NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 25 (19/6/2023 – 25/6/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

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

- **Cảnh báo:** Chiến dịch tấn công tiền điện tử mới nhắm vào hệ thống Linux và Internet of Things (IoT).

2. Điểm yếu, lỗ hổng

- **562** 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: 289** 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 tấn công APT15 của Trung Quốc trở lại với mã độc Graphican"

Gần đây, một nhóm tấn công do chính phủ Trung Quốc hậu thuẫn có tên là APT15 đã sử dụng backdoor Graphican trong chiến dịch tấn công diễn ra từ khoảng cuối năm 2022 cho tới đầu năm 2023.

Nhóm APT15 còn có các tên gọi khác như Nickel, Flea, Ke3Chang và Vixen Panda đã hoạt động kể từ năm 2004 và thường nhằm mục tiêu vào các tổ chức công và tư có tiếng trên thế giới.

Nhóm này đã sử dụng nhiều loại mã độc và các backdoor tự chế trong thời gian hoạt động bao gồm: RoyalCLI và Royal DNS, Okrum, Ketrum, cùng với các phần mềm gián điệp (spyware) trên hệ điều hành Android như SilkBean và Moonshine.

Hiện nay, các chuyên gia bảo mật cảnh báo rằng chiến dịch mới nhất của APT15 đang nhằm vào các cơ quan Bộ Ngoại giao đặt tại Trung Mỹ và Nam Mỹ.

Backdoor Graphican

Theo báo cáo, Graphican là một phiên bản nâng cấp của một mã độc đã từng được sử dụng bởi nhóm APT15 chứ không phải là một công cụ hoàn toàn mới.

Điểm đáng chú ý của mã độc này là việc sử dụng Microsoft Graph API và OneDrive để mã hóa địa chỉ của hạ tầng điều khiển C&C, khiến cho mã độc trở nên linh hoạt và có khả năng chống cự trước các cuộc tấn công.

Hoạt động của Graphican trên một thiết bị nhiễm mã độc được mô tả như sau:

• Vô hiệu hóa "wizard chạy lần đầu" (first-run wizard) và trang chào mừng của Internet Explorer 10 bằng cách sử dụng khóa registry.

• Xác minh xem tiến trình 'iexplore.exe' có đang hoạt động hay không.

• Xây dựng một đối tượng COM global – IwebBrowser2 để truy cập internet.

• Xác thực với Microsoft Graph API để lấy mã thông báo truy cập hợp lệ (access token) và mã làm mới (refresh_token).

• Liệt kê các tệp và thư mục con trong thư mục "Person" trên OneDrive bằng cách sử dụng Graph API.

• Giải mã tên thư mục đầu tiên để sử dụng nó làm máy chủ điều khiển (C&C server).

• Tạo một Bot ID duy nhất bằng cách sử dụng tên máy chủ, địa chỉ IP cục bộ, phiên bản Windows, định danh ngôn ngữ mặc định và kiểu bit của tiến trình (32/64-bit).

• Thêm bot vào máy chủ điều khiển bằng cách sử dụng chuỗi định dạng cụ thể được tạo bởi dữ liệu đã thu thập được trên máy của nạn nhân.

• Thường xuyên kiểm tra máy chủ điều khiển để tìm các câu lệnh mới cần thực thi.

Nguồn:
https://www.bleepingcomputer.com/news/security/chinese-apt15-hackers-resurface-with-new-graphican-malware/?&web_view=true

Tin tức An toàn thông tin

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

Khi kết nối với máy chủ điều khiển C&C, đối tượng tấn công có thể đưa ra các câu lệnh để thực thi trên máy nhiễm mã độc, bao gồm việc khởi chạy các chương trình và tải các file mới về.

Danh sách các câu lệnh được gửi từ máy chủ điều khiển cho Graphican gồm có:

- C – Tạo một dòng lệnh tương tác (command line) được điều khiển từ máy chủ C&C.
- U – Tạo một tệp tin trên máy tính từ xa.
- D – Tải một tệp tin từ thiết bị nhiễm mã độc vào máy chủ điều khiển C&C.
- N – Tạo một tiến trình mới với cửa sổ ẩn.
- P – Tạo một tiến trình PowerShell mới với cửa sổ ẩn và lưu lại các kết quả vào một tệp tạm thời trong thư mục TEMP, sau đó gửi các kết quả này về máy chủ điều khiển C&C.

Một số công cụ khác được các nhà nghiên cứu bảo mật chỉ ra trong chiến dịch mới nhất của APT15 bao gồm:

- EWSTEW – Backdoor tự chế của nhóm APT15 dùng để thu thập các email từ máy chủ Microsoft Exchange bị nhiễm mã độc.
- Mimikatz, Pypykatz, Safetykatz – Các công cụ lấy thông tin đăng nhập của người dùng (credential dumping), lợi dụng việc nhớ thông tin đăng nhập (Windows single - Sign On là một tính năng trong hệ điều hành Windows cho phép người dùng đăng nhập vào một lần và sử dụng chứng chỉ xác thực đó để truy cập nhiều ứng dụng và dịch vụ khác nhau mà không cần phải nhập lại thông tin đăng nhập) để trích xuất mật khẩu từ bộ nhớ.
- Lazagne – Công cụ mã nguồn mở dùng để thu thập mật khẩu từ nhiều ứng dụng khác nhau.
- Quarks PwDump – Trích xuất hàng loạt các thông tin xác thực của Windows. Được phát hiện vào năm 2013.
- SharpSecDump – Phiên bản .net của secretsdump.py của Impacket, được dùng để trích xuất hàng loạt các thông tin bí mật từ xa trong SAM và LSA.
- K8Tools – Một bộ công cụ có khả năng leo thang đặc quyền, phá mật khẩu, quét, khai thác lỗ hổng và tấn công vào các hệ thống khác nhau.
- EHole – Xác định các sơ hở của hệ thống dễ bị tấn công.
- Web shells – AntSword, Behinder, China Chopper, Godzilla là các webshell cho phép đối tượng tấn công truy cập backdoor để xâm nhập vào các hệ thống.
- CVE-2020-1472 – Lỗ hổng leo thang đặc quyền ảnh hưởng đến giao thức Netlogon Remote Protocol.

Tóm lại, các hoạt động gần đây của APT15 cùng với việc cập nhật lại backdoor tự chế cho thấy các nhóm tấn công mạng có liên quan đến Trung Quốc vẫn đang là một mối đe dọa hiện hữu đối với các tổ chức trên toàn cầu, thông qua việc nâng cấp công cụ, điều chỉnh quá trình hoạt động kín đáo và bí ẩn hơn.

Nhóm tấn công này sử dụng các email phishing làm vector lây nhiễm; tuy nhiên, nhóm này cũng được biết tới với việc khai thác lỗ hổng trên các thiết bị điểm cuối có kết nối tới Internet và sử dụng VPN làm vector truy cập khởi điểm.

Nguồn: https://www.bleepingcomputer.com/news/security/chinese-apt15-hackers-resurface-with-new-graphican-malware/?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Chiến dịch tấn công tiền điện tử mới nhắm vào hệ thống Linux và Internet of Things (IoT)"

Một chiến dịch mới đã được triển khai nhằm tấn công các thiết bị Linux và Internet of Things (IoT) nhằm mục đích khai thác trái phép tiền điện tử.

Các đối tượng tấn công sử dụng một backdoor nhằm triển khai các công cụ và cài đặt rootkit cùng với bot IRC để đánh cắp dữ liệu của thiết bị. Backdoor được cài cắm vào phần mềm OpenSSH đã được vá lỗi trên các thiết bị ảnh hưởng, cho phép đối tượng tấn công đánh cắp thông tin đăng nhập SSH để duy trì truy cập trên thiết bị, xâm nhập vào mạng nội bộ và che giấu các kết nối SSH độc hại khác.

Để tiến hành kế hoạch tấn công này, các máy chủ Linux sẽ được cấu hình để yêu cầu quyền truy cập ban đầu. Sau đó, đối tượng tấn công thực hiện vô hiệu hóa lịch sử trình duyệt đồng thời cài cắm phiên bản OpenSSH bị trojan hóa. Phiên bản OpenSSH giả mạo được cấu hình để cài đặt để khởi chạy backdoor và một tập lệnh shell cho phép đối tượng tấn công triển khai các payload bổ sung và backdoor khai thác khác.

Điều này cho phép kẻ tấn công lấy trộm thông tin từ các thiết bị, cài đặt rootkit Reptile và Diamorphine nhằm che giấu hoạt động độc hại trên các hệ thống bị xâm nhập. Để đảm bảo quyền truy cập liên tục vào thiết bị thông qua SSH, backdoor sẽ thêm hai public key vào tệp authorized_keys của tất cả người dùng trên hệ thống.

Các đối tượng tấn công cũng cố gắng giành quyền sử dụng độc quyền các tài nguyên trên hệ thống bị nhiễm bằng cách loại bỏ các chương trình khai thác tiền điện tử cạnh tranh có thể đã được chạy trước đó.

Ngoài ra, mã độc này còn chạy một phiên bản sửa đổi của ZiggyStarTux, đây là một ứng dụng khách cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DDoS) dựa trên bot IRC, có khả năng thực thi các lệnh bash được đưa ra từ máy chủ điều khiển và điều hành (C&C). Mã độc này dựa trên một botnet khác được gọi là Kaiten (hay còn được gọi là Tsunami).

Cuộc tấn công tận dụng tên miền phụ của một tổ chức tài chính giấu tên ở Đông Nam Á làm đường truyền cho máy chủ C&C, nhằm mục đích ngụy trang lưu lượng độc hại của nó.

Các cuộc tấn công nhằm vào các máy chủ Linux bằng mã độc khai thác tiền điện tử và một biến thể botnet Tsunami được gọi là Ziggy đã trở nên phổ biến.

Để tránh trở thành nạn nhân của các chiến dịch tấn công tương tự, người dùng nên thiết lập hạn chế truy cập đến các thiết bị của mình, tắt các cổng (port) và các dịch vụ không sử dụng. Đồng thời cập nhật đầy đủ các bản vá bảo mật cho các phần mềm, ứng dụng trên các thiết bị.

Nguồn: https://thehackernews.com/2023/06/new-cryptocurrency-mining-campaign.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 **562** lỗ hổng, trong đó có 19 lỗ hổng mức Cao, 20 lỗ hổng mức Trung bình, 0 lỗ hổng mức Thấp và 523 lỗ hổng chưa đánh giá. Trong đó có ít nhất 68 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 03 lỗ hổng trong Microsoft, Nhóm 12 lỗ hổng trong Linux, Nhóm 03 lỗ hổng trong Fortinet, Nhóm 99 lỗ hổng trong Wordpress, Nhóm 35 lỗ hổng trong Dell, Nhóm 70 lỗ hổng trong Apple, Nhóm 02 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-2023-32027, CVE-2023-32028,...*
- *Linux: CVE-2023-3212, CVE-2023-3220,…*
- *Fortinet: CVE-2023-33306, CVE-2023-33307,...*
- *Wordpress: CVE-2023-3325, CVE-2023-3387,...*
- *Dell: CVE-2023-25936, CVE-2023-25937,...*
- *Apple: CVE-2023-28191, CVE-2023-28202,...*
- *IBM: CVE-2023-33842, CVE-2023-28956.*

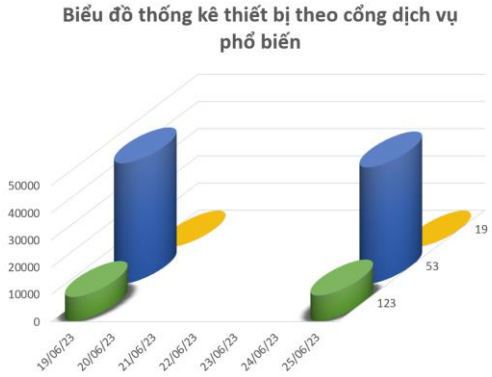
Thông tin điểm yếu, lỗ hổng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-32027 CVE-2023-32028 CVE-2023-33141	Nhóm 03 lỗ hổng trong Microsoft (SQL Server) cho phép đối tượng tấn công thực thi mã từ xa, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
2	Linux	CVE-2023-3212 CVE-2023-3220 CVE-2023-3317 …	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.	Chưa có thông tin xác nhận và bản vá
3	Fortinet	CVE-2023-33306 CVE-2023-33307 CVE-2023-33299	Nhóm 03 lỗ hổng trong Fortinet (FortiOS, FortiNAC) 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-2023-3325 CVE-2023-3387 CVE-2023-3320 …	Nhóm 99 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-2023-25936 CVE-2023-25937 CVE-2023-25938 …	Nhóm 35 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-2023-28204	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-2023-33842 CVE-2023-28956	Nhóm 02 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

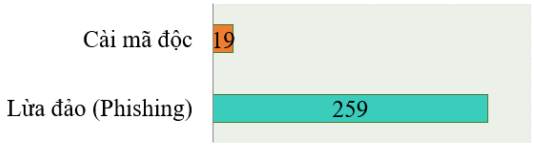
Thông kê nguy cơ, các cuộc tấn công mạng vào Việt Nam

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.

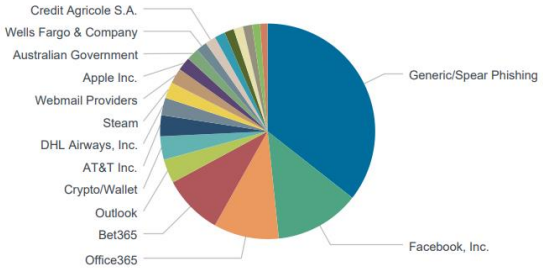


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có 278 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 259 trường hợp tấn công lừa đảo (Phishing), 19 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: 16696 IP	xjpakmdcfuqe.ru:144 IP
disorderstatus.ru: 5365 IP	xjpakmdcfuqe.in:103 IP
atomictrivia.ru: 2488 IP	restlesz.su: 336 IP
xjpakmdcfuqe.biz: 489 IP	amnsreiuojy.ru: 885 IP
xjpakmdcfuqe.com: 215 IP	hzmksreiuojy.ru: 62 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **289** 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	tadcb.com tadcqv.com aets22.com aets88.com 009855.com aets99.com tiki588.com	Website giả mạo sàn TMĐT Tiki
2	vnshop111.com	Website giả mạo sàn TMĐT Shopee

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