TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

NCSC VN
National Cyber Security Center

CẢNH BÁO TUẦN

SỐ 29 (18/7/2022 – 24/7/2022)

Thông tin liên hệ: Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 – ais.@mic.gov.vn

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

NỘI DUNG TUẦN

"NỖ LỰC ĐỂ KHÔNG GIAN MẠNG VIỆT NAM LUÔN AN TOÀN, LÀNH MẠNH"

TIN CẢNH BÁO

- **Cảnh báo:** Phần mềm độc hại mới cho phép đối tượng tấn công cài cắm rootkit trên hệ thống Linux được nhằm mục tiêu

- **Chiến dịch tấn công APT:** Nhóm tấn công APT 29 khai thác dịch vụ lưu trữ trực tuyến Google Drive và Dropbox

ĐIỂM YẾU, LỖ HỔNG

- **655** 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.

SỐ LIỆU, THỐNG KÊ

- Tấn công DRDoS
- Tấn công Web
- Tấn công lừa đảo người dùng Việt Nam

Hot News!

Tài liệu lưu trữ:

Chuyên mục **Báo cáo định kỳ** tại địa chỉ:

https://service.khonggianmang.vn

https://khonggianmang.vn

TIN CẢNH BÁO

Cảnh báo: Phần mềm độc hại mới cho phép đối tượng tấn công cài cắm rootkit trên hệ thống Linux được nhằm mục tiêu

Gần đây, một phần mềm độc hại mới trên hệ điều hành Linux được phát hiện có khả năng cho phép cài cắm rootkit, có tên gọi là Lightning Framework. Phần mềm độc hại được trang bị nhiều tính năng khiến nó trở thành một trong những framework phức tạp được phát triển để nhằm mục tiêu hệ thống sử dụng Linux. Lightning Framework có khả năng thụ động và chủ động để giao tiếp với đối tượng tấn công, bao gồm mở SSH trên một máy bị nhiễm và cấu hình C&C tùy ý.

Lightning Framework bao gồm downloader (kbioset) và mô-đun lõi (kkdmflush). Mô-đun lõi thiết lập liên lạc với máy chủ C&C để thực hiện các lệnh cần thiết được yêu cầu, đồng thời che dấu sự hiện diện của chính nó trong máy bị lây nhiễm.

Một số lệnh đáng chú ý nhận được từ máy chủ cho phép phần mềm độc hại lấy dấu vân tay cài đặt trên máy, chạy lệnh shell, tải tệp tên máy chủ C&C, ghi dữ liệu tùy ý vào tệp, thậm chí cập nhật và xóa chính nó khỏi máy chủ bị nhiễm.

Lightning Framework trở thành chủng phần mềm độc hại Linux thứ 5 được phát hiện trong khoảng thời gian ngắn là 3 tháng sau BPFDoor, Symbiote, Syslogk và OrBit. Theo các chuyên gia bảo mật, Lightning Framework là một phần mềm đáng chú ý vì chưa thấy một framework lớn như vậy trước đây để nhằm mục tiêu hệ điều hành Linux.

Nguồn: https://thehackernews.com/2022/07/new-linux-malware-framework-let.html

Nhóm tấn công APT 29 khai thác dịch vụ lưu trữ trực tuyến Google Drive và Dropbox

Nhóm tấn công APT 29 đang khai thác các dịch vụ trực tuyến như Google Drive và Dropbox trong các cuộc tấn công để tránh bị phát hiện. Nhóm đã áp dụng chiến thuật mới này nhằm vào các cơ quan đại diện ngoại giao phương Tây và các đại sứ quán nước ngoài trên khắp thế giới. Hai chiến dịch gần đây được các nhà nghiên cứu quan sát bắt đầu từ đầu tháng 5 đến tháng 6 năm 2022. Chiến dịch đầu tiên sử dụng DropBox, chiến dịch thứ 2 sử dụng Google Drive.

APT 29 sử dụng Agenda[.]Html để giải mã payload và cài cắm tệp ISO độc hại vào ổ cứng của mục tiêu. Phương pháp này được gọi là HTML Smuggling. Tệp payload là tệp ISO Agenda[.]Iso, được tải xuống máy mục tiêu. Khi người dùng kích đúp vào, quá trình lây nhiễm sẽ bắt đầu và thực thi mã độc hại trên hệ thống.

Các chiến dịch gần đây của APT29 thể hiện sự tinh vi và sự linh hoạt trong chiến thuật tấn công. Hơn nữa, nhóm đã khai thác thành công các dịch vụ DropBox và Google Drive, những dịch vụ rất phổ biến được sử dụng bởi hàng triệu người dùng trên khắp thế giới. Việc đưa các dịch vụ này vào quy trình phát tán phần mềm độc hại của APT thực sự là một vấn đề nghiêm trọng và đáng chú ý. Các cơ quan, tổ chức cần quan tâm và thường xuyên cập nhật thông tin về mối đe dọa nghiêm trọng để có biện pháp phòng tránh và ngăn ngừa kịp thời.

Nguồn: https://cyware.com/news/apt29-abuses-online-storage-services-google-drive-and-dropbox-2d799b4b

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 655 lỗ hổng, trong đó có 05 lỗ hổng mức Cao, 31 lỗ hổng mức Trung bình, 15 lỗ hổng mức Thấp và 604 lỗ hổng chưa đánh giá. Trong đó có ít nhất 132 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 32 lỗ hổng trong sản phẩm Adobe, Nhóm 83 lỗ hổng trong Oracle, Nhóm 32 lỗ hổng trong Wordpress, 01 lỗ hổng trong sản phẩm Windows, Nhóm 34 lỗ hổng trong Google, Nhóm 05 lỗ hổng trong thiết bị Dell, 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:

- Adobe: CVE-2022-34230, CVE-2022-34229,...

- Oracle: CVE-2022-21508, CVE-2022-21428,...

- Wordpress: CVE-2022-2443, CVE-2022-2435,...

- Windows: CVE-2021-42923

- Google: CVE-2022-23745, CVE-2022-1136,...

- Dell: CVE-2022-31234, CVE-2022-22555,...

- IBM: CVE-2021-38936, CVE-2021-29788,...

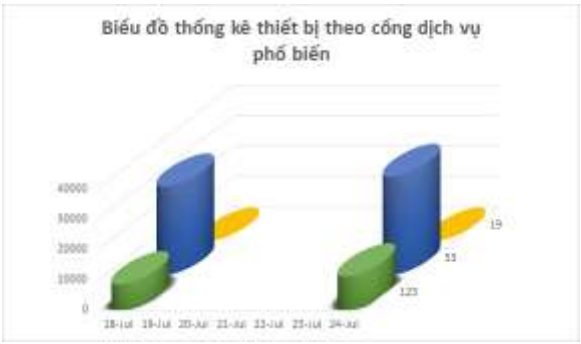
Thông tin điểm yếu, lỗ hổng

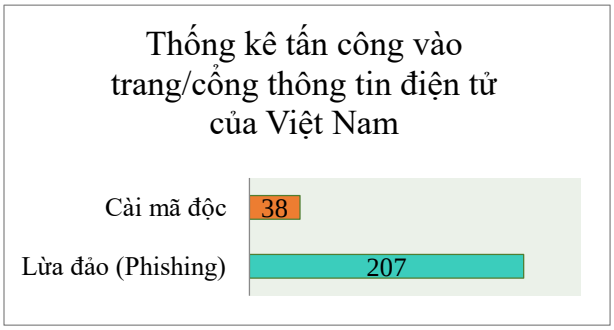
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Adobe	CVE-2022-34230 CVE-2022-34229 CVE-2022-34228 …	Nhóm 32 lỗ hổng trong sản phẩm Adobe (Acrobat Reader, Character Animator, InCopy,..) cho phép đối tượng tấn công làm tràn bộ đệm, thực thi mã tùy ý, tấn công XSS, truy cập/thực hiện các hành động trái phép	Chưa có thông tin xác nhận và bản vá
2	Oracle	CVE-2022-21508 CVE-2022-21428 CVE-2022-21518 …	Nhóm 83 lỗ hổng trong các thiết bị Oracle (Essbase, FLEXCUBE...) cho phép đối tượng tấn công không cần xác thực có quyền truy cập vào hệ thống, tấn công từ chối dịch vụ, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Wordpress	CVE-2022-2443 CVE-2022-2435 CVE-2022-2224 …	Nhóm 32 lỗ hổng trong thiết bị Wordpress cho phép đối tượng tấn công XSS, thu thập thông tin, tải lên tệp tùy ý, SQL Injection, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Windows	CVE-2021-42923	01 lỗ hổng trong sản phẩm Windows (ShowMyPC 3606) cho phép đối tượng tấn công ghi đè tệp và chạy các mã độc hại.	Đã có thông tin xác nhận và bản vá
5	Google	CVE-2022-23745 CVE-2022-1136 CVE-2022-0980 …	Nhóm 34 lỗ hổng trong Google (Capsule Workspace Android, Chrome,..) cho phép đối tượng tấn công làm tràn bộ đệm, thu thập thông tin, cài đặt các tiện ích độc hại, truy cập/thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
6	Dell	CVE-2022-31234 CVE-2022-22555 CVE-2022-33967 …	Nhóm 05 lỗ hổng trong thiết bị Dell (EMC PowerStore, PowerStore,..) cho phép đối tượng tấn công thực thi mã tùy ý, tấn công leo thang đặc quyền, chiếm đoạt tài khoản người dùng	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2021-38936 CVE-2021-29788 CVE-2021-29799 …	Nhóm 13 lỗ hổng trong IBM (QRadar SIEM, Engineering Requirements Quality Assistant On-Premises, …) cho phép đối tượng tấn công thực thu thập thông tin, thực thi mã JavaScript độc hại, truy cập/thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

Thống kê nguy cơ, các cuộc tấn công tại 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 **43,136** (tăng so với tuần trước **37,379)** 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.



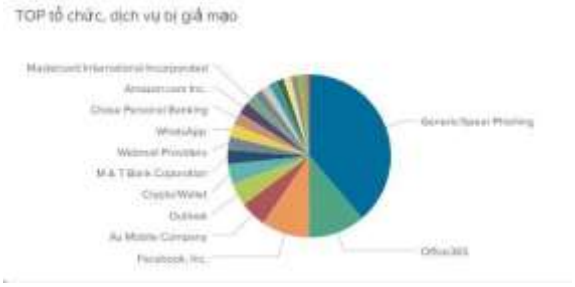


Tấn công Phishing

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, Paypment, 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.

Tấn công Web

Trong tuần, có 245 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 207 trường hợp tấn công lừa đảo (Phishing), 38 trường hợp tấn công cài cắm mã độc.



Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

differentia.ru: 14,688 IP	xjpakmdcfuqe.ru: 191 IP
disorderstatus.ru: 4,919 IP	restlesz.su: 151 IP
atomictrivia.ru: 2,415 IP	xjpakmdcfuqe.in: 145 IP
xjpakmdcfuqe.biz: 735 IP	amnsreiuojy.ru: 70 IP
xjpakmdcfuqe.com: 353 IP	hzmksreiuojy.ru: 46 IP

New

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 27 phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam thông báo 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	https://clmm.tv http://clmm113.me https://trumbemmomo.club https://clmm29.fun	Web lừa đảo cờ bạc qua ví điện tử Momo
2	https://shopee.nhanqua.online/	Giả mạo sàn TMĐT Shopee
3	https://vn-dienmayxanh.com/sua-tu-lanh-tai-nha-hcm/ https://suachuadienmayxanh.com.vn/sua-may-lanh/ https://dienmayxanhhcm24h.com/ https://baohanhdienmayxanhvn.com/ve-sinh-may-lanh/ https://cskh-dienmayxanhvn.com/ dien-may-xanh.net https://trungtammayxanh.com/ve-sinh-may-lanh/	Giả mạo website Điện máy xanh
4	https://nguyenkim.co/dich-vu-sua-chua-may-lanh https://dienlanhnguyenkim.ctyvn.net/	Giả mạo website Điện Máy Nguyễn Kim

Khuyến nghị đối với các cơ quan, đơn vị

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin cảnh báo** 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 **Nguy cơ tấn công mạng từ điểm yếu lỗ hổng**, 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.

***

4. 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.

***

Thông tin liên hệ:

Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 - ais@mic.gov.vn

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