NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 21 (22/5/2023 – 28/5/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công APT Agrius của Iran sử dụng ransomware Moneybird nhằm mục tiêu vào các tổ chức của Israel.

- **Cảnh báo:** Phát hiện lỗ hổng gây rò rỉ dữ liệu trong Cloud SQL của Google Cloud.

2. Điểm yếu, lỗ hổng

- **514** 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: 285** 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

Tin tức An toàn thông tin

"Nhóm tấn công APT Agrius của Iran sử dụng ransomware Moneybird nhằm mục tiêu vào các tổ chức của Israel"

Nhóm tấn công APT Agrius (còn được biết đến với tên Pink Sandstorm hay Americium) của Iran đã hoạt động kể từ tháng 12/2020. Mới đây, nhóm Agrius đã triển khai ransomware mới Moneybird trong các cuộc tấn công nhằm mục tiêu vào các tổ chức của Israel.

Tháng 12/2022, Agrius bị cáo buộc đã thực hiện các cuộc tấn công nhằm vào các ngành công nghiệp mũi nhọn ở Nam Phi, Israel và Hồng Kông.

Các cuộc tấn công của Agrius liên quan đến việc sử dụng ransomware Apostle và Fantasy dựa trên nền tảng lập trình .NET. Tuy nhiên, ransomware Moneybird mới đây được lập trình bằng C++.

Mã độc khai thác các lỗ hổng trong máy chủ web nhằm triển khai Web Shell ASPXSpy. Các Web Shell này được sử dụng làm đường dẫn cung cấp các công cụ nhằm xâm nhập, chọn lọc và thu thập thông tin đăng nhập trái phép. Sau khi máy chủ bị ransomware Moneybird xâm nhập sẽ thực hiện mã hóa các tệp quan trọng trong thư mục F:\User Shares sau đó nhóm này sẽ đưa ra đe dọa và yêu cầu tiền chuộc trong vòng 24 giờ hoặc những thông tin bị đánh cắp sẽ rò rỉ ra ngoài.

Agrius không phải là nhóm tấn công APT duy nhất được nhà nước Iran tài trợ tham gia các hoạt động nhằm vào Israel.

Các cuộc tấn công mới của Agrius có thể sử dụng nhiều ransomware khác cho các chiến dịch lừa đảo và tống tiền. Các cá nhân, tổ chức cần cẩn thận trước khi nhấp chuột vào bất kỳ trang web nào. Đồng thời tăng cường nâng cao hệ thống bảo mật của mạng nội bộ tổ chức, doanh nghiệp.

Nguồn: https://thehackernews.com/2023/05/iranian-agrius-hackers-targeting.html?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện lỗ hổng gây rò rỉ dữ liệu trong Cloud SQL của Google Cloud"

Lỗ hổng bảo mật mới được phát hiện trong Cloud SQL được lưu trữ trên Google Cloud Platform GCP cho phép đối tượng tấn công thực hiện leo thang đặc quyền, truy cập vào dữ liệu GCP nội bộ và đánh cắp các dữ liệu nhạy cảm như tên tài khoản, mật khẩu, các file dữ liệu của người dùng.

Cloud SQL là dịch vụ cơ sở dữ liệu được quản lý toàn diện giúp người dùng dễ dàng thiết lập, duy trì, quản lý và quản trị cơ sở dữ liệu của mình trên nền tảng đám mây của Google, được xây dựng dựa trên cơ sở dữ liệu của MySQL, PostgreSQL và SQL Server dành cho các ứng dụng Cloud-Based.

Các cuộc tấn công lợi dụng lỗ hổng trong lớp bảo mật của nền tảng đám mây được liên kết với SQL Server nhằm nâng cao đặc quyền từ người dùng lên quản trị viên để thực hiện kiểm soát hoàn toàn máy chủ. Đối tượng tấn công có thể truy cập vào toàn bộ tệp được lưu trữ trên hệ thống, sao chép các tệp và đánh cắp mật khẩu, điều này đóng vai trò như một bước đệm cho các cuộc tấn công kế tiếp.

Tháng 4/2023, Google đã khắc phục lỗ hổng này và công bố tính năng API của giao thức Automated Certificate Management Environment – ACME cho người dùng Google Cloud để tự động lấy và gia hạn chứng chỉ Transport Layer Security (TLS) miễn phí.

Để giảm thiểu nguy cơ bị tấn công mạng thì các cơ quan, tổ chức cần thường xuyên cập nhập bản vá, đồng thời tăng cường lớp bảo mật cho mạng nội bộ và kiểm tra kỹ các trang web trước khi thực hiện truy cập.

Nguồn: https://thehackernews.com/2023/05/severe-flaw-in-google-clouds-cloud-sql.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 **514** lỗ hổng, trong đó có 115 lỗ hổng mức Cao, 52 lỗ hổng mức Trung bình, 02 lỗ hổng mức Thấp và 345 lỗ hổng chưa đánh giá. Trong đó có ít nhất 74 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 04 lỗ hổng trong Dell, Nhóm 06 lỗ hổng trong Linux, Nhóm 10 lỗ hổng trong Apache, Nhóm 73 lỗ hổng trong Wordpress, Nhóm 19 lỗ hổng trong Huawei, Nhóm 03 lỗ hổng trong Samsung Mobile, Nhóm 07 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:

- Dell: CVE-2023-23693, CVE-2023-23694,...

- Linux: CVE-2020-36694, CVE-2023-33250,…

- Apache: CVE-2023-28709, CVE-2023-31058,...

- Wordpress: CVE-2022-41635, CVE-2022-41987,...

- Apache: CVE-2023-28709, CVE-2023-31058,...

- Samsung Mobile: CVE-2023-21514, CVE-2023-21515,...

- IBM: CVE-2023-22878, CVE-2023-28514,...

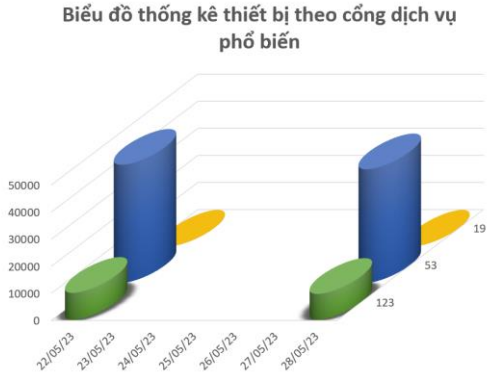
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Dell	CVE-2023-23693 CVE-2023-23694 CVE-2023-25537 ...	Nhóm 04 lỗ hổng trong Dell cho phép đối tượng tấn công thực hiện tấn công thực thi mã tùy ý, thực hiện leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2020-36694 CVE-2023-33250 CVE-2023-33288 …	Nhóm 06 lỗ hổng trong Linux (kernel) 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
3	Apache	CVE-2023-28709 CVE-2023-31058 CVE-2023-31064 …	Nhóm 10 lỗ hổng trong Apache cho phép đối tượng tấn công 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
4	Wordpress	CVE-2022-41635 CVE-2022-41987 CVE-2022-43490 …	Nhóm 73 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	Huawei	CVE-2021-46887 CVE-2022-48478 CVE-2022-48479 …	Nhóm 19 lỗ hổng trong Huawei cho phép đối tượng tấn công thực hiện leo thang đặc quyền, gây ra lỗ hổng trong quá trình xử lý dữ liệu, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Samsung Mobile	CVE-2023-21514 CVE-2023-21515 CVE-2023-21516 …	Nhóm 03 lỗ hổng trong Samsung Mobile (Galaxy Store) 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-2023-22878 CVE-2023-28514 CVE-2023-28950 …	Nhóm 07 lỗ hổng trong IBM phép đối tượng tấn công thực thi mã từ xa, thu thập thông tin dữ liệu nhạy cảm, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá

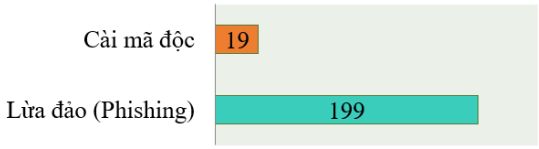
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **51.601,** (giảm so với tuần trước **53.635)** 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.

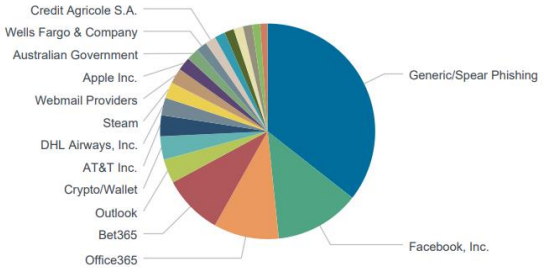


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 218 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 199 trường hợp tấn công lừa đảo (Phishing), 19 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: 7613 IP	xjpakmdcfuqe.ru:89 IP
disorderstatus.ru: 3272 IP	xjpakmdcfuqe.in:131 IP
atomictrivia.ru: 1554 IP	restlesz.su: 221 IP
xjpakmdcfuqe.biz: 166 IP	amnsreiuojy.ru: 300 IP
xjpakmdcfuqe.com: 104 IP	hzmksreiuojy.ru: 48 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **285** 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	pqrm9.com 887vn.com	Website giả mạo sàn TMĐT Tiki
2	nhungmiu.me	Website giả mạo Ví điện tử Momo
3	amazonbig.asia	Giả mạo website Amazon
4	tuyendung203.com	Giả mạo website Lazada
5	vipshopee.com	Website giả mạo sàn TMĐT Shopee

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