NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 41 (09/10/2023 – 15/10/2023)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Grayling - Nhóm APT mới xuất hiện tấn công nhiều tổ chức tại Đài Loan.

- **Cảnh báo:** Microsoft phát hành bản vá tháng 10/2023 cho 103 lỗi, trong đó có 2 lỗi đang bị khai thác.

2. Điểm yếu, lỗ hổng

- **711** 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: 302** 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: Grayling - Nhóm APT mới xuất hiện tấn công nhiều tổ chức tại Đài Loan"

Nhóm APT Grayling là một nhóm tấn công mạng chưa từng được biết đến trước đây và mới được phát hiện vào năm 2023. Grayling đã sử dụng mã độc tùy chỉnh cùng một số bộ công cụ có sẵn để tấn công các tổ chức tại Đài Loan trong lĩnh vực sản xuất, công nghệ thông tin và y tế. Chiến dịch tấn công này cũng nhằm vào các cơ quan chính phủ tại Quần đảo Thái Bình Dương, Việt Nam và Mỹ. Grayling đã bắt đầu chiến dịch này từ 02/2023 cho tới tháng 05/2023.

Hoạt động của nhóm APT Grayling

Grayling đã thực hiện một chiến dịch tấn công phức tạp với nhiều kỹ thuật và công cụ để tiếp cận và tấn công đối tượng mục tiêu. Nhóm này khởi đầu cho chuỗi hoạt động tấn công bằng cách tận dụng cơ sở hạ tầng công khai để truy cập vào thiết bị của nạn nhân. Trước khi thực hiện hoạt động DLL sideloading, Grayling đã triển khai các Web shell trên một số thiết bị bị xâm nhập. Kỹ thuật này được sử dụng để tải các phần mềm độc hại, bao gồm: Cobalt Strike, NetSpy và framework Havoc. Đây là cách nhóm Grayling chiếm quyền truy cập vào thiết bị nạn nhân và thực hiện tấn công leo thang đặc quyền, quét hệ thống mạng và sử dụng các bộ tải. Quy trình và các kỹ thuật tấn công (TTPs) trong chiến dịch bao gồm:

- Havoc: Một framework mã nguồn mở có khả năng thực thi nhiều tác vụ như: thực thi câu lệnh, quản lý tiến trình, tải xuống payload, điều khiển token của Windows và thực thi shellcode.
- Cobalt Strike: Công cụ cho phép thực thi lệnh, chèn tiến trình, giả mạo tiến trình, tải lên và tải xuống tệp tin. Đây là một ứng dụng kiểm thử hợp pháp nhưng thường bị lợi dụng để thực hiện các hoạt động độc hại khác.
- NetSpy: Công cụ gián điệp công khai.
- Khai thác lỗ hổng CVE-2019-0803 để leo thang đặc quyền Windows.
- Mimikatz: Công cụ khai thác thông tin xác thực.
- Vô hiệu hóa các tiến trình không mong muốn.
- Downloaders được sử dụng để tải các phần mềm độc hại sau khi đối tượng tấn công đã xâm nhập vào hệ thống mục tiêu.
- Một số payload chưa rõ được tải xuống từ imfsb.ini

Một điểm đáng chú ý trong cách thức tấn công của nhóm APT Grayling là sử dụng kỹ thuật DLL sideloading thông qua API SbieDll_Hook với bộ giải mã tùy chỉnh để triển khai payload. Nhóm này đã sử dụng hàng loạt các kỹ thuật và công cụ để tiến hành chiến dịch tấn công tinh vi, bao gồm việc tận dụng cơ sở hạ tầng công khai, triển khai Web shell, sử dụng DLL sideloading và thực hiện tấn công ngay sau khi chiếm quyền kiểm sát các thiết bị của nạn nhân.

Động cơ của nhóm APT Grayling

Động cơ chính của Grayling là thu thập thông tin vì không có bằng chứng cho thấy nhóm này trích xuất dữ liệu từ các thiết bị người dùng. Nhóm này sử dụng kỹ thuật tùy chỉnh và công cụ có sẵn để tấn công nhằm vượt qua phần mềm bảo mật và tránh bị phát hiện. Việc sử dụng công cụ có sẵn và ngắt tiến trình cho thấy nhóm này ưu tiên việc che giấu hoạt động và nguồn gốc của chiến dịch tấn công. Hiện chưa xác định nhóm APT Grayling đang hoạt động tại quốc gia nào.

Nguồn: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks?web_view=true

Tin tức An toàn thông tin

"Cảnh báo: Microsoft phát hành bản vá tháng 10/2023 cho 103 lỗi, trong đó có 2 lỗi đang bị khai thác"

Trong bản vá Patch Tuesday của tháng 10/2023, Microsoft đã khắc phục tổng cộng 103 lỗ hổng bảo mật. Trong số này, có 13 lỗ hổng được đánh giá là Nghiêm trọng và 90 lỗ hổng quan trọng. Những lỗ hổng này không liên quan đến 18 lỗ hổng bảo mật trước đây đã được vá trên trình duyệt Edge.

Có hai trong số 103 lỗ hổng được phát hiện đang bị khai thác trong các cuộc tấn công zero-day, cụ thể như sau:

- CVE-2023-36562 (Điểm CVSS: 6.5): Lỗ hổng làm lộ lọt thông tin trong Microsoft WordPad.
- CVE-2023-41763 (Điểm CVSS: 5.3): Lỗ hổng leo thang đặc quyền trên ứng dụng "Skype for Business" có thể dẫn tới việc lộ lọt thông tin quan trọng như địa chỉ IP, cho phép đối tượng tấn công truy cập vào mạng nội bộ.

Để khai thác lỗ hổng CVE-2023-36563, ban đầu, đối tượng tấn công cần đăng nhập vào hệ thống và thực thi một ứng dụng tùy chỉnh để chiếm quyền kiểm soát. Bên cạnh đó, thông qua việc khai thác lỗ hổng này, các đối tượng tấn công cũng có thể dẫn dụ người dùng mở file độc hại qua email hoặc tin nhắn.

Ngoài ra, bản vá tháng 10/2023 cũng giải quyết một loạt các lỗ hổng liên quan đến Microsoft Message Queuing (MSMQ) và giao thức Layer 2 Tunneling, có thể dẫn đến thực thi mã từ xa và từ chối dịch vụ. Microsoft cũng đã vá một lỗ hổng leo thang đặc quyền nghiêm trọng trên Windows IIS Server (CVE-2023-36434, Điểm CVSS: 9.8) cho phép đối tượng tấn công giả mạo và đăng nhập dưới tên người dùng khác thông qua brute-force.

Microsoft đã phát hành một bản vá cho lỗ hổng CVE-2023-44487, hay còn gọi là tấn công HTTP/2 Rapid Reset, đã bị các tác nhân chưa rõ danh tính sử dụng như một lỗ hổng zero-day để thực hiện các cuộc tấn công phân tán từ chối dịch vụ (DDoS). Mặc dù cuộc tấn công DDoS này có khả năng làm ảnh hưởng đến tính khả dụng của dịch vụ, nhưng nó không dẫn đến việc lộ lột dữ liệu khách hàng.

Cuối cùng, Microsoft thông báo về việc ngừng cung cấp chức năng Visual Basic Script (VBScript), một ngôn ngữ thường bị lợi dụng để phát tán mã độc. Trong các phiên bản sau này của Windows, VBScript sẽ không còn mặc định nữa nhưng người dùng có thể cài đặt thêm.

Nguồn: https://thehackernews.com/2023/10/microsoft-releases-october-2023-patches.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 **711** lỗ hổng, trong đó có 310 lỗ hổng mức Cao, 153 lỗ hổng mức Trung bình, 01 lỗ hổng mức Thấp và 247 lỗ hổng chưa đánh giá. Trong đó có ít nhất 161 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 07 lỗ hổng trong Linux, Nhóm 104 lỗ hổng trong Microsoft, Nhóm 58 lỗ hổng trong Google, Nhóm 89 lỗ hổng trong Wordpress, Nhóm 12 lỗ hổng trong Adobe, Nhóm 08 lỗ hổng trong Oracle, Nhóm 14 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-2023-39189, CVE-2023-39192,...

- Microsoft: CVE-2023-36561, CVE-2023-36419,...

- Google: CVE-2023-35646, CVE-2023-35647,...

- Wordpress: CVE-2023-25480, CVE-2023-27615,...

- Adobe: CVE-2023-38218, CVE-2023-38219,...

- Oracle: CVE-2023-42663, CVE-2023-42780,...

- IBM: CVE-2023-43058, CVE-2023-33160,...

Thông tin điểm yếu, lỗ hổng

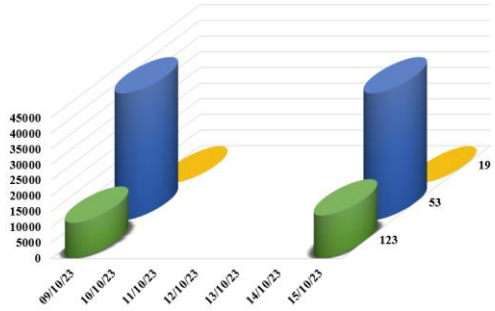
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2023-39189 CVE-2023-39192 CVE-2023-39193 …	Nhóm 07 lỗ hổng trong Linux cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
2	Microsoft	CVE-2023-36561 CVE-2023-36419 CVE-2023-36414 …	Nhóm 104 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực thi mã từ xa, leo thang đặc quyền, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
3	Google	CVE-2023-35646 CVE-2023-35647 CVE-2023-35648 …	Nhóm 58 lỗ hổng trong Google cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-25480 CVE-2023-27615 CVE-2023-45047 …	Nhóm 89 lỗ hổng trong Wordpress cho phép đối tượng tấn công khai thác lỗi CSRF, khai thác lỗi SQL Injection, thực thi mã từ xa.	Chưa có thông tin xác nhận và bản vá
5	Adobe	CVE-2023-38218 CVE-2023-38219 CVE-2023-38220 …	Nhóm 12 lỗ hổng trong Adobe cho phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa, khai thác lỗi XSS.	Chưa có thông tin xác nhận và bản vá
6	Oracle	CVE-2023-42663 CVE-2023-42780 CVE-2023-42792 …	Nhóm 08 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-2023-43058 CVE-2022-33160 CVE-2023-35897 …	Nhóm 14 lỗ hổng trong IBM phép đối tượng tấn công leo thang đặc quyền, thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá

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

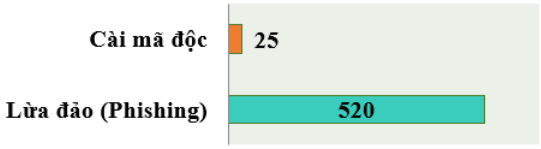
Tấn công DRDoS

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 **54.132**, (tăng so với tuần trước **52.492**) 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

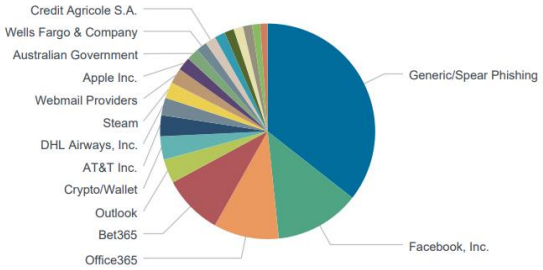


Thống kê tấn công vào trang/cổng thông tin điện tử của Việt Nam



Tấn công Web

Trong tuần, có **520** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 495 trường hợp tấn công lừa đảo (Phishing), 25 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: 17392 IP	hzmksreiuojy.ru: 286 IP
disorderstatus.ru: 6071 IP	xjpakmdcfuqe.biz: 284 IP
atomictrivia.ru: 2839 IP	xjpakmdcfuqe.com: 136 IP
amnsreiuojy.ru: 837 IP	xjpakmdcfuqe.ru: 84 IP
restlesz.su: 346 IP	xjpakmdcfuqe.in: 83 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **302** 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	vietcapital-vn.vip vietcapital-vay.com vietcapital.cyou vietcapital.vip vietcapital-vn.top vietcapitalv.cc vietcapitalc.top	Website giả mạo Ngân hàng TMCP Bản Việt
2	tfi6678.com rwrb55.com sodj88.com	Website giả mạo sàn TMĐT Tiki
3	shoopaem.com shopee.coepes.com sopper68.com kkh818.com	Website giả mạo sàn TMĐT Shopee
4	travelokeaaa.xyz	Website giả mạo Traveloka
5	ebeuboay.cc	Website giả mạo Ebay
6	amazonsg.shop	Website giả mạo sàn TMĐT Amazon

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