NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 26 (26/6/2023 – 02/07/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Từ MuddyC3 đến PhonyC2: Một vũ khí mới trên không gian mạng được phát triển bởi nhóm MuddyWater của Iran.

- **Cảnh báo:** Người dùng macOS nên cẩn trọng với biến thể mới của mã độc RustBucket

2. Điểm yếu, lỗ hổng

- **675** 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: 280** 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

"Chiến dịch tấn công APT: Từ MuddyC3 đến PhonyC2: Một vũ khí mới trên không gian mạng được phát triển bởi nhóm MuddyWater của Iran"

MuddyWater, nhóm tấn công mạng được hậu thuẫn bởi chính phủ Iran được cho là đang sử dụng một framework C2 chưa từng được phát hiện trước đây có tên là PhonyC2, công cụ đã được nhóm này sử dụng từ năm 2021.

Bằng chứng cho thấy framework này được tạo riêng và đang trong giai đoạn phát triển tích cực. Vào tháng 02/2023, nhóm MuddyWater đã sử dụng Framework PhonyC2 trong chiến dịch tấn công nhằm vào Technion, một viện nghiên cứu tại Israel.

Ngoài ra, một số bằng chứng bổ sung cũng chỉ ra rằng chương trình chạy trên Python 3 có liên quan đến các cuộc tấn công khác của nhóm MuddyWater, bao gồm cả việc liên tục khai thác các máy chủ PaperCut.

Các nhà nghiên cứu bảo mật cho rằng Framework PhonyC2 có cấu trúc và chức năng tương tự với MuddyC3, trong khi framework C2 cũ của nhóm MuddyWater sử dụng Python2. Hiện nay, Framework PhonyC2 đang được cập nhật và thay đổi TTP để tránh bị phát hiện.

Nhóm MuddyWater thực hiện chuỗi tấn công tương tự như các bộ công cụ của Iran-nexus, bằng cách sử dụng các máy chủ công khai dễ bị tấn công và kỹ thuật tấn công xâm nhập thông qua social engineering để tiếp cận mục tiêu.

Framework PhonyC2 được phát hiện vào tháng 4 năm 2023 trên các máy chủ hạ tầng được sử dụng bởi MuddyWater trong cuộc tấn công nhắm vào Technion. Máy chủ này sau đó được xác định là đang lưu trữ một công cụ có tên Ligolo và đang được nhóm tấn công sử dụng.

Sự liên kết với Technion vẫn còn tồn tại trong các vết tích trên hệ thống với hai tập tin "C:\programdata\db.sqlite" và "C:\programdata\db.ps1", cả hai đều được Microsoft mô tả là backdoor PowerShell mà MuddyWater đang sử dụng và được tạo bởi framework PhonyC2 nhằm mục đích thực thi trên thiết bị nhiễm mã độc.

PhonyC2 được mô tả là một framework được sử dụng để tạo các loại payload có khả năng kết nối với máy chủ C&C và chờ lệnh để thực hiện các bước cuối cùng trong chuỗi tấn công xâm nhập (intrusion kill chain).

Nguồn: https://thehackernews.com/2023/06/from-muddyc3-to-phonyc2-irans.html?&web_view=true

"Chiến dịch tấn công APT: Nhóm tấn công APT15 của Trung Quốc trở lại với mã độc Graphican"

Một số câu lệnh đáng chú ý trong framework gồm:

- **Payload:** Tạo ra payload "C:\programdata\db.sqlite" và "C:\programdata\db.ps1" cũng như là lệnh PowerShell để thực thi db.ps1 có nhiệm vụ thực thi db.sqlite

- **Droper:** Tạo một biến thể của câu lệnh PowerShell để tạo "C:\programdata\db.sqlite" bằng cách kết nối tới máy chủ C&C và ghi nội dung được mã hóa gửi về từ máy chủ vào file

- **Execute:** Tạo một biến thể của câu lệnh PowerShell để tạo "C:\programdata\db.ps1" – một đoạn script chứa logic để giải mã db.sqlite – và là giai đoạn cuối cùng
- **List:** Liệt kê toàn bộ thiết bị đang kết nối tới máy chủ C&C
- **Setcommandforall:** Thực thi câu lệnh giống nhau trên tất cả thiết bị đang kết nối tới máy chủ cùng một lúc.
- **Use:** Tạo một PowerShell shell trên thiết bị từ xa để thực thi nhiều lệnh hơn
- **Persist:** Tạo một đoạn mã PowerShell cho phép đối tượng tấn công có khả năng duy trì kết nối trên thiết bị nhiễm mã độc, qua đó tự động kết nối thiết bị tới máy chủ mỗi khi khởi động lại.

MuddyWater không phải là nhóm tấn công duy nhất của Iran thực hiện các chiến dịch nhằm vào Israel. Trong những tháng gần đây, đã có nhiều nhóm tấn công khác nhau như Charming Kitten (APT35), Imperial Kitten (Tortoiseshell) và Agrius (Pink Sandstorm) nhắm vào nhiều đối tượng mục tiêu tại Israel.

Các chuyên gia bảo mật cho rằng framework C2 như PhonyC2 đóng vai trò quan trọng trong việc cho phép nhóm tấn công ẩn danh và thu thập dữ liệu từ các nạn nhân, đồng thời chỉ ra PhonyC2 không phải là framework C2 tự chế đầu tiên cũng như là cuối cùng được MuddyWater sử dụng trong các chiến dịch tấn công nghiêm trọng.

Nguồn: https://thehackernews.com/2023/06/from-muddyc3-to-phonyc2-irans.html?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Người dùng macOS nên cẩn trọng với biến thể mới của mã độc RustBucket"

Mới đây, các nhà nghiên cứu đã phát hiện một biến thể mới của RustBucket, một loại mã độc nhằm vào hệ điều hành macOS, được phát triển bởi BlueNoroff - một đối tượng tấn công thuộc nhóm Lazarus của Triều Tiên. Phiên bản mới này đã được cải tiến để cài đặt một cách bền vững và tránh bị phát hiện bởi phần mềm bảo mật.

Vào tháng 04/2023, phát hiện mã độc REF9135 sử dụng một backdoor dựa trên AppleScript có khả năng truy xuất payload bậc hai từ máy chủ từ xa.

Mã độc phụ này được viết bằng Swift và được thiết kế để tải xuống mã độc chính từ máy chủ C&C, đó là một tệp nhị phân dựa trên Rust với các tính năng thu thập thông tin trái phép và thực thi các tệp Mach-O bổ sung nhị phân hoặc tập lệnh shell trên hệ thống đã bị xâm nhập.

Đây là phiên bản đầu tiên của mã độc BlueNoroff nhắm vào người dùng macOS.

Chuỗi lây nhiễm bao gồm một trình cài đặt macOS tạo ra backdoor trình đọc PDF. Phần lớn các cuộc tấn công sẽ kích hoạt khi tệp PDF được mã hóa để khởi chạy trình đọc PDF giả mạo. Các hoạt động xâm nhập ban đầu bao gồm việc gửi email lừa đảo và sử dụng tài khoản giả mạo trên các mạng xã hội như LinkedIn.

Các cuộc tấn công nhằm mục tiêu chủ yếu vào các tổ chức liên quan đến tài chính ở Châu Á, Châu u và Hoa Kỳ để thu lợi bất hợp pháp.

Cơ chế hoạt động của phiên bản mới này hoạt động thông qua việc:

- Thêm một tệp plist tại đường dẫn /Users/<user>/Library/LaunchAgents/com.apple.systemupdate.plist;
- Sao chép tệp nhị phân của mã độc vào theo đường dẫn /Users/<user>/Library/Metadata/SystemUpdate.
- Đồng thời, RustBucket còn sử dụng miền Domain DNS (docsend.linkpc[.]net) để gửi tập lệnh và chiếm quyền kiểm soát.

Người dùng cần kiểm tra kỹ các email hay tài khoản trước khi nhấp chuột vào bất kỳ liên kết đính kèm nào. Đồng thời, người dùng cần lưu ý cập nhật các bản vá mới và sớm nhất để tránh nguy cơ bị khai thác bởi loại mã độc này.

Nguồn: https://thehackernews.com/2023/07/beware-new-rustbucket-malware-variant.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 **675** lỗ hổng, trong đó có 96 lỗ hổng mức Cao, 192 lỗ hổng mức Trung bình, 09 lỗ hổng mức Thấp và 378 lỗ hổng chưa đánh giá. Trong đó có ít nhất 81 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 11 lỗ hổng trong Microsoft, Nhóm 12 lỗ hổng trong Linux, Nhóm 32 lỗ hổng trong Trend Micro, Nhóm 97 lỗ hổng trong Wordpress, Nhóm 32 lỗ hổng trong Dell, Nhóm 70 lỗ hổng trong Apple, 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-2022-29144, CVE-2022-29146,...*
- *Linux: CVE-2023-1206, CVE-2023-1295,…*
- *Trend Micro: CVE-2023-32524, CVE-2023-32527,...*
- *Wordpress: CVE-2020-36742, CVE-2020-36743,...*
- *Dell: CVE-2023-28073, CVE-2023-28065,...*
- *Apple: CVE-2023-28191, CVE-2023-28202,...*
- *IBM: CVE-2022-34352, CVE-2023-26273,…*

Thông tin điểm yếu, lỗ hổng

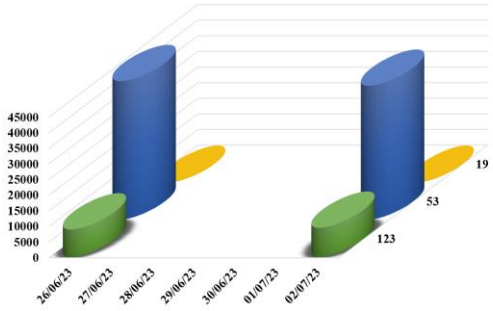
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2022-29144 CVE-2022-29146 CVE-2021-31937 …	Nhóm 11 lỗ hổng trong Microsoft (Edge,…) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, tấn công từ chối dịch vụ, làm rò rỉ thông tin dữ liệu nhạy cảm.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-1206 CVE-2023-1295 CVE-2023-3357 …	Nhóm 12 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công làm rò rỉ thông tin dữ liệu, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Trend Micro	CVE-2023-32524 CVE-2023-32527 CVE-2023-32528 …	Nhóm 32 lỗ hổng trong Trend Micro 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
4	Wordpress	CVE-2020-36742 CVE-2020-36743 CVE-2020-36744 …	Nhóm 97 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công XSS, SQL injection, tiết lộ thông tin nhạy cảm, tải lên các tệp tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
5	Dell	CVE-2023-28073 CVE-2023-28065 CVE-2023-25936 …	Nhóm 32 lỗ hổng trong Dell (BIOS,..) cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
6	Apple	CVE-2023-28191 CVE-2023-28202 CVE-2023-32352 …	Nhóm 70 lỗ hổng trong Apple cho phép đối tượng tấn công làm rò rỉ thông tin dữ liệu nhạy cảm, 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-2022-34352 CVE-2023-26273 CVE-2023-26276 …	Nhóm 09 lỗ hổng trong IBM phép đối tượng tấn công 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

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

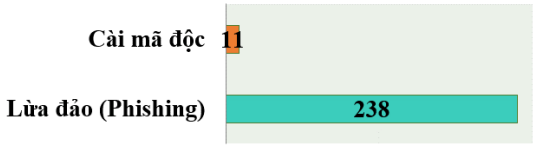
Tấn công DRDoS

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 **52.307,** (giảm so với tuần trước **53.243**) 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

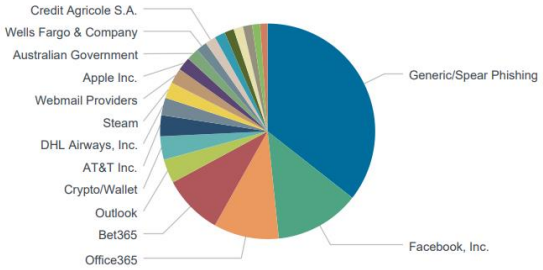


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 249 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 238 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: 13022 IP	xjpakmdcfuqe.ru:141 IP
disorderstatus.ru: 5246 IP	xjpakmdcfuqe.in:92 IP
atomictrivia.ru: 2487 IP	restlesz.su: 336 IP
xjpakmdcfuqe.biz: 355 IP	amnsreiuojy.ru: 549 IP
xjpakmdcfuqe.com: 193 IP	hzmksreiuojy.ru: 62 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **280** 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	vaba11.com	Website giả mạo sàn TMĐT Tiki
2	shopepvip.com vvshopp.com	Website giả mạo sàn TMĐT Shopee
3	mxl167280.com	Website giả mạo sàn TMĐT Lazada
4	muahebengiadiiinh2023.weebly.com	Website giả mạo Facebook
5	zzb.lol	Website giả mạo Dịch vụ công Quốc Gia
6	smartphonethongminh.online	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 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