NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 48 (27/11/2023 – 03/12/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công Black Basta thu về 100 triệu đô thông qua hoạt động tống tiền sử dụng mã độc ransomware.

- **Cảnh báo:** Mã độc FjordPhantom trên Android nhằm vào các ứng dụng tại Đông Nam Á.

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: 306** 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

"Chiến dịch tấn công APT: Nhóm tấn công Black Basta thu về 100 triệu đô thông qua hoạt động tống tiền sử dụng mã độc ransomware"

Nhóm tấn công sử dụng mã độc ransomware có tên Black Basta bắt đầu hoạt động kể từ tháng 04/2022 dưới hình thức tấn công Ransomware (RaaS), nhóm chủ yếu nhằm vào các doanh nghiệp toàn cầu bằng hình thức tấn công tống tiền kép và đã thu về ít nhất 100 triệu đô từ các khoản tiền chuộc do hơn 90 đơn vị cung cấp.

Hơn 329 đơn vị trên toàn cầu đã trở thành nạn nhân của chiến dịch tấn công do nhóm này thực hiện bằng hình thức tống tiền kép, một hình thức mà nhóm tấn công đánh cắp dữ liệu nhạy cảm từ hệ thống bị ảnh hưởng bởi mã độc trước khi triển khai ransomware lên hệ thống mạng để mã hóa dữ liệu của người dùng.

Những dữ liệu bị đánh cắp sau đó được sử dụng để ép người dùng phải chi trả tiền chuộc nếu không sẽ bị đăng lên trang web trái phép. Dựa theo con số thu thập từ phân tích của các chuyên gia bảo mật, ít nhất 35% đơn vị bị ảnh hưởng bởi Black Basta đã chịu trả khoản tiền chuộc.

Nhóm tấn công Conti ngừng hoạt động vào tháng 06/2022 sau khi bị phát hiện, các thành viên đã tách ra thành các nhóm nhỏ, một trong số đó được cho là Black Basta.

Theo nhận định từ các chuyên gia bảo mật, việc nhóm này đã nhằm vào ít nhất 20 đơn vị trong 2 tuần hoạt động đầu tiên cho thấy rằng nhóm có kinh nghiệm về việc sử dụng ransomware và có một nguồn truy cập đầu vào ổn định; cũng như việc các đối tượng điều khiển mã độc trong nhóm này có kĩ năng tinh vi, thành thạo và sự miễn cưỡng tuyển dụng hay quảng cáo trên các diễn đàn Dark Web càng củng cố khả năng Black Basta là một phần của Conti.

Ngoài ra, Black Basta cũng đã được gán với nhóm APT FIN7, một nhóm tội phạm không gian mạng với động cơ tài chính khét tiếng hoạt động từ năm 2015.

Kể từ khi đi vào hoạt động, Black Basta đã xâm nhập và tống tiền, dữ liệu từ các đơn vị có tiếng như: Sobeys, Knauf, Yellow Pages Canada, Capita,….

Nguồn:
https://www.bleepingcomputer.com/news/security/black-basta-ransomware-made-over-100-million-from-extortion/?&web_view=true#google_vignette

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Mã độc FjordPhantom trên Android nhằm vào các ứng dụng tại Đông Nam Á"

Kể từ đầu tháng 09/2023, đã phát hiện mã độc trên nền tảng Android có tên FjordPhantom trong các chiến dịch tấn công nhằm vào người dùng tại Đông Nam Á như Indonesia, Thái Lan và Việt Nam.

FjordPhantom được phát tán thông qua các ứng dụng, dịch vụ nhắn tin với hình thức tấn công kết hợp giữa mã độc ứng dụng và kỹ thuật Social engineering để lừa đảo người dùng. Cụ thể hơn, người dùng sẽ được đối tượng tiếp cận qua email, SMS và ứng dụng nhắn tin rồi bị lừa tải xuống ứng dụng ngân hàng giả mạo.

Sau đó, đối tượng sẽ sử dụng kỹ thuật Social engineering tương tự như một cuộc tấn công định hướng qua điện thoại (TOAD), đây là một kỹ thuật khiến người dùng gọi tới các tổng đài giả mạo để được hướng dẫn cách thực thi ứng dụng ngân hàng đã tải xuống.

Một đặc điểm nổi bật của mã độc là việc sử dụng ảo hóa để thực thi các câu lệnh độc hại trong một khoang chứa nhằm tránh bị phát hiện. Biện pháp này giúp mã độc vượt qua lớp bảo vệ sandbox trên Android do nó cho phép nhiều ứng dụng chạy trên cùng một sandbox, qua đó giúp mã độc truy cập tới nơi chứa dữ liệu quan trọng mà không cần tới quyền truy cập root.

Các chuyên gia bảo mật cho biết giải pháp ảo hóa được sử dụng bởi mã độc cũng có thể chèn đoạn mã vào một ứng dụng do cơ chế hoạt động nạp câu lệnh của giải pháp lên một tiến trình trước khi nạp câu lệnh của ứng dụng.

Đối với mã độc FjordPhantom, ứng dụng được tải xuống có chứa một module độc hại và giải pháp ảo hóa có mục đích tải và cài đặt ứng dụng nhúng của ngân hàng đối tượng trong một môi trường ảo.

Hay nói cách khác, ứng dụng giả mạo được thiết kế để nạp ứng dụng chính thống của ngân hàng vào môi trường ảo, đồng thời triển khai một framework cho phép thay đổi hoạt động của API quan trọng nhằm thu thập thông tin quan trọng từ màn hình ứng dụng rồi đóng các cảnh báo về hoạt động độc hại đang diễn ra trên thiết bị của người dùng.

Google cho biết người dùng của họ luôn được bảo vệ bởi Google Play Protect thông qua các cảnh báo tới người dùng hoặc chặn ứng dụng có biểu hiện độc hại trên thiết bị Android với dịch vụ Google Play Services, kể cả khi các ứng dụng này được cài đặt qua các nguồn không phải là Google Play.

Nguồn: https://thehackernews.com/2023/12/new-fjordphantom-android-malware.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 105 lỗ hổng mức Cao, 83 lỗ hổng mức Trung bình, 02 lỗ hổng mức Thấp và 324 lỗ hổng chưa đánh giá. Trong đó có ít nhất 102 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 12 lỗ hổng trong Google, Nhóm 02 lỗ hổng trong Apple, Nhóm 06 lỗ hổng trong Foxit Software, Nhóm 110 lỗ hổng trong Wordpress, Nhóm 14 lỗ hổng trong Apache, Nhóm 09 lỗ hổng trong GitLab, Nhóm 13 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:

- Google: CVE-2023-6345, CVE-2023-6346,...

- Apple: CVE-2023-42916, CVE-2023-42917

- Foxit Software: CVE-2023-32616, CVE-2023-35985,...

- Wordpress: CVE-2023-4922, CVE-2023-5604,...

- Apache: CVE-2023-48796, CVE-2023-49068,...

- GitLab: CVE-2023-3443, CVE-2023-3949,...

- IBM: CVE-2023-26279, CVE-2023-45168,...

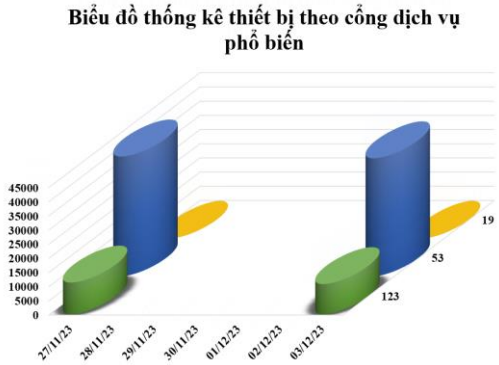
Thông tin điểm yếu, lỗ hổng

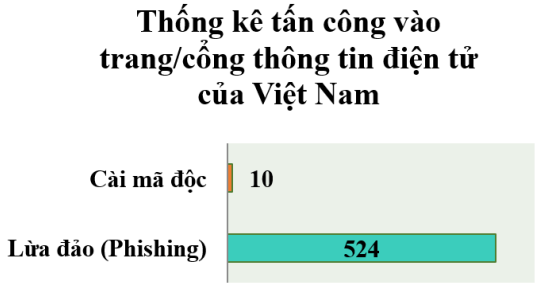
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Google	CVE-2023-6345 CVE-2023-6346 CVE-2023-6347 …	Nhóm 12 lỗ hổng trong Google cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Apple	CVE-2023-42916 CVE-2023-42917	Nhóm 02 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	Foxit Software	CVE-2023-32616 CVE-2023-35985 CVE-2023-38573 …	Nhóm 06 lỗ hổng trong Foxit Software 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
4	Wordpress	CVE-2023-4922 CVE-2023-5604 CVE-2023-5974 …	Nhóm 110 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗi SSRF, khai thác lỗi XSS, khai thác lỗi CSRF, thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa.	Chưa có thông tin xác nhận và bản vá
5	Apache	CVE-2023-48796 CVE-2023-49068 CVE-2023-40610 …	Nhóm 14 lỗ hổng trong Apache cho phép đối tượng tấn công leo thang đặc quyền, khai thác lỗi XSS, khai thác lỗi SQL Injeciton.	Đã có thông tin xác nhận và bản vá
6	GitLab	CVE-2023-3443 CVE-2023-3949 CVE-2023-3964 …	Nhóm 09 lỗ hổng trong GitLab cho phép đối tượng tấn công thực thi mã từ xa, 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
7	IBM	CVE-2023-26279 CVE-2023-45168 CVE-2023-42006 …	Nhóm 13 lỗ hổng trong IBM phép đối tượng tấn công thực thi mã từ xa, khai thác lỗi CSRF, khai thác lỗi XSS, thực hiện tấn công từ chối dịch vụ.	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 **52.324**, (giảm so với tuần trước **53.503**) 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.



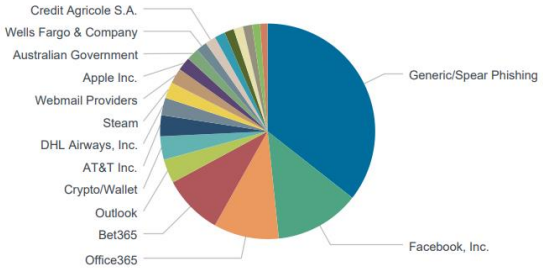


Tấn công Web

Trong tuần, có **534** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 524 trường hợp tấn công lừa đảo (Phishing), 10 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: 12968 IP	hzmksreiuojy.ru: 237 IP
disorderstatus.ru: 4145 IP	xjpakmdcfuqe.biz: 216 IP
atomictrivia.ru: 1897 IP	xjpakmdcfuqe.com: 86 IP
amnsreiuojy.ru: 691 IP	xjpakmdcfuqe.ru: 59 IP
restlesz.su: 392 IP	xjpakmdcfuqe.in: 33 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **306** 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	tin-dung-uu-tien-vib.com vib.chamsockhachang-tructuyen-the.online vib.chamsockhachang-tructuyen.online vib-tindung-khcn.com vib.chamsockhachang-tructuyen.online vib.tuvan-chamsockhachhang.com vib.chamsockhachhang-tructuyen-the-visa.com tin-dung-khcn-vib.com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
2	viettelvngroup.com viettel6.com	Website giả mạo Tập đoàn Công nghiệp – Viễn thông Quân đội (Viettel)
3	lazmail.com.vn looklazada.com	Website giả mạo sàn TMĐT Lazada
4	vn66954shp.com spohopena.com	Website giả mạo sàn TMĐT Shopee
5	dichvucong.hgov.cc dichvucong.vgovn.net	Website giả mạo Dịch vụ công Quốc Gia
6	khcn-tindung-vp.com visa-vpbank-uu-tien.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
7	shinhanbank.chamsockhachang-the.com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
8	chamsockhachhangnanghanmuctindungmsb.com	Website giả mạo Ngân hàng TMCP Hàng hải Việt Nam
9	hotrokhachhangtindungvietinbank.com	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
10	homecredit1.com	Website giả mạo Công ty Tài chính TNHH MTV Home Credit 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 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