NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 20 (15/5/2023 – 21/5/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT FIN7 sử dụng ransomware Cl0p trong đợt tấn công mới.

- **Cảnh báo:** Phát hiện hơn 8.9 triệu điện thoại Android trên toàn thế giới bị lây nhiễm mã độc mới.

2. Điểm yếu, lỗ hổng

- **502** 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: 278** 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 APT FIN7 sử dụng ransomware Cl0p trong đợt tấn công mới"

Tháng 04/2023, các nhà nghiên cứu đã phát hiện ra nhóm tấn công APT Sangria Tempest (ELBRUS, FIN7) bắt đầu hoạt động trở lại kể từ sau chiến dịch tấn công ransomware bắt đầu từ cuối năm 2021 và nhóm tấn công APT FIN7 đã triển khai ransomware Cl0p (hay còn được gọi là Clop) trong cuộc tấn công gần đây. Các đối tượng sử dụng tập lệnh PowerShell POWERTRASH và tải xuống backdoor Lizar trên các thiết bị bị xâm nhập. Điều này cho phép đối tượng tấn công chiếm quyền truy cập trong hệ thống mục tiêu, sử dụng OpenSSH và Impacket để triển khai ransomware Clop.

Hoạt động kể từ năm 2012, FIN7 (hay còn được biết đến với tên gọi Carbanak, ELBRUS và ITG14) đã sử dụng các dòng ransomware khác như Black Basta, DarkSide, REvil và LockBit, Maze và Ryuk. Nhóm tấn công APT FIN7 nhằm mục tiêu vào các tổ chức bao gồm công ty phần mềm, truyền thông, dịch vụ đám mây, y tế, giao thông vận tải.

Ngoài ra, chiến thuật tấn công được sử dụng trong playbook của FIN7 là thành lập các công ty bảo mật giả mạo Combi Security và Bastion Secure để tuyển nhân viên thực hiện các cuộc tấn công ransomware.

Theo các nhà nghiên cứu, việc FIN7 sử dụng mã độc POWERTRASH để cung cấp backdoor Lizar (hay còn được biết đến với tên gọi DICELOADER hoặc Tirion) liên quan đến các cuộc tấn công khai thác lỗ hổng bảo mật CVE-2023-27532 (điểm CVSS: 7.5) có mức ảnh hưởng Cao trong phần mềm Veeam Backup & Replication cho phép đối tượng tấn công giành quyền truy cập và thực hiện các hành động trái phép.

Các cuộc tấn công mới của FIN7 sử dụng nhiều ransomware khác nhau nhằm thay đổi chiến lược tống tiền, chuyển từ đánh cắp dữ liệu thẻ tín dụng sang tấn công tống tiền người dùng. Các cá nhân, tổ chức cần thường xuyên thực hiện kiểm tra, rà soát và cập nhật các bản vá để phòng chống, giảm thiểu các nguy cơ bị tấn công mạng.

Nguồn:
https://thehackernews.com/2023/05/notorious-cyber-gang-fin7-returns-cl0p.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện hơn 8.9 triệu điện thoại Android trên toàn thế giới bị lây nhiễm mã độc mới"

Nhóm tấn công Lemon Group hiện đang nỗ lực khai thác hàng triệu điện thoại thông minh Android bị lây nhiễm mã độc nhằm biến các thiết bị này thành proxy mobile, đây là công cụ đánh cắp thông tin và bán tin nhắn SMS, kiếm tiền trái phép thông qua tài khoản mạng xã hội và nhắn tin trực tuyến, gian lận quảng cáo theo mỗi lần click chuột (Click Fraud).

Hiện đã có hơn 8.9 triệu thiết bị Android bị lây nhiễm, đặc biệt là các dòng điện thoại giá rẻ tập trung chủ yếu ở Mỹ, Mexico, Indonesia, Thái Lan, Nga, Nam Phi, Ấn Độ, Angola, Philippines và Argentina.

Nhóm tấn công này đang mở rộng cuộc tấn công nhằm vào các thiết bị IoT dựa trên Android khác như Smart TV, Android TV box, phần mềm giải trí và cả đồng hồ trẻ em.

Mã độc được phát tán có tên là Guerilla, được phát hiện lần đầu tiên vào năm 2018 khi các nhà nghiên cứu tìm ra 15 ứng dụng trên Play Store có chức năng gian lận quảng cáo theo mỗi lần click chuột (Click Fraud) và hoạt động như một backdoor. Theo các nhà nghiên cứu, nhóm tấn công đã phát tán mã độc này trong 5 năm qua và hiện đã lan rộng trên toàn cầu tại hơn 180 quốc gia, với hơn 50 thương hiệu thiết bị di động bị lây nhiễm.

Đầu năm 2022, mã độc Guerilla được biết đến với khả năng chặn tin nhắn SMS như mật khẩu sử dụng một lần (OTP) được liên kết với nhiều nền tảng trực tuyến khác nhau, ngay sau đó đối tượng tấn công đổi tên thành Durian Cloud SMS nhằm xóa dấu vết của Lemon.

Mỗi plugin của Guerilla đều phục vụ một chức năng kinh doanh trái phép phục vụ cho nhóm tấn công Lemon Group. Một số plugin được các nhà nghiên cứu liệt kê:

- Plugin proxy để thiết lập reverse proxy từ điện thoại bị nhiễm và cho phép các đối tượng tấn công cho thuê quyền truy cập vào tài nguyên mạng của người dùng trái phép.
- Plugin cookie để thu thập cookie Facebook của người dùng và thông tin cá nhân khác.
- Plugin WhatsApp để chiếm phiên truy cập (Session Hijacking) và gửi tin nhắn trái phép.
- Plugin Splash để phân phát quảng cáo không chính đáng khi mở một số ứng dụng nhất định.
- Plugin Silent để cài đặt tệp APK trái phép và mở ứng dụng.

Người dùng cần nâng cao cảnh giác với các tệp đính kèm và thực hiện đầy đủ các bước kiểm tra bảo mật cần thiết trước khi nhấp chuột. Ngoài ra, để hạn chế khả năng dữ liệu riêng tư gặp rủi ro, người dùng nên cẩn thận với những yêu cầu buộc sao chép các tệp vào một thư mục công khai.

Nguồn: https://thehackernews.com/2023/05/this-cybercrime-syndicate-pre-infected.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 **502** lỗ hổng, trong đó có 28 lỗ hổng mức Cao, 19 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 454 lỗ hổng chưa đánh giá. Trong đó có ít nhất 59 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 17 lỗ hổng trong Cisco, Nhóm 04 lỗ hổng trong Linux, Nhóm 23 lỗ hổng trong Google, Nhóm 78 lỗ hổng trong Wordpress, Nhóm 04 lỗ hổng trong Huawei, Nhóm 04 lỗ hổng trong VMware, Nhóm 09 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:

- *Cisco: CVE-2023-20182, CVE-2023-20183,...*
- *Linux: CVE-2023-1195, CVE-2023-1859,...*
- *Google: CVE-2023-21104, CVE-2023-21106,...*
- *Wordpress: CVE-2023-0233, CVE-2023-0490,...*
- *Huawei: CVE-2023-1692, CVE-2023-1693,...*
- *VMware: CVE-2023-20877, CVE-2023-20878,...*
- *IBM: CVE-2023-28520, CVE-2022-43877,...*

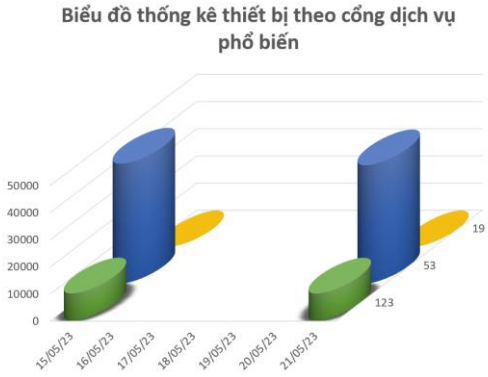
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Cisco	CVE-2023-20182 CVE-2023-20183 CVE-2023-20184 ...	Nhóm 17 lỗ hổng trong Cisco cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thu thập thông tin dữ liệu, thực thi mã tùy ý với đặc quyền root, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-1195 CVE-2023-21106 CVE-2023-2124 …	Nhóm 04 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, đánh cắp thông tin dữ liệu, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2023-21104 CVE-2022-48244 CVE-2023-21107 …	Nhóm 23 lỗ hổng trong Google (Chrome,…) 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-2023-0233 CVE-2023-0490 CVE-2023-0520 …	Nhóm 78 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-2023-1692 CVE-2023-1693 CVE-2023-1694 …	Nhóm 04 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	VMware	CVE-2023-20877 CVE-2023-20878 CVE-2023-20879 …	Nhóm 04 lỗ hổng trong VMware cho phép đối tượng tấn công thực thi lệnh 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
7	IBM	CVE-2023-28520 CVE-2023-27863 CVE-2022-47984 …	Nhóm 09 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

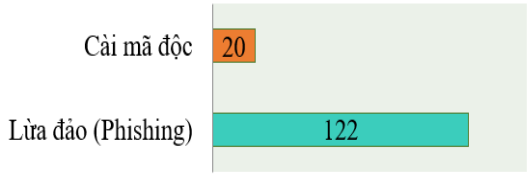
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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 **53,635,** (giảm so với tuần trước **54,292**) 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.

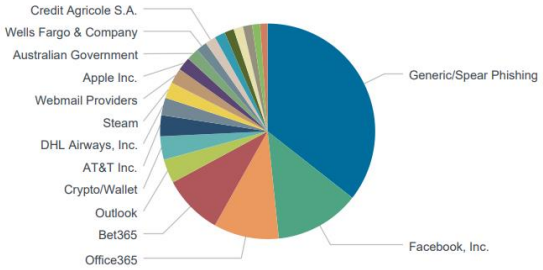


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 142 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 122 trường hợp tấn công lừa đảo (Phishing), 20 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: 8528 IP	xjpakmdcfuqe.ru:155 IP
disorderstatus.ru: 4122 IP	xjpakmdcfuqe.in:196 IP
atomictrivia.ru: 1939 IP	restlesz.su: 291 IP
xjpakmdcfuqe.biz: 206 IP	amnsreiuojy.ru: 381 IP
xjpakmdcfuqe.com: 151 IP	hzmksreiuojy.ru: 52 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **278** 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	216569.com tadmaz.com	Website giả mạo sàn TMĐT Tiki
2	clmm.bar tiawizj.com	Website giả mạo Ví điện tử Momo
3	vn-lottefinance.com	Giả mạo website Lotte
4	vp7811.com 888b.biz 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