

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 08 (19/02/2024 – 25/02/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Mustang Panda sử dụng mã độc backdoor DOPLUGS để tấn công vào châu Á.
- **Cảnh báo:** Mã độc VietCredCare đánh cắp tài khoản Facebook thông qua các nhà cung cấp dịch vụ quảng cáo tại Việt Nam.

2. Điểm yếu, lỗ hổng

- **593** 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: 254** 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://khonggianmang.vn>

Tin tức An toàn thông tin

“Nhóm APT Mustang Panda sử dụng mã độc backdoor DOPLUGS để tấn công vào châu Á.”

Nhóm APT Mustang Panda có nguồn gốc từ Trung Quốc đang tiến hành một chiến dịch tấn công mạng nhằm vào nhiều quốc gia tại châu Á như Việt Nam, Đài Loan và Malaysia. Trong chiến dịch này, Mustang Panda sử dụng một phiên bản biến thể của mã độc backdoor PlugX, được gọi là DOPLUGS.

Nhóm APT Mustang Panda đã hoạt động từ năm 2012, chủ yếu nhằm vào các tổ chức chính phủ, viện nghiên cứu, tổ chức phi chính phủ ở Châu Âu và Châu Mỹ, và thậm chí cả các tổ chức tôn giáo tại Vatican. Tuy nhiên, trong các chiến dịch gần đây, nhóm này đã chuyển mục tiêu sang các quốc gia Châu Á như Đài Loan, Hồng Kông, Mông Cổ, Tibet và Myanmar. Vào năm 2022, Mustang Panda đã sử dụng các báo cáo về tình hình chiến sự tại Ukraine và báo cáo từ chính phủ Ukraine làm mồi nhử để dẫn dụ người dùng mở các tệp này, từ đó, quá trình lây nhiễm mã độc sẽ bắt đầu triển khai trên thiết bị.

Trong chiến dịch mới nhất, nhóm APT Mustang Panda đã sử dụng một biến thể của mã độc PlugX có tên là DOPLUGS, đi kèm với một module backdoor hoàn chỉnh. Phân tích mã độc đã phát hiện ra sự tồn tại của module KillSomeOne hỗ trợ khả năng lây lan qua USB, module này đã được phát hiện lần đầu vào tháng 11/2020.

Trong các chiến dịch tấn công, Mustang Panda thực hiện tấn công spear-phishing bằng cách gửi các tập tin văn bản với nội dung mang tính thời sự như cuộc bầu cử tổng thống Đài Loan diễn ra vào tháng 01/2024 để làm mồi nhử. Các email spear-phishing chứa đường dẫn Google Drive đến các tệp được bảo vệ bằng mật khẩu, mục đích là để tải xuống mã độc DOPLUGS.

Mã độc DOPLUGS có chức năng như một bộ tải và hỗ trợ thực thi bốn câu lệnh backdoor khác nhau. Một trong số đó là để tải xuống mã độc PlugX. Trong mẫu phân tích DOPLUGS, có chứa module KillSomeOne và sử dụng thành phần thực thi file thực thi hợp pháp để thực hiện DLL-sideload. Thành phần này cũng tải thêm mã độc giai đoạn kế tiếp từ một máy chủ từ xa.

Tin tức An toàn thông tin

“Mã độc VietCredCare đánh cắp tài khoản Facebook thông qua các nhà cung cấp dịch vụ quảng cáo tại Việt Nam.”

Mã độc VietCredCare là một loại mã độc chủ yếu nhằm vào các nhà cung cấp dịch vụ quảng cáo trên Facebook tại Việt Nam. Mã độc VietCredCare bị phát hiện từ tháng 8 năm 2022, có khả năng lọc tự động các cookie và thông tin đăng nhập Facebook từ các thiết bị bị nhiễm mã độc. Đồng thời, mã độc này cũng kiểm tra được các tài khoản này có quản lý hồ sơ các doanh nghiệp và duy trì số dư tích cực trong tài khoản quảng cáo của Meta hay không.

Mục tiêu chính của chiến dịch sử dụng mã độc VietCredCare là chiếm đoạt các tài khoản Facebook của doanh nghiệp bằng cách nhắm vào người quản lý trang Facebook của các doanh nghiệp và tổ chức có tiếng tại Việt Nam. Đối tượng tấn công sẽ sử dụng tài khoản Facebook bị chiếm đoạt để đăng các bài viết có nội dung chính trị hoặc thực hiện lừa đảo tiếp thị nhằm trục lợi tài chính.

VietCredCare được quảng cáo và rao bán dưới dạng dịch vụ “stealer-as-a-service” trên các nền tảng như Facebook, Youtube và Telegram. Hiện tại, đã xác định rằng mã độc này đang được sử dụng bởi các cá nhân hoặc nhóm người Việt Nam. Các khách hàng mua mã độc này có thể lựa chọn giao dịch quyền truy cập vào một botnet do nhà phát triển mã độc quản lý hoặc mua quyền truy cập vào mã nguồn để bán lại hoặc sử dụng mã độc cho mục đích cá nhân. Ngoài ra, các đối tượng mua mã độc này cũng được cung cấp một bot Telegram riêng để quản lý việc trích xuất và chuyển tiếp thông tin xác thực từ các thiết bị bị nhiễm mã độc.

VietCredCare là một loại mã độc được viết bằng .NET, được phát tán thông qua các liên kết lừa đảo trên mạng xã hội và các ứng dụng nhắn tin, thường được giả mạo dưới hình thức các phần mềm chính thống như Microsoft Office hoặc Acrobat Reader để đánh lừa người dùng cài đặt mã độc. Điểm nổi bật của mã độc này là khả năng trích xuất thông tin xác thực, cookies và ID phiên từ các trình duyệt web phổ biến tại Việt Nam như Google Chrome, Microsoft Edge và Cốc Cốc.

Ngoài ra, mã độc VietCredCare còn thu thập địa chỉ IP của người dùng và kiểm tra xem tài khoản Facebook của họ có phải là tài khoản doanh nghiệp không, đồng thời đánh giá xem tài khoản đó có đang chạy quảng cáo hay không. Để tránh bị phát hiện, mã độc tắt Windows Antimalware Scan Interface (AMSI) và tự thêm vào danh sách bỏ qua của Windows Defender Antivirus.

Hiện nay, các thông tin xác thực thuộc sở hữu của chính phủ, các trường đại học, các nền tảng thương mại điện tử, ngân hàng và các công ty tại Việt Nam đã bị trích xuất bằng mã độc này. VietCredCare là mã độc mới nhất được thêm vào danh sách các mã độc đánh cắp thông tin tài khoản Facebook, có nguồn gốc từ Việt Nam, tương tự như Ducktail và NodeStealer. Tuy nhiên, hiện vẫn chưa có bằng chứng cụ thể nào cho thấy mối liên kết trực tiếp giữa VietCredCare và các mã độc cùng dòng này.



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 **593** lỗ hổng, trong đó có 107 lỗ hổng mức Cao, 152 lỗ hổng mức Trung bình, 22 lỗ hổng mức Thấp và 312 lỗ hổng chưa đánh giá. Trong đó có ít nhất 97 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 51 lỗ hổng trong Linux, Nhóm 33 lỗ hổng trong Google, Nhóm 03 lỗ hổng trong Microsoft, Nhóm 26 lỗ hổng trong Apple, Nhóm 26 lỗ hổng trong Oracle, Nhóm 07 lỗ hổng trong Gitlab, Nhóm 10 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:

- *Linux: CVE-2024-1784, CVE-2023-52446, ...*
- *Google: CVE-2023-21165, CVE-2023-40085, ...*
- *Microsoft: CVE-2024-26192, CVE-2024-21423, ...*
- *Apple: CVE-2023-42823, CVE-2023-42843, ...*
- *Oracle: CVE-2024-20980, CVE-2024-20913, ...*
- *Gitlab: CVE-2024-1451, CVE-2024-0410, ...*
- *IBM: CVE-2024-25021, CVE-2022-43842, ...*

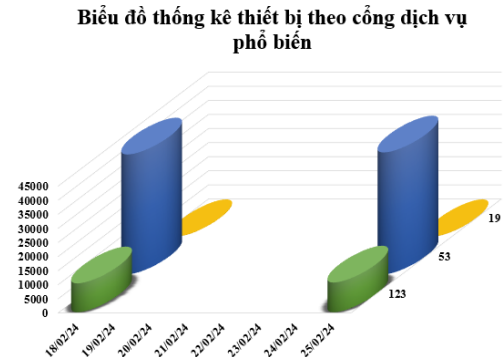
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2024-1784 CVE-2023-52446 CVE-2023-52433 ...	Nhóm 51 lỗ hổng trong Linux 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
2	Google	CVE-2023-21165 CVE-2023-40085 CVE-2023-40093 ...	Nhóm 33 lỗ hổng trong Google cho phép đối tượng tấn công leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	Microsoft	CVE-2024-26192 CVE-2024-21423 CVE-2024-26188	Nhóm 03 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Apple	CVE-2023-42823 CVE-2023-42843 CVE-2023-42848 ...	Nhóm 26 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
5	Oracle	CVE-2024-20980 CVE-2024-20913 CVE-2024-20947 ...	Nhóm 26 lỗ hổng trong Oracle 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
6	Gitlab	CVE-2024-1451 CVE-2024-0410 CVE-2023-4895 ...	Nhóm 07 lỗ hổng trong Gitlab cho phép đối tượng tấn công khai thác lỗ hổng XSS, leo thang đặc quyền.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2024-25021 CVE-2022-43842 CVE-2023-50306 ...	Nhóm 10 lỗ hổng trong IBM phép đối tượng tấn công khai thác lỗ hổng SQL Injection, thực thi mã từ xa, khai thác lỗ hổng XSS.	Chưa có thông tin xác nhận và bản vá

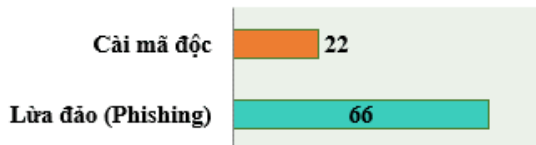
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

Tấn công DRDoS

Tuần vừa qua tại Việt Nam, có rất nhiều máy chủ, thiết bị có thể trở thành nguồn phát tấn công DRDoS. Trong tuần có **53.886** (tăng so với tuần trước **52.826**) 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 công dịch vụ phổ biến trong tuần.

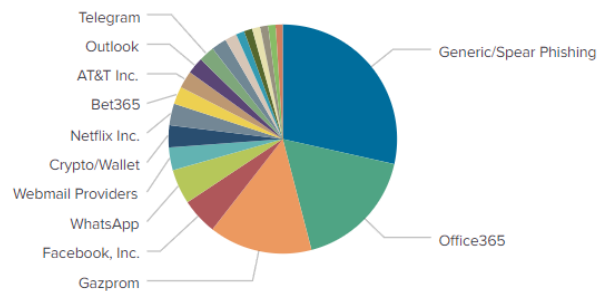


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **88** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 66 trường hợp tấn công lừa đảo (Phishing), 22 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: 9269 IP	hzmksreioujy.ru: 102 IP
disorderstatus.ru: 4222 IP	xjpakmdcfuqe.biz: 182 IP
atomictrivia.ru: 1947 IP	xjpakmdcfuqe.com: 105 IP
amnsreioujy.ru: 566 IP	xjpakmdcfuqe.ru: 101 IP
restlesz.su: 245 IP	xjpakmdcfuqe.in: 84 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **254** 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	amadbfbk.shop	Website giả mạo sàn TMĐT Amazon
2	hgff11.com	Website giả mạo sàn TMĐT Tiki
3	scb.chamsockhachhang-truc-tuyen-the.online	Website giả mạo Ngân hàng TMCP Sài Gòn
4	soppe68.com vn88631p.com spmail86.com	Website giả mạo sàn TMĐT Shopee
5	cskh-vib-canhan.com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam

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/>

f <https://www.facebook.com/govSOC>

📍 Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp. Hà Nội