NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 43 (23/10/2023 – 29/10/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Tortoiseshell khởi động chiến dịch tấn công mới bằng mã độc IMAPLoader.

- **Cảnh báo:** VMWare phát hành bản vá cho lỗ hổng RCE nghiêm trọng trên vCenter Server.

2. Điểm yếu, lỗ hổng

- **750** 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: 287** 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 Tortoiseshell khởi động chiến dịch tấn công mới bằng mã độc IMAPLoader"

Nhóm APT Tortoiseshell vừa thực hiện một chiến dịch tấn công sử dụng mã độc có tên IMAPLoader thông qua hình thức watering hole. Đây là một loại mã độc chạy trên .NET, có khả năng lấy dấu vân tay của người dùng trên hệ thống nhiễm mã độc bằng cách biến các tiện ích có sẵn trên hệ điều hành Windows thành bộ tải cho các phần mềm độc hại (payload). Mã độc này sử dụng email để liên lạc với máy chủ C&C và có khả năng thực thi các phần mềm độc hại được trích xuất từ các tệp đính kèm trong email bằng cách tạo các dịch vụ mới trên thiết bị của nạn nhân.

Nhóm APT Tortoiseshell, còn được gọi là Crimson Sandstorm, Curium, Imperial Kitten, TA456 và Yellow Liderc, có liên quan đến IRGC (Quân đội Cách mạng Hồi giáo Iran) và đã xuất hiện từ năm 2018. Vào tháng 05/2023, nhóm này đã bị phát hiện khi xâm nhập vào 8 trang web của các doanh nghiệp trong lĩnh vực vận chuyển, hậu cần và tài chính tại Israel.

Trong khoảng thời gian từ năm 2022 đến năm 2023, nhóm APT Tortoiseshell đã tiến hành nhiều chiến dịch tấn công bằng cách nhúng mã JavaScript độc hại vào các trang web chính thống sau khi xâm nhập. Mục tiêu là thu thập thông tin về người dùng đã truy cập trang web, bao gồm thông tin về vị trí, thiết bị sử dụng và thời gian truy cập. Các ngành chính bị ảnh hưởng bởi cuộc tấn công này bao gồm ngành hàng hải, vận tải và hậu cần tại khu vực Địa Trung Hải. Trong một số trường hợp, khi xác định được rằng mục tiêu có giá trị thì Tortoiseshell mới tiếp tục triển khai mã độc IMAPLoader để thực hiện các cuộc tấn công cụ thể hơn.

Nguồn: https://thehackernews.com/2023/10/iranian-group-tortoiseshell-launches.html

Nhóm APT Tortoiseshell sử dụng mã độc IMAPLoader như một phiên bản thay thế cho mã độc IMAP ban đầu viết bằng Python. IMAPLoader đóng vai trò như một bộ tải cho payload giai đoạn kế tiếp bằng việc truy vấn vào các tài khoản email IMAP cố định, cụ thể hơn là quét thư mục "Recive" để tải xuống các tệp thực thi từ phần đính kèm trên email.

Trong một số các chiến dịch tấn công khác, nhóm APT Tortoiseshell sử dụng tài liệu giả mạo trên Microsoft Excel như một điểm khởi đầu để tiếp tục triển khai nhiều giai đoạn tấn công khác nhằm tải về và thực thi mã độc IMAPLoader. Điều này cho thấy Tortoiseshell đang áp dụng nhiều chiến thuật và kỹ thuật khác nhau để đạt được mục tiêu. Ngoài ra, Tortoiseshell còn tạo ra một số trang web giả mạo trong lĩnh vực du lịch và y tế ở Châu u nhằm thu thập trái phép thông tin đăng nhập người dùng bằng các trang giả mạo của Microsoft.

Theo nhận định từ các chuyên gia bảo mật, nhóm APT Tortoiseshell vẫn tiếp tục mà một mối đe dọa tiềm ẩn đối với các doanh nghiệp trên nhiều quốc gia khác nhau trong các lĩnh vực như hàng hải, vận chuyển và hậu cần ở Địa Trung Hải; ngành hạt nhân, hàng không vũ trụ, quốc phòng tại Mỹ và Châu u; các nhà cung cấp dịch vụ được quản lý Công nghệ thông tin tại Trung Đông.

Tin tức An toàn thông tin

"Cảnh báo: VMWare phát hành bản vá cho lỗ hổng RCE nghiêm trọng trên vCenter Server"

VMWare vừa phát hành bản cập nhật bảo mật nhằm khắc phục một lỗ hổng Nghiêm trọng trên vCenter Server, cho phép đối tượng tấn công thực thi mã từ xa trên các hệ thống bị ảnh hưởng.

Lỗ hổng Nghiêm trọng có mã CVE-2023-34048 (Điểm CVSS: 9.8) là một lỗ hổng ghi ngoài phạm vi (out-of-bounds write) trong việc thực hiện giao thức DCE/RPC. Cụ thể, đối tượng tấn công có quyền truy cập mạng vào vCenter Server để gây ra một lỗ hổng ghi ngoài phạm vi, qua đó dẫn đến việc thực thi mã từ xa.

VMWare thông báo rằng hiện không có biện pháp tạm thời nào để khắc phục lỗ hổng này, bởi vậy, người dùng cần phải cập nhật bản vá cho các phiên bản bị ảnh hưởng, bao gồm:

- VMware vCenter Server 8.0 (8.0U1d hoặc 8.0U2)
- VMware vCenter Server 7.0 (7.0U3o)
- VMware Cloud Foundation 5.x và 4.x

Hiện tại, VMWare đang phát triển một bản vá cho vCenter Server 6.7U3, 6.5U3 và VCF 3.x. Bản vá này cũng đã giải quyết lỗ hổng CVE-2023-34056 (Điểm CVSS: 4.3), một lỗ hổng gây lộ lọt thông tin một phần ảnh hưởng đến vCenter Server, cho phép người tấn công truy cập vào dữ liệu mà không cần quyền của quản trị viên.

Để bảo vệ thông tin trên hệ thống của cơ quan và doanh nghiệp, khuyến nghị các đơn vị cần cập nhật bản vá này sớm nhất có thể để tránh nguy cơ xảy ra sự cố bảo mật.

Nguồn: https://thehackernews.com/2023/10/act-now-vmware-releases-patch-for.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 **750** lỗ hổng, trong đó có 143 lỗ hổng mức Cao, 118 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 489 lỗ hổng chưa đánh giá. Trong đó có ít nhất 170 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 Linux, Nhóm 39 lỗ hổng trong Apple, Nhóm 07 lỗ hổng trong Apache, Nhóm 158 lỗ hổng trong Wordpress, Nhóm 08 lỗ hổng trong VMware, Nhóm 20 lỗ hổng trong Google, Nhóm 11 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-2023-5633, CVE-2023-46813,...

- Apple: CVE-2023-32359, CVE-2023-40445,...

- Apache: CVE-2023-31122, CVE-2023-46288,...

- Wordpress: CVE-2023-4668, CVE-2023-3342,...

- VMware: CVE-2023-34045, CVE-2023-34046,...

- Google: CVE-2023-40116, CVE-2023-40117,...

- IBM: CVE-2023-38275, CVE-2023-38276,...

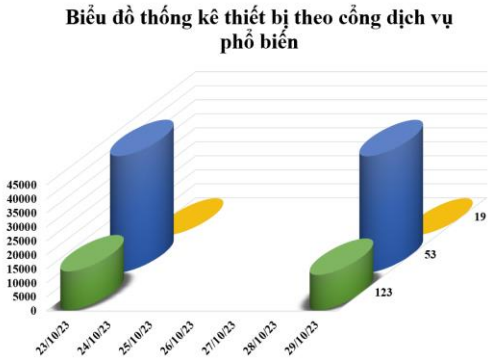
Thông tin điểm yếu, lỗ hổng

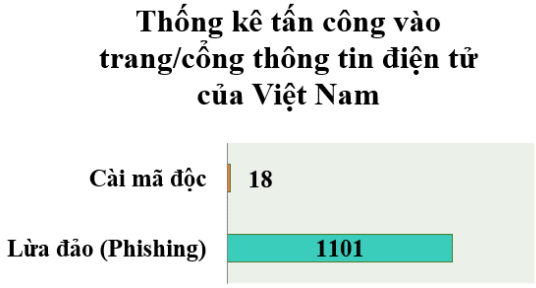
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-5633 CVE-2023-46813 CVE-2023-5717	Nhóm 03 lỗ hổng trong Linux cho phép đối tượng tấn công leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Apple	CVE-2023-32359 CVE-2023-40445 CVE-2023-40401 …	Nhóm 39 lỗ hổng trong Apple cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Apache	CVE-2023-31122 CVE-2023-46288 CVE-2023-44483 …	Nhóm 07 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
4	Wordpress	CVE-2023-4668 CVE-2022-3342 CVE-2020-36714 …	Nhóm 158 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công SQL Injection, thực thi mã từ xa, khai thác lỗi CSRF, khai thác lỗi XSS.	Đã có thông tin xác nhận và bản vá
5	VMware	CVE-2023-34045 CVE-2023-34046 CVE-2023-34044 …	Nhóm 08 lỗ hổng trong VMware cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Google	CVE-2023-40116 CVE-2023-40117 CVE-2023-40120 …	Nhóm 20 lỗ hổng trong Google cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công SQL Injection, thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
7	IBM	CVE-2023-38275 CVE-2023-38276 CVE-2022-22466 …	Nhóm 11 lỗ hổng trong IBM phép đối tượng tấn công 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 **54.241**, (giảm so với tuần trước **55.542**) 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.



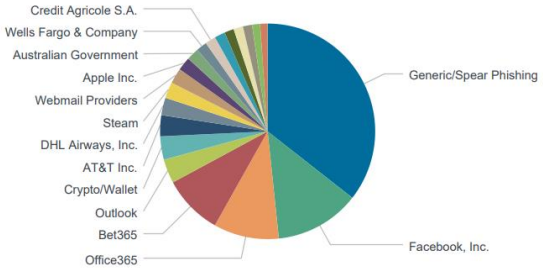


Tấn công Web

Trong tuần, có **1119** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 1101 trường hợp tấn công lừa đảo (Phishing), 18 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: 17674 IP	hzmksreiuojy.ru: 277 IP
disorderstatus.ru: 8027 IP	xjpakmdcfuqe.biz: 285 IP
atomictrivia.ru: 3765 IP	xjpakmdcfuqe.com: 168 IP
amnsreiuojy.ru: 957 IP	xjpakmdcfuqe.ru: 106 IP
restlesz.su: 325 IP	xjpakmdcfuqe.in: 78 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **287** 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	thevip-khcn-vpb.com nang-han-muc-vip-vpbank.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
2	hpy88yu.com	Website giả mạo sàn TMĐT Lazada
3	hotrovayvoneximbak.com	Website giả mạo Ngân Hàng TMCP Xuất Nhập Khẩu Việt Nam
4	shop-ama-zon.net	Website giả mạo Amazon
5	bigc.net.vn	Website giả mạo BigC 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 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