NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 37 (11/9/2023 –17/9/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Charming Kitten sử dụng mã độc Backdoor "Sponsor" để tấn công Brazil, Israel và UAE.

- **Cảnh báo:** Mã độc NodeStealer tấn công các tài khoản Facebook Business trên nhiều trình duyệt khác nhau.

2. Điểm yếu, lỗ hổng

- **425** 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: 394** 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 APT Charming Kitten sử dụng mã độc Backdoor "Sponsor" để tấn công Brazil, Israel và UAE"

Gần đây, nhóm tấn công APT Charming Kitten đến từ Iran, đã bị phát hiện đang tham gia vào chiến dịch tấn công mới nhắm vào Brazil, Israel và UAE. Nhóm này tấn công bằng cách sử dụng một backdoor mới chưa từng được phát hiện trước đó, được gọi là "Sponsor". Các chuyên gia bảo mật đang theo dõi nhóm cầm chiến dịch tấn công này với tên mã "Ballistic Bobcat". Dựa trên các mẫu nạn nhân trước đây, chuyên gia nhận định rằng Charming Kitten đang tập trung tấn công vào các tổ chức giáo dục, chính phủ, y tế, cũng như các hoạt động nhân quyền và báo chí.

Mã độc Sponsor chứa các tệp cấu hình trên ổ đĩa và được phát tán thông qua các tệp batch, được thiết kế để trông giống như các tệp vô hại để tránh bị phát hiện bởi các công cụ quét mã độc. Ít nhất có 34 người dùng đã bị ảnh hưởng bởi Sponsor, và trường hợp nhiễm mã độc đầu tiên được ghi nhận vào khoảng tháng 9/2021.

Chiến dịch "Sponsoring Access" đang triển khai với mục tiêu xâm nhập thông qua việc khai thác các lỗ hổng trên máy chủ Microsoft Exchange để thực hiện các tác vụ hậu xâm nhập, mô phỏng một cảnh báo đã được phát hành bởi Úc, Anh và Mỹ vào tháng 11/2021.

Trong một sự cố vào tháng 8/2021, một công ty tại Israel đã bị xâm nhập với mục đích phát tán các phần mềm độc hại như PowerLess, Plink và một toolkit mã nguồn mở viết bằng Go có tên Merlin. Toolkit Merlin này thực hiện một reverse shell Meterpreter kết nối đến máy chủ C&C. Vào ngày 12/12/2021, reverse shell này đã tải xuống một tệp batch có tên "install.bat" và thực thi nó, giúp đối tượng tấn công thành công trong việc cài đặt backdoor Sponsor.

Sponsor được viết bằng C++ với mục tiêu thu thập thông tin về các thiết bị nhiễm mã độc và thực hiện các chỉ dẫn từ xa được gửi từ máy chủ. Những chỉ dẫn này bao gồm: thực thi tệp, lệnh; tải tệp; cập nhật danh sách máy chủ bị kiểm soát bởi đối tượng tấn công.

Hiện tại, Ballistic Bobcat đang tiếp tục hoạt động với mô hình "quét-và-khai thác", đồng thời không ngừng tìm kiếm các mục tiêu tiềm năng còn tồn tại lỗ hổng chưa được vá trên máy chủ Microsoft Exchange. Nhóm này vẫn sử dụng nhiều công cụ mã nguồn mở kết hợp với ứng dụng tùy chỉnh, bao gồm backdoor Sponsor.

Nguồn:
https://thehackernews.com/2023/09/charming-kitens-new-backdoor-sponsor.html

Tin tức An toàn thông tin

"Cảnh báo: Mã độc NodeStealer tấn công các tài khoản Facebook Business trên nhiều trình duyệt khác nhau"

Một chiến dịch tấn công đang nhằm vào các tài khoản Facebook Business thông qua tin nhắn giả mạo. Mục tiêu của chiến dịch này là thu thập thông tin đăng nhập của nạn nhân bằng cách sử dụng một biến thể của mã độc NodeStealer dựa trên Python, sau đó sử dụng các thông tin thu thập trái phép để thực hiện các chiến dịch tấn công khác.

Chiến dịch này chủ yếu nhằm vào các ngành công nghiệp sản xuất và công nghệ ở Nam Âu và Bắc Mỹ. Ban đầu, NodeStealer là mã độc JavaScript, được Meta phát hiện vào tháng 05/2023. Tại thời điểm đó, NodeStealer có khả năng đánh cắp cookies và mật khẩu từ trình duyệt để xâm nhập vào tài khoản Facebook, Gmail và Outlook. Ngoài ra, đã từng có một chiến dịch tấn công khác diễn ra vào tháng 12/2022 sử dụng phiên bản Python của mã độc NodeStealer, với một số biến thể được thiết kế để thực hiện hành vi đánh cắp tiền ảo.

Dựa trên các phân tích của các chuyên gia bảo mật, đối tượng tấn công có thể là người Việt Nam. Nhóm tấn công này có khả năng đang hoạt động trở lại với các chiến thuật được sử dụng bởi các nhóm tấn công cùng mục tiêu khác trên toàn cầu.

Trong tuần vừa qua, đã ghi nhận về một vụ gửi hàng loạt tin nhắn lừa đảo trên ứng dụng Facebook Messenger. Tất cả các tin nhắn này đều được gửi từ một mạng botnet chứa các tài khoản cá nhân bị đánh cắp, với mục tiêu phát tán các tệp nén ZIP hoặc RAR chứa mã độc.

Quá trình lây nhiễm này là một phần trong chuỗi xâm nhập của mã độc NodeStealer, nhằm phát tán các tệp nén RAR lưu trữ trên mạng truyền nội dung (CDN) của Facebook. Những tệp nén này chứa một tập lệnh batch, khi được thực thi sẽ mở trình duyệt Chrome và điều hướng người dùng tới một trang web vô hại ngẫu nhiên. Cùng lúc đó, câu lệnh PowerShell được thực thi ẩn để tải xuống các tệp hỗ trợ bao gồm trình thông dịch Python cùng với mã độc NodeStealer.

Ngoài việc đánh cắp thông tin đăng nhập và cookies từ nhiều trình duyệt và nền tảng khác nhau, NodeStealer cũng có khả năng thu thập dữ liệu metadata từ thiết bị và gửi về cho các đối tượng tấn công thông qua ứng dụng Telegram.

Chiến dịch tấn công này được xem là bước khởi đầu cho các cuộc tấn công tập trung khác thông qua việc thu thập thông tin quan trọng. Sau đó, thông tin đăng nhập và cookies của tài khoản Facebook có thể bị chiếm đoạt và thực hiện giao dịch lừa đảo bằng việc lợi dụng danh tiếng của các trang doanh nghiệp uy tín.

Nguồn: https://thehackernews.com/2023/09/nodestealer-malware-now-targets.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 **425** lỗ hổng, trong đó có 179 lỗ hổng mức Cao, 99 lỗ hổng mức Trung bình, 05 lỗ hổng mức Thấp và 142 lỗ hổng chưa đánh giá. Trong đó có ít nhất 117 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 59 lỗ hổng trong Microsoft, Nhóm 14 lỗ hổng trong Mozilla, Nhóm 34 lỗ hổng trong Google, Nhóm 28 lỗ hổng trong Wordpress, Nhóm 21 lỗ hổng trong Adobe, Nhóm 03 lỗ hổng trong Linux, 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:

- Microsoft: CVE-2023-33136, CVE-2023-36764,...

- Mozilla: CVE-2023-4582, CVE-2023-4584,...

- Google: CVE-2023-35681, CVE-2023-35658,...

- Wordpress: CVE-2023-4153, CVE-2023-4213,...

- Adobe: CVE-2023-38204, CVE-2022-24093,...

- Linux: CVE-2023-4881, CVE-2023-4155,...

- IBM: CVE-2023-33164, CVE-2023-38736,...

Thông tin điểm yếu, lỗ hổng

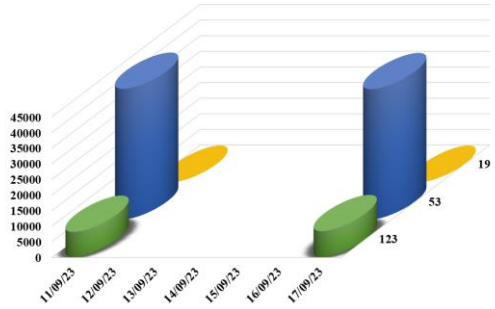
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-33136 CVE-2023-36764 CVE-2023-38146 ...	Nhóm 59 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, khai thác lỗi XSS, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
2	Mozilla	CVE-2023-4582 CVE-2023-4584 CVE-2023-4585 ...	Nhóm 14 lỗ hổng trong Mozilla cho phép đối tượng tấn công thực thi mã từ xa, khai thác lỗi Buffer Overflow.	Chưa có thông tin xác nhận và bản vá
3	Google	CVE-2023-35681 CVE-2023-35658 CVE-2023-35673 ...	Nhóm 34 lỗ hổng trong Google cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-4153 CVE-2023-4213 CVE-2023-4916 ...	Nhóm 28 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực thi mã từ xa, khai thác lỗi XSS, thực hiện tấn công CSRF.	Chưa có thông tin xác nhận và bản vá
5	Adobe	CVE-2023-38204 CVE-2022-24093 CVE-2022-28831 ...	Nhóm 21 lỗ hổng trong Adobe cho phép đối tượng tấn công thực thi mã từ xa, khai thác lỗi XSS, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	Linux	CVE-2023-4881 CVE-2023-4155 CVE-2023-4921 ...	Nhóm 03 lỗ hổng trong Linux cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
7	IBM	CVE-2022-33164 CVE-2023-38736 CVE-2022-22401 ...	Nhóm 09 lỗ hổng trong IBM phép đối tượng tấn công thực hiện leo thang đặc quyền, thực thi mã từ xa, 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

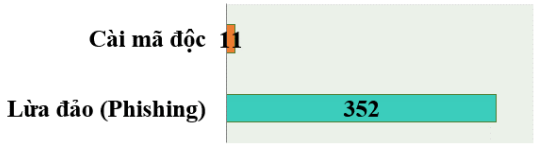
Tấn công DRDoS

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 **50.021**, (tăng so với tuần trước **46.847**) 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

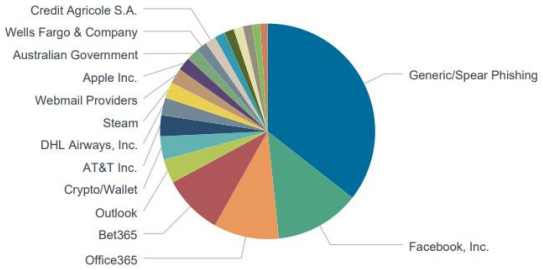


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **363** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 352 trường hợp tấn công lừa đảo (Phishing), 11 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: 8170 IP	xjpakmdcfuqe.ru: 38 IP
disorderstatus.ru: 3005 IP	xjpakmdcfuqe.in: 29 IP
atomictrivia.ru: 1510 IP	restlesz.su: 218 IP
xjpakmdcfuqe.biz: 180 IP	amnsreiuojy.ru: 368 IP
xjpakmdcfuqe.com: 66 IP	hzmksreiuojy.ru: 107 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **394** 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	shoosse.com ksdp997.com	Website giả mạo sàn TMĐT Shopee
2	nang-han-muc-the.miles-vpbank.com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
3	adwf33.com adwf66.com	Website giả mạo sàn TMĐT Tiki
4	tf12lbm.com lookctv-vn.com	Website giả mạo sàn TMĐT Lazada
5	hotromayxanh.com	Website giả mạo Điện máy xanh

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