NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 30 (24/7/2023 – 30/07/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT BlueBravo triển khai backdoor GraphicalProton nhằm vào các tổ chức tại Châu Âu.

- **Cảnh báo:** Ransomware ALPHV bổ sung API rò rỉ dữ liệu trong chiến thuật tống tiền mới.

2. Điểm yếu, lỗ hổng

- **473** 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: 355** 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 BlueBravo triển khai backdoor GraphicalProton nhằm vào các tổ chức tại Châu Âu"

Gần đây, nhóm tấn công APT BlueBravo đã bị phát hiện khi tấn công nhằm vào các tổ chức ngoại giao tại Đông Âu. Mục tiêu của nhóm này là triển khai một backdoor mới mang tên GraphicalProton.

Các hoạt động của BlueBravo đã được quan sát từ tháng 3 đến tháng 5 năm 2023, điểm nổi bật trong chiến dịch tấn công của BlueBravo là việc sử dụng các dịch vụ Internet hợp pháp (LIS) để che giấu các máy chủ C&C.

Nhóm tấn công BlueBravo, còn được gọi là APT29, Cloaked Ursa và Midnight Blizzard (tên cũ Nobelium), là một nhóm tấn công có liên quan đến Cơ quan Tình báo Nước ngoài của Nga (SVR). Trước đây, nhóm này đã sử dụng nhiều dịch vụ như Dropbox, Firebase, Google Drive, Notion và Trello để che giấu việc kết nối với các máy tính bị nhiễm mã độc. Hành vi này cho thấy tính đa dạng và sự tiến hóa liên tục trong cách thức thực hiện các cuộc tấn công của họ. Việc nhằm vào các tổ chức trong lĩnh vực ngoại giao đánh dấu sự nỗ lực của BlueBravo trong việc đa dạng hóa công cụ và mở rộng danh mục dịch vụ bị tấn công.

Đánh giá kỹ thuật cho thấy GraphicalProton hoạt động như một "loader" - một loại mã độc phụ thuộc vào một "payload" khác để thực hiện các tác vụ khai thác tiếp theo. Nó được ẩn trong một file ISO hoặc ZIP và phát tán thông qua email lừa đảo có nội dung về các phương tiện giao thông. Trong file ISO chứa các file .LNK được ngụy trang thành ảnh dạng .PNG của một chiếc xe BMW đang được rao bán. Khi người dùng bấm vào ảnh, GraphicalProton sẽ tự động triển khai để tiến hành các bước khai thác tiếp theo. Điều này được thực hiện bằng cách sử dụng Microsoft OneDrive làm máy chủ C&C và định kỳ chọn một thư mục trong dịch vụ lưu trữ này để tải thêm các payload bổ trợ.

Có lẽ một trong những mục tiêu chiến lược trong chiến dịch tấn công của BlueBravo có liên quan đến sự quan tâm của chính phủ Nga đối với dữ liệu trong cuộc chiến tại Ukraine. Trước tình hình địa chính trị phức tạp tại châu u và xung đột ở Ukraine, BlueBravo có thể sẽ tiếp tục tấn công vào các cơ quan ngoại giao cùng các mục tiêu quan trọng khác. Do đó, các tổ chức cần tăng cường bảo mật và nâng cao nhận thức an toàn thông tin để bảo đảm an toàn hệ thống thông tin một cách tốt nhất.

Nguồn:
https://thehackernews.com/2023/07/bluebravo-deploys-graphicalproton.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Ransomware ALPHV bổ sung API rò rỉ dữ liệu trong chiến thuật tống tiền mới"

Ransomware ALPHV, hay còn được gọi là BlackCat, đang cố gắng tạo áp lực để ép buộc các nạn nhân trả tiền chuộc bằng cách cung cấp một API cho trang web gây rò rỉ dữ liệu, nhằm tăng khả năng hiển thị cho các cuộc tấn công. Hành động này diễn ra ngay sau khi nhóm BlackCat tấn công vào Estée Lauder, tuy nhiên, công ty mỹ phẩm này đã hoàn toàn phớt lờ mọi nỗ lực của nhóm tấn công trong việc thương lượng trả tiền chuộc.

Lệnh gọi API và Python crawler

Các nhà nghiên cứu cho rằng nhóm ALPHV/BlackCat đã thêm một hướng dẫn sử dụng API vào trang web gây rò rỉ dữ liệu để thu thập thông tin về các nạn nhân. Những nội dung này đã tồn tại trong vài tháng nhưng bị giới hạn quyền truy cập.

Nhóm tấn công cung cấp lệnh gọi API để thu thập thông tin về nạn nhân và cập nhật nó trên trang web rò rỉ của nhóm. Ngoài ra, nhóm BlackCat cung cấp một crawler viết bằng Python để hỗ trợ thu thập thông tin mới nhất từ trang web rò rỉ dữ liệu.

Số lượng nạn nhân trả tiền chuộc giảm đi

Một trong những lý do có thể khiến nhóm phát hành API là vì ngày càng ít nạn nhân chịu chi trả tiền chuộc đề ra bởi nhóm này. Trong báo cáo của các chuyên gia bảo mật, tỷ lệ nạn nhân chịu thiệt hại từ các cuộc tấn công ransomware đã giảm xuống 34% trong quý 2 năm nay.

Tuy nhiên, vẫn tồn tại những nhóm tấn công tiếp tục kiếm lời bằng cách tập trung vào các chiến dịch nhằm vào chuỗi cung ứng, ảnh hưởng đến nhiều tổ chức. Ví dụ, ransomware Clop được ước tính đã thu về ít nhất 75 triệu đô la từ chiến dịch đánh cắp dữ liệu MOVEit của nhóm này. Chiến dịch Clop sử dụng lỗ hổng zero-day trong nền tảng chuyển file bảo mật "MOVEit Transfer" và được cho rằng đã ảnh hưởng đến hàng trăm công ty, trong đó có Estée Lauder cũng bị tấn công bởi ALPHV/BlackCat.

Theo chuyên gia, với ít nạn nhân trả tiền chuộc hơn, các nhóm tấn công ransomware đang phải tìm kiếm những biện pháp mới để gia tăng sức ép tống tiền các nạn nhân.

Nguồn: https://www.bleepingcomputer.com/news/security/alphv-ransomware-adds-data-leak-api-in-new-extortion-strategy/?&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 **473** lỗ hổng, trong đó có 44 lỗ hổng mức Cao, 39 lỗ hổng mức Trung bình, 02 lỗ hổng mức Thấp và 388 lỗ hổng chưa đánh giá. Trong đó có ít nhất 71 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 19 lỗ hổng trong Linux, Nhóm 35 lỗ hổng trong Google, Nhóm 67 lỗ hổng trong Wordpress, Nhóm 05 lỗ hổng trong Nokia, Nhóm 01 lỗ hổng trong Github, Nhóm 02 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-2023-38187, CVE-2023-36887,...*
- *Linux: CVE-2023-38409, CVE-2023-38426,...*
- *Google: CVE-2021-4316, CVE-2021-4317,...*
- *Wordpress: CVE-2023-2761, CVE-2023-3248,...*
- *Nokia: CVE-2022-28863, CVE-2022-28864,...*
- *Github: CVE-2023-23764.*
- *IBM: CVE-2023-25929, CVE-2023-28530.*

Thông tin điểm yếu, lỗ hổng

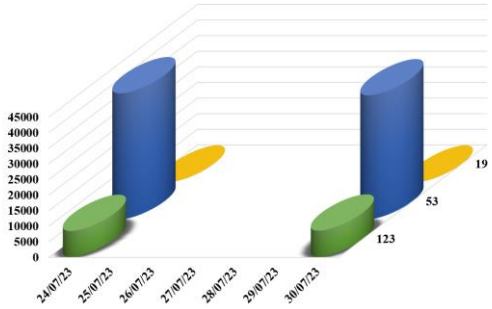
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-38187 CVE-2023-36887 CVE-2023-35392	Nhóm 03 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện leo thang đặc quyền, thực thi mã từ xa, thực hiện lỗi Spoofing, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2023-38409 CVE-2023-38426 CVE-2023-38427 …	Nhóm 19 lỗ hổng trong Linux (kernel) 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
3	Google	CVE-2021-4317 CVE-2021-4316 CVE-2021-4317 …	Nhóm 35 lỗ hổng trong Google 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-2023-3344 CVE-2023-2761 CVE-2023-3248 …	Nhóm 29 lỗ hổng trong Wordpress 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
5	Nokia	CVE-2022-28864 CVE-2022-28863 CVE-2022-28865 …	Nhóm 05 lỗ hổng trong Nokia 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
6	Github	CVE-2023-23764	Nhóm 01 lỗ hổng trong Github 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-2023-28530 CVE-2023-25929	Nhóm 02 lỗ hổng trong IBM 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

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

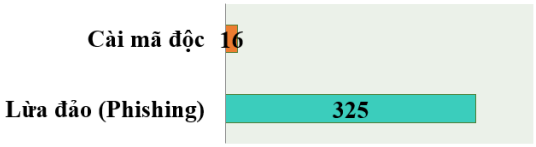
Tấn công DRDoS

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 **48.145**, (giảm so với tuần trước **48.688**) 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.

Biểu đồ thống kê thiết bị theo cổng dịch vụ phổ biến

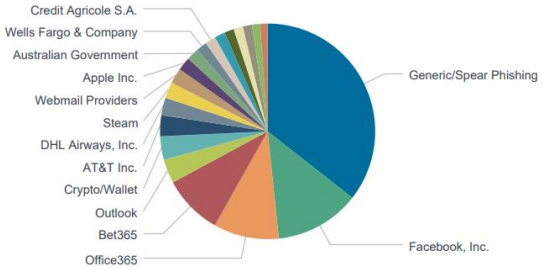


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 341 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 325trường hợp tấn công lừa đảo (Phishing), 16 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: 10784 IP	xjpakmdcfuqe.ru:60 IP
disorderstatus.ru: 3524 IP	xjpakmdcfuqe.in: 54 IP
atomictrivia.ru: 1578 IP	restlesz.su: 269 IP
xjpakmdcfuqe.biz: 257 IP	amnsreiuojy.ru: 391 IP
xjpakmdcfuqe.com: 115 IP	hzmksreiuojy.ru: 43 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **355** 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	eqav77.com amqa11.com eqav33.com	Website giả mạo sàn TMĐT Tiki
2	shoopaean.com	Website giả mạo sàn TMĐT Shopee
3	dichvucongbaohiemxahoi.com dangkyhosotructuyen2023.com handico.vaytienmat-nhanh24h.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