NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 29 (17/7/2023 – 23/07/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** FIN8 phát tán mã độc Noberus Ransomware bằng phiên bản nâng cấp của Sardonic Backdoor.

- **Cảnh báo:** Biến thể mới của mã độc AsyncRAT lây lan qua các phần mềm vi phạm bản quyền.

2. Điểm yếu, lỗ hổng

- **523** 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: 288** 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: FIN8 phát tán mã độc Noberus Ransomware bằng phiên bản nâng cấp của Sardonic Backdoor"

Gần đây, các chuyên gia bảo mật đã phát hiện nhóm APT Syssphinx (còn được gọi là FIN8) đang phát triển phiên bản nâng cấp của Sardonic backdoor để phát tán mã độc ransomware Noberus. Mặc dù backdoor này thuộc framework Sardonic đã từng được nhóm này sử dụng trước đó và bị phát hiện vào năm 2021, nhưng hầu hết các tính năng của nó đã được chỉnh sửa với giao diện mới.

Syssphinx (còn được gọi là FIN8) là một nhóm tấn công có động cơ tài chính hoạt động từ tháng 1 năm 2016. Nhóm này nổi tiếng với việc tấn công các tổ chức trong lĩnh vực chăm sóc khách hàng, bán lẻ, giải trí, bảo hiểm, công nghệ, hóa chất và tài chính. Syssphinx sử dụng các chiến thuật "living-off-the-land", tận dụng các công cụ và giao diện tích hợp sẵn như PowerShell và WMI, lợi dụng các dịch vụ hợp pháp trong hệ thống để ngụy trang cho các hoạt động tấn công mạng của mình. Kỹ thuật "social engineering" và "spear-phishing" là hai phương thức mà nhóm này thường sử dụng để bước đầu xâm nhập vào các tổ chức.

Syssphinx and Ransomware

Ban đầu, Syssphinx chủ yếu tấn công vào POS tại các điểm bán hàng, nhưng trong vài năm gần đây nhóm này đã chuyển sang sử dụng ransomware trong các chiến dịch tấn công. Vào tháng 6 năm 2021, lần đầu tiên nhóm APT Syssphinx bị phát hiện phát tán mã độc ransomware Ragnar Locker để tấn công một công ty dịch vụ tài chính tại Mỹ.

Vào tháng 01 năm 2022, Syssphinx đã sử dụng một nhóm các biến thể mã độc ransomware có tên White Rabbit thông qua một đoạn URL độc hại. Syssphinx đã sử dụng phiên bản nâng cấp của Sardonic backdoor để triển khai chiến dịch phán tán mã độc White Rabbit. Sau đó, vào tháng 12 năm 2022, nhóm này tiếp tục phát tán mã độc ransomware Noberus (còn được gọi là ALPHV hoặc BlackCat) trong các cuộc tấn công cùng với nhóm tấn công Coreid (hay còn được biết đến với các tên khác như Blackmatter, Carbon Spider, FIN7).

Việc nhóm Syssphinx chuyển sang sử dụng ransomware là dấu hiệu cho thấy các nhóm tấn công mạng đang thay đổi chiến lược tấn công bằng cách đa dạng hóa lĩnh vực nhằm tối ưu hóa lợi nhuận từ các tổ chức bị tấn công.

Backdoor

Đặc biệt, Syssphinx thường tạm dừng hoạt động giữa các chiến dịch tấn công nhằm cải thiện chiến thuật, kỹ thuật và quy trình (TTPs) của nhóm.

Từ năm 2019, Syssphinx đã sử dụng backdoor có tên Badhatch trong các cuộc tấn công. Sau đó, vào tháng 12 năm 2020 và tháng 1 năm 2021, nhóm này đã cập nhật và nâng cấp Badhatch.

Vào tháng 8 năm 2021, Syssphinx tiếp tục phát triển và triển khai một backdoor mới mang tên Sardonic. Sardonic là một backdoor dựa trên ngôn ngữ lập trình C++ với khả năng thu thập thông tin và thực thi lệnh. Backdoor này cũng có hệ thống plugin để tải và thực thi các payload mã độc khác qua dạng DLL.

Gần đây, backdoor Sardonic được phát hiện với phiên bản mới nhất vào năm 2022. Phiên bản nâng cấp này đã thay đổi giao diện và không còn sử dụng thư viện C++. Thêm vào đó, một số tính năng hướng đối tượng đã được thay thế bằng ngôn ngữ lập trình C thông thường.

Mục tiêu của quá trình nâng cấp backdoor chủ yếu là thay đổi giao diện để tránh bị phát hiện. Tuy nhiên, Syssphinx vẫn sử dụng các kỹ thuật quen thuộc trong các cuộc tấn công gần đây.

Qua việc mở rộng đối tượng tấn công từ các điểm POS sang ransomware, không ngừng nâng cấp công cụ và chiến thuật tấn công trong một thời gian dài cho thấy Syssphinx là mối đe dọa nghiêm trọng đối với các tổ chức có các hoạt động liên quan đến tài chính.

Nguồn: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/Syssphinx-FIN8-backdoor?web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Biến thể mới của mã độc AsyncRAT lây lan qua các phần mềm vi phạm bản quyền"

HotRat là một biến thể mới của mã độc AsyncRAT, hiện đang được phát tán thông qua các phần mềm vi phạm bản quyền miễn phí vi phạm bản quyền như Microsoft Office và các phần mềm, tiện ích phổ biến khác.

Mã độc HotRat cho phép đối tượng tấn công đánh cắp thông tin đăng nhập, ví điện tử, chụp ảnh màn hình, cài cắm các mã độc khác và giành quyền truy cập hoặc thay đổi dữ liệu của người dùng.

Theo các nhà nghiên cứu bảo mật, trojan này đã trở nên phổ biến từ tháng 10/2022, mục tiêu nhắm đến tập trung chủ yếu ở Thái Lan, Guyana, Libya, Suriname, Mali, Pakistan, Campuchia, Nam Phi và Ấn Độ.

Các cuộc tấn công sử dụng phần mềm crack có sẵn trên trang web Torrent và lệnh AutoHotkey AHK để khởi tạo chuỗi lây nhiễm đã được thiết kế trước, vô hiệu hóa phần mềm chống vi-rút trên máy chủ bị xâm nhập, và cuối cùng triển khai payload HotRat thông qua Visual Basic Script VBS.

Mã độc HotRat là một mã trojan truy cập từ xa RAT (Remote access trojan), đi kèm với gần 20 lệnh, mỗi lệnh thực thi một module .NET từ máy chủ từ xa, cho phép đối tượng tấn công mở rộng các tính năng trái phép. Cuộc tấn công nhằm nâng cao đặc quyền quản trị của đối tượng tấn công để thu thập dữ liệu trái phép.

Để tránh lây nhiễm mã độc, người dùng không nên tải xuống những phần mềm và trò chơi điện tử từ các trang web không chính thức. Đồng thời, luôn cập nhật trình duyệt và hệ điều hành bằng các bản vá bảo mật.

Nguồn: https://thehackernews.com/2023/07/hotrat-new-variant-of-asyncrat-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 **523** lỗ hổng, trong đó có 46 lỗ hổng mức Cao, 51 lỗ hổng mức Trung bình, 13 lỗ hổng mức Thấp và 413 lỗ hổng chưa đánh giá. Trong đó có ít nhất 70 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 04 lỗ hổng trong Microsoft, Nhóm 13 lỗ hổng trong Linux, Nhóm 02 lỗ hổng trong Asus, Nhóm 67 lỗ hổng trong Wordpress, Nhóm 02 lỗ hổng trong Adobe, Nhóm 58 lỗ hổng trong Oracle, Nhóm 20 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-2023-38187, CVE-2023-36887,...*
- *Linux: CVE-2023-38409, CVE-2023-38426,...*
- *Asus: CVE-2023-35086, CVE-2023-21247*
- *Wordpress: CVE-2023-3714, CVE-2023-3813,...*
- *Adobe: CVE-2023-38203, CVE-2021-39822*
- *Oracle: CVE-2023-21994, CVE-2023-22037,...*
- *IBM: CVE-2022-43908, CVE-2022-43910,...*

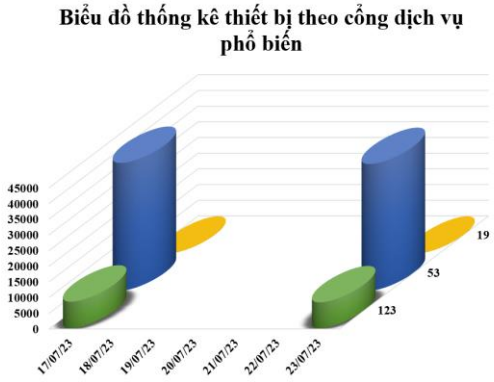
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-38187 CVE-2023-36887 CVE-2023-35392 …	Nhóm 04 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện leo thang đặc quyền, thực thi mã từ xa, thực hiện lỗi Spoofing, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2023-38409 CVE-2023-38426 CVE-2023-38427 …	Nhóm 13 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Asus	CVE-2023-35086 CVE-2023-35087	Nhóm 02 lỗ hổng trong Asus cho phép đối tượng tấn công thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-3714 CVE-2023-3813 CVE-2023-3459 …	Nhóm 67 lỗ hổng trong Wordpress cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
5	Adobe	CVE-2023-38203 CVE-2021-39822	Nhóm 02 lỗ hổng trong Adobe 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
6	Oracle	CVE-2023-21994 CVE-2023-22022 CVE-2023-22037 …	Nhóm 58 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
7	IBM	CVE-2022-43908 CVE-2022-43910 CVE-2023-25929 …	Nhóm 19 lỗ hổng trong IBM phép đối tượng tấn công thực thi mã tùy ý, 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

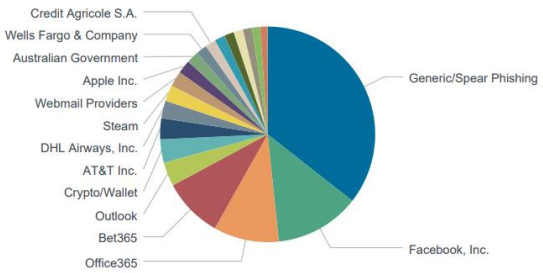
Tấn công DRDoS

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 **48.688**, (giảm so với tuần trước **49.275**) 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 738 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 725 trường hợp tấn công lừa đảo (Phishing), 13 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: 8634 IP	xjpakmdcfuqe.ru:272 IP
disorderstatus.ru: 4001 IP	xjpakmdcfuqe.in: 56 IP
atomictrivia.ru: 1935 IP	restlesz.su: 286 IP
xjpakmdcfuqe.biz: 169 IP	amnsreiuojy.ru: 272 IP
xjpakmdcfuqe.com: 98 IP	hzmksreiuojy.ru: 24 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **288** 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	vietgov5.cc	Website giả mạo cổng Dịch vụ công Quốc Gia
2	anzvn.net	Website giả mạo Công ty TNHH Aeon Việt Nam
3	sendovip.com	Website giả mạo sàn TMĐT Sendo
4	dichvucongbaohiemxahoi.com dangkyhosotructuyen2023.com handico.vaytienmat-nhanh24h.com …	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 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