mềm PaperCut nên cập nhật lên các phiên bản 20.1.7, 21.2.11 và 22.0.9 trở lên.

Nguồn:
https://www.bleepingcomputer.com/news/security/microsoft-iranian-hacking-groups-join-papercut-attack-spree/?&web_view=true

Tin tức An toàn thông tin

"Cảnh báo: 9 loại ransomware từ mã nguồn Babuk nhằm vào máy chủ VMware ESXi"

Tháng 09/2021, nhiều đối tượng tấn công đã lợi dụng sự rò rỉ ransomware Babuk (còn được biết đến là Babak hoặc Babyk) để tạo ra 9 loại ransomware khác nhau, có khả năng tấn công vào các máy chủ VNware ESXi.

Theo các nhà nghiên cứu, biến thể này xuất hiện từ năm 2022 cho thấy xu hướng sử dụng mã nguồn Babyk ngày càng tăng. Mã nguồn bị rò rỉ của Babyk cho phép đối tượng tấn công vào hệ thống của Linux ngay cả khi chúng không có khả năng tự phát triển các chủng ransomware của riêng mình. Một số đối tượng tấn công nhằm vào các máy ảo VMware ESXi, đã có ít nhất 3 chủng ransomware khác nhau là Cylance, Rorschach (hay còn được biết là BabLock) và RTM Locker – đã xuất hiện kể từ đầu năm 2023 dựa trên mã nguồn Babuk bị rò rỉ.

Các nhà nghiên cứu bảo mật đã phát hiện ra mã nguồn trùng khớp giữa bộ khóa của Babuk và ESXi được quy trách nhiệm cho 2 nhóm APT là Conti và Revil. Các dòng ransomware khác đã chuyển các tính năng từ Babuk sang mã tương ứng của chúng bao gồm LOCK4, DATAF, Mario, Play và Babuk 2023 (hay còn được biết đến là XVGV) ransomware.

Các cuộc tấn công có xu hướng kết hợp ransomware Royal do cựu thành viên nhóm Conti tạo ra, để mở rộng bộ công cụ tấn công bằng biến thể ELF nhằm vào hệ thống ESXi và Linux.

Kể từ khi xuất hiện vào tháng 09/2022, ransomware Royal đã nhằm mục tiêu vào hơn 157 tổ chức ở Hoa Kỳ, Canada và Đức. Các cuộc tấn công bằng ransomware Royal bắt nguồn từ các cuộc gọi lừa đảo, lây nhiễm BATLOADER hoặc thông tin đăng nhập bị xâm phạm, sau đó bị lạm dụng để cài cắm Cobalt Strike Beacon nhằm thực thi ransomware.

Để đảm bảo an toàn thông tin cho hệ thống của các cơ quan, tổ chức, doanh nghiệp nên thực hiện kiểm tra, rà soát thường xuyên, sẵn sàng các phương án xử lý để tránh các nguy cơ bị tấn công mạng.

Nguồn: https://thehackernews.com/2023/05/babuk-source-code-sparks-9-new.html?&web_view=true

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 **890** lỗ hổng, trong đó có 143 lỗ hổng mức Cao, 182 lỗ hổng mức Trung bình, 08 lỗ hổng mức Thấp và 557 lỗ hổng chưa đánh giá. Trong đó có ít nhất 116 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 35 lỗ hổng trong Microsoft, Nhóm 65 lỗ hổng trong Apple, Nhóm 48 lỗ hổng trong Google, Nhóm 54 lỗ hổng trong Wordpress, Nhóm 93 lỗ hổng trong Intel, Nhóm 08 lỗ hổng trong HP, 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-2023-24898, CVE-2023-24901,...*
- *Apple: CVE-2023-27929, CVE-2023-27931,…*
- *Google CVE-2022-48243, CVE-2022-48244,...*
- *Wordpress:CVE-2022-46817, CVE-2022-46819,...*
- *Intel: CVE-2022-41690, CVE-2022-41693,...*
- *HP: CVE-2023-22779, CVE-2023-22781,...*
- *IBM: CVE-2020-4914, CVE-2022-43877,...*

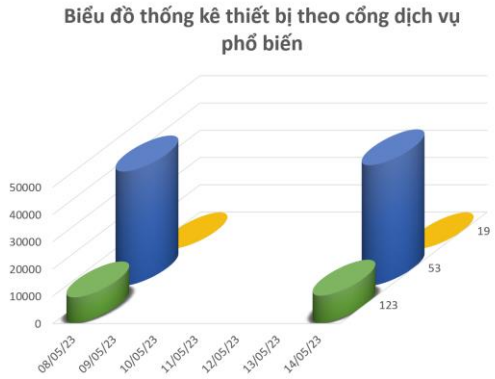
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-24898 CVE-2023-24939 CVE-2023-24901 ...	Nhóm 35 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass), thực hiện leo thang đặc quyền, 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	Apple	CVE-2023-27929 CVE-2023-27931 CVE-2023-27932 …	Nhóm 65 lỗ hổng trong Apple (macOS, Iphone,…) cho phép đối tượng tấn công thu thập thông tin dữ liệu, đọc các tệp tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2022-48243 CVE-2022-48244 CVE-2022-48245 …	Nhóm 48 lỗ hổng trong Google (Android) cho phép đối tượng tấn công thu thập thông tin dữ liệu, thực hiện leo thang đặc quyền, 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-2022-46817 CVE-2022-46819 CVE-2022-4686 …	Nhóm 54 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện 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	Intel	CVE-2022-41690 CVE-2022-41693 CVE-2022-41699 …	Nhóm 93 lỗ hổng trong Intel cho phép đối tượng tấn công thực hiện leo thang đặc quyền, 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
6	HP	CVE-2023-22779 CVE-2023-22780 CVE-2023-22781 …	Nhóm 08 lỗ hổng trong HP cho phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2020-4914 CVE-2022-38707 CVE-2022-43877 …	Nhóm 17 lỗ hổng trong IBM phép đối tượng tấn công thu thập thông tin đăng nhập, 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

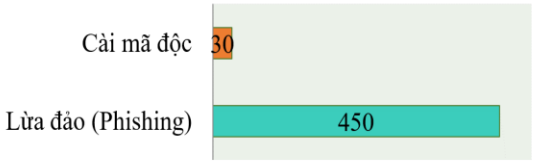
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **54,292** (tăng so với tuần trước **51,359**) 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.

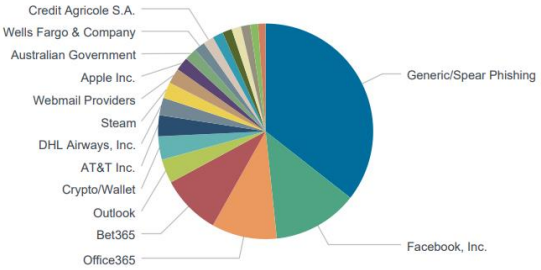


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 480 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 450 trường hợp tấn công lừa đảo (Phishing), 30 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: 12713 IP	xjpakmdcfuqe.ru:231 IP
disorderstatus.ru: 6412 IP	xjpakmdcfuqe.in:300 IP
atomictrivia.ru: 3158 IP	restlesz.su: 304 IP
xjpakmdcfuqe.biz: 322 IP	amnsreiuojy.ru: 678 IP
xjpakmdcfuqe.com: 256 IP	hzmksreiuojy.ru: 30 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **368** 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	mcfa11.com shek66.com	Website giả mạo sàn TMĐT Tiki
2	9smomo.com	Website giả mạo Ví điện tử Momo
3	datgrabsaigon.com	Giả mạo website Grab
4	ebayshopnet.com	Giả mạo website Ebay
5	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 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