NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 45 (04/11/2024 – 10/11/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Chiến dịch "VEILDrive" lợi dụng các dịch vụ của Microsoft để phát tán mã độc và né tránh bị phát hiện.

- **Cảnh báo:** Synology phát hành bản vá cho lỗi RCE nghiêm trọng "không chạm" đe dọa hàng triệu thiết bị NAS.

2. Điểm yếu, lỗ hổng

- TOP **10** lỗ hổng đáng chú ý trong tuần.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Botnet ảnh hưởng tới người dùng Việt Nam**

- **Tấn công lừa đảo người dùng Việt Nam: 5.213** 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://khonggianmang.vn

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Chiến dịch "VEILDrive" lợi dụng các dịch vụ của Microsoft để phát tán mã độc và né tránh bị phát hiện"

Các chuyên gia bảo mật đã phát hiện một chiến dịch tấn công có tên "VEILDrive" lợi dụng các dịch vụ của Microsoft như Teams, SharePoint, Quick Assist, và OneDrive nhằm phát tán mã độc và thực hiện các cuộc tấn công spear-phishing. Việc này giúp nhóm tấn công tránh bị phát hiện bởi các hệ thống giám sát thông thường.

Chiến dịch được ghi nhận lần đầu vào tháng 9/2024 khi các chuyên gia ứng cứu sự cố an toàn thông tin nhằm vào một tổ chức hạ tầng trọng yếu tại Mỹ, được mã hóa danh tính là "Org C." Chiến dịch được cho là bắt đầu từ tháng trước, với mục tiêu chính là phát tán mã độc dựa trên Java và sử dụng OneDrive làm nền tảng C&C.

Nhóm tấn công khởi đầu chiến dịch bằng cách gửi tin nhắn trên Microsoft Teams tới bốn nhân viên của Org C, giả danh nhân viên IT và yêu cầu truy cập từ xa vào thiết bị của họ thông qua công cụ Quick Assist.

Điểm đặc biệt là các tin nhắn này không được gửi từ một tài khoản mới tạo mà từ tài khoản của một tổ chức khác đã bị khai thác trước đó, gọi là Org A.

Sau khi có được sự tin tưởng từ các nhân viên, nhóm tấn công tiếp tục chia sẻ một đường dẫn tải xuống trên SharePoint cho tệp ZIP "Client_v8.16L.zip" được lưu trữ trên hạ tầng của một tổ chức thứ ba, gọi là Org B. Bên trong tệp ZIP này có chứa LiteManager, một công cụ truy cập từ xa, cùng các tệp khác. Sau khi truy cập thành công, kẻ tấn công sử dụng quyền truy cập để thiết lập lịch tác vụ nhằm thực thi LiteManager định kỳ.

Sau đó, đối tượng tấn công gửi cho người dùng một đường dẫn tải xuống trên SharePoint, dẫn tới tệp "Client_v8.16L.zip" được lưu trên hệ thống của một tổ chức khác. Bên trong tệp này chứa nhiều tệp tin, bao gồm LiteManager, một công cụ truy cập từ xa. Sau khi tải xuống, đối tượng tấn công thiết lập lịch trình tự động để LiteManager có thể chạy định kỳ trên hệ thống, đảm bảo duy trì quyền truy cập từ xa mà không cần sự can thiệp thủ công.

Nguồn: https://thehackernews.com/2024/11/veildrive-attack-exploits-microsoft.html

"Chiến dịch tấn công APT: Chiến dịch "VEILDrive" lợi dụng các dịch vụ của Microsoft để phát tán mã độc và né tránh bị phát hiện"

Tiếp đó, một tệp ZIP khác có tên "Cliento.zip" cũng được tải xuống với phương thức tương tự, chứa mã độc dạng Java Archive (.JAR) cùng bộ công cụ Java Development Kit (JDK) để kích hoạt mã độc này. Mã độc sử dụng tài khoản OneDrive do đối tượng kiểm soát, đăng nhập bằng thông tin xác thực Entra ID được mã hóa sẵn, và dùng OneDrive làm C&C để tải và thực thi các lệnh PowerShell trên hệ thống bị nhiễm thông qua Microsoft Graph API. Một phương án dự phòng cũng được tích hợp, với một socket HTTPS kết nối đến máy ảo Azure từ xa để nhận và thực thi lệnh PowerShell.

Được biết, đây không phải là lần đầu Quick Assist bị khai thác cho mục đích tấn công. Trước đó, vào tháng 5/2024, Microsoft đã cảnh báo về nhóm Storm-1811, giả danh nhân viên hỗ trợ kỹ thuật qua Quick Assist để phát tán mã độc tống tiền Black Basta.

Thông tin về chiến dịch VEILDrive được công bố sau khi Windows thông báo phát hiện các cuộc tấn công lợi dụng dịch vụ lưu trữ tệp như SharePoint, OneDrive, và Dropbox làm phương thức né tránh các hệ thống phát hiện thông thường.

Một số IoC được ghi nhận:

SafeShift390[.]onmicrosoft[.]com	GreenGuard036[.]onmicrosoft[.]com
40.90.196[.]221	40.90.196[.]228
38.180.136[.]85	213.87.86[.]192

Nguồn: https://thehackernews.com/2024/11/veildrive-attack-exploits-microsoft.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo Synology phát hành bản vá cho lỗi RCE nghiêm trọng "không chạm" đe dọa hàng triệu thiết bị NAS"

Synology vừa phát hành bản vá cho lỗi nghiêm trọng gây ảnh hưởng tới DiskStation và BeePhotos, lỗ hổng này cho phép đối tượng tấn công khai thác thực thi mã từ xa.

Lỗ hổng này có mã CVE-2024-10443 và có tên RISK:STATION, đã được công khai tại cuộc thi Pwn2Own tại Ireland vào năm 2024. Cụ thể, đây là lỗ hổng "không chạm" và không yêu cầu xác thực, cho phép đối tượng tấn công chiếm quyền root trên thiết bị NAS mà không cần người dùng thực hiện bất kỳ thao tác nào. Điều này có nghĩa là đối tượng tấn công có thể xâm nhập vào hệ thống từ xa và phát tán mã độc mà không cần tương tác từ phía người dùng.

Các phiên bản bị ảnh hưởng bao gồm BeePhotos for BeeStation OS 1.0, BeePhotos for BeeStation OS 1.1, Synology Photos 1.6 cho DSM 7.2 và Synology Photos 1.7 cho DSM 7.2.

Hiện tại, Synology chưa công bố chi tiết kỹ thuật về lỗ hổng này để đảm bảo người dùng có thời gian cập nhật bản vá. Ước tính có khoảng 1-2 triệu thiết bị Synology đang nằm trong diện bị đe dọa trên không gian mạng.

Thông báo của Synology được đưa ra trong bối cảnh QNAP cũng đang xử lý ba lỗ hổng nghiêm trọng ảnh hưởng đến các dịch vụ QuRouter, SMB Service, và HBS 3 Hybrid Backup Sync. Ba lỗ hổng này đã xuất hiện tại cuộc thi Pwn2Own và có mã như sau:

- CVE-2024-50389 – Đã được vá trong QuRouter phiên bản mới hơn 2.4.5.032
- CVE-2024-50387 – Đã được vá trong SMB Service phiên bản 4.15.002 và các phiên bản mới hơn
- CVE-2024-50388 – Đã được vá trong HBS 3 Hybrid Backup Sync phiên bản mới hơn 25.1.1.673

Mặc dù chưa có ghi nhận về việc các lỗ hổng trên bị khai thác trong thực tế, người dùng vẫn nên cập nhật bản vá ngay khi có thể. Trong bối cảnh các cuộc tấn công nhằm vào thiết bị NAS để phát tán mã độc ngày càng gia tăng, đặc biệt là ransomware, việc bảo mật thiết bị trở nên quan trọng hơn bao giờ hết.

Nguồn: https://thehackernews.com/2024/11/synology-urges-patch-for-critical-zero.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 **833** lỗ hổng, trong đó có 292 lỗ hổng mức Cao, 467 lỗ hổng mức Trung bình, 27 lỗ hổng mức Thấp và 47 lỗ hổng chưa đánh giá. Trong đó có ít nhất 120 lỗ hổng cho phép chèn và thực thi mã lệnh.

Ngoài ra, tuần hệ thống kỹ thuật của NCSC cũng đã ghi nhận TOP **10** lỗ hổng đáng chú ý, là những lỗ hổng có mức độ nghiêm trọng cao hoặc đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.

Trong đó, đáng chú ý có **03** lỗ hổng ảnh hưởng các sản phẩm của Microsoft, Fortinet và X.org, cụ thể là như sau:

- **CVE-2024-38094 (Điểm CVSS: 7.2 – Cao):** Lỗ hổng tồn tại trên Microsoft SharePoint cho phép đối tượng tấn công thực thi mã từ xa. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công
- **CVE-2024-47575 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên FortiManager cho phép đối tượng thực thi mã từ xa. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024- 9632 (Điểm CVSS: 7.8 – Cao):** Lỗ hổng tồn tại trên máy chủ X.org cho phép đối tượng tấn công với quyền truy cập nội bộ vào máy chủ có thể khai thác lỗi buffer overflow, qua đó cho phép đối tượng thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-38094	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: Microsoft SharePoint - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-38094
2	CVE-2024-47575	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: FortiManager - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-47575
3	CVE-2024-9632	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Máy chủ X.org - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, leo thang đặc quyền - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-9632
4	CVE-2024-45519	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Zimbra - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-45519
5	CVE-2024-23692	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Rejetto HTTP File Server - Mô tả: Lỗ hổng cho phép đối tượng tấn công - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-23692

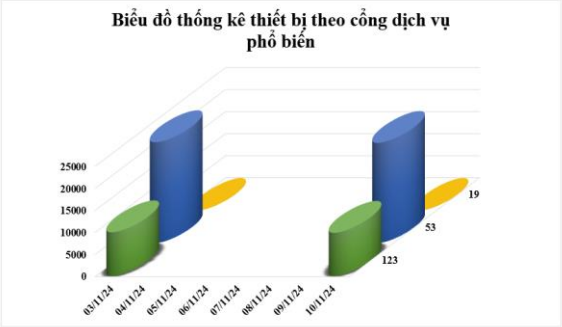
TOP 10 lỗ hổng đáng chú ý trong tuần

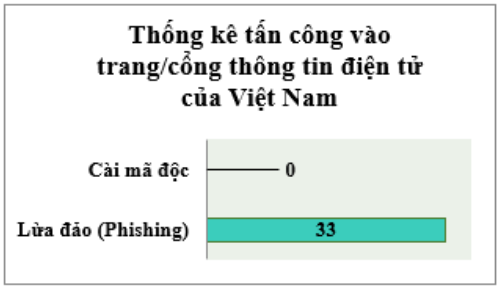
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-43047	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Qualcomm - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-43047
7	CVE-2024-20418	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: Cisco Ultra-Reliable Wireless Backhaul (URWB) Access Points - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-20418
8	CVE-2024-5910	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Palo Alto Networks Expedition - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-5910
9	CVE-2024-49328	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Vivek Tamrakar WP REST API - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-49328
10	CVE-2024-40711	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Veeam - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-40711

Thống 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 **32.599** (giảm so với tuần trước **32.883**) 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.



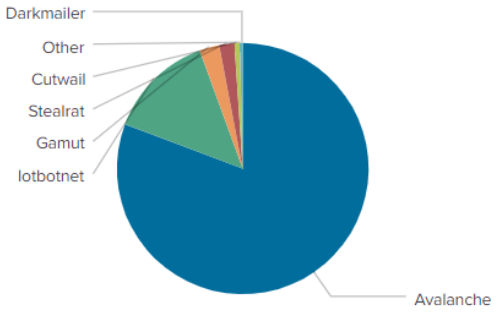


Tấn công Web

Trong tuần, có **33** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 33 trường hợp tấn công lừa đảo (Phishing), 0 trường hợp tấn công cài cắm mã độc.

Botnet

Trên thế giới có nhiều địa chỉ IP/domain độc hại được các nhóm đối tượng tấn công sử dụng làm máy chủ C&C trong botnet. Những địa chỉ này cho phép nhóm đối tượng điều khiển thiết bị thuộc các mạng botnet để thực hiện các hành vi trái phép như triển khai tấn công DDoS, phát tán mã độc, gửi thư rác, truy cập và đánh cắp dữ liệu trên thiết bị. Trong tuần, ghi nhận **20** địa chỉ IP/domain thuộc botnet có ảnh hưởng tới người dùng Việt Nam.



Địa chỉ được sử dụng trong các mạng botnet

disorderstatus.ru	gjogvvpsf.biz
differentia.ru	morphed.ru
atomictrivia.ru	ygiudewsqhct.in
a.asense.in	hzmksreiuojy.ru
sdk.asense.in	xjpakmdcfuqe.biz
statis.multispacesext.net	a.deltaheavy.ru
egksyqv.info	hzmksreiuojy.in
thesecond.in	restlesz.su
amnsreiuojy.ru	trn4x9dc.ru
cp.lg82n82g.ru	yunalwv.biz

Tấn công lừa đảo người dùng Việt Nam

Trong tuần, hệ thống của Cục An toàn thông tin đã ghi nhận **5.213** phản ánh trường hợp lừa đảo trực tuyến do người dùng Internet Việt Nam gửi về. Trong đó:

- **258** trường hợp phản ánh được tiếp nhận thông qua hệ thống Trang cảnh báo an toàn thông tin Việt Nam (canhbao.khonggianmang.vn).
- **4.955** trường hợp phản ánh cuộc gọi, tin nhắn lừa đảo thông qua tổng đài 156/5656

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	https://sellings-global[.]com/shop	Website giả mạo sàn TMĐT Amazon
2	giaohangtietkiem247[.]com[.]vn	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	dkvn[.]zvogo[.]com	Website giả mạo Cục Đăng kiểm Việt Nam
4	vn-chinhphu[.]com	Website giả mạo Dịch vụ công Quốc Gia
5	dichvucong[.]wrgov[.]com	Website giả mạo Dịch vụ công Quốc Gia
6	https://ebayve[.]com	Website giả mạo sàn TMĐT Ebay
7	https://ocbcccreonline[.]com/	Website giả mạo Ngân hàng TMCP Phương Đông
8	https://vimoney[.]credit	Website giả mạo Ngân hàng TMCP Quân đội
9	Ungdung6buoc[.]com	Website giả mạo Ngân hàng TMCP Quân đội
10	khachhangcnvib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	vaythechapvib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
12	https://shinhan[.]hotrokhachhang-uudaithemoi-thang11[.]com[.]vn/	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
13	https://shinhan[.]hotrokhachhang-uudaithemoi-thang11[.]com[.]vn	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
14	www[.]sp7588p[.]com	Website giả mạo sàn TMĐT Shopee
15	https://evnsp[.]com/	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
16	https://www[.]evnsspc[.]com/	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
17	https://www[.]tikifreeship[.]cc	Website giả mạo sàn TMĐT Tiki
18	https://tiktok-svip11[.]com/r?code=YFVEZA	Website giả mạo TikTok
19	Evaluatetravels[.]com	Website giả mạo Traveloka
20	https://evaluatetravels[.]com/login	Website giả mạo Traveloka

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, các đơn vị chủ động cập nhật các thông tin về các rủi ro an toàn thông tin mạng tại địa chỉ https://alert.khonggianmang.vn..

***

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**, Đề nghị các đơn vị, tổ chức, doanh nghiệp cần chủ động rà quét, phát hiện sớm các website lừa đảo giả mạo tổ chức của mình, cảnh báo sớm đến người dùng của nhằm ngăn chặn các hoạt động lừa đảo đến người dùng, đảm bảo an toàn thông tin cho người dùng, bảo vệ chính thương hiệu của tổ chức.

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