NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 16 (15/04/2024 – 21/04/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công FIN7 sử dụng mã độc backdoor Carbanak để tấn công ngành công nghiệp ô tô tại Mỹ.

- **Cảnh báo:** Khai thác lỗ hổng an toàn thông tin nghiêm trọng trên Atlassian để phát tán mã độc Ransomware Cerber.

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: 286** 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: Nhóm tấn công FIN7 sử dụng mã độc backdoor Carbanak để tấn công ngành công nghiệp ô tô tại Mỹ."

Nhóm tấn công FIN7, nổi tiếng với các chiến dịch spear-phishing, đã nhằm vào ngành công nghiệp ô tô ở Mỹ để phát tán mã độc Carbanak (hay Anunak). Để thực hiện điều này, FIN7 xác định tập trung vào các nhân viên trong đơn vị IT có quyền hạn cao rồi sử dụng một công cụ quét IP miễn phí như một chiêu trò để lừa đảo và triển khai mã độc Anunak.Qua đó, FIN7 có thể phát tán mã độc vào các thiết bị sử dụng các tệp thực thi, script và thư viện đã được chuẩn bị trước.

Nhóm FIN7 còn được biết đến với các cái tên như Carbon Spider, Elbrus, Gold Niagara, ITG14, và Sangria Tempest. Từ năm 2012, nhóm này đã liên tục tấn công với động cơ tài chính vào nhiều lĩnh vực và ngành nghề khác nhau, đặc biệt là hệ thống thanh toán PoS để phát tán mã độc và đánh cắp dữ liệu.

Trong những năm gần đây, nhóm đối tượng đã chuyển sang thực hiện các chiến dịch tấn công ransomware để lây nhiễm Black Basta, Cl0p, DarkSide, và REvil. Hai thành viên người Ukraine của nhóm hiện đã bị kết án tại Mỹ.

Một chiến dịch mới đã được phát hiện vào cuối năm 2023, bắt đầu từ một email spear-phishing với đường dẫn độc hại giả mạo trang web của một công cụ quét IP tiên tiến. Đường dẫn này hướng người dùng đến một thư mục Dropbox do nhóm tấn công quản lý, với mục tiêu lừa đảo họ tải xuống một file thực thi độc hại có tên là WsTaskLoad.exe. File này tiếp tục thực hiện một chuỗi các bước để triển khai mã độc Carbanak. Hơn nữa, file cũng được thiết kế để tải về các payload khác như POWERTRASH và thiết lập OpenSSH để duy trì một kết nối từ xa.

Nguồn: https://thehackernews.com/2024/04/fin7-cybercrime-group-targeting-us-auto.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm tấn công FIN7 sử dụng mã độc backdoor Carbanak để tấn công ngành công nghiệp ô tô tại Mỹ."

Hiện vẫn chưa rõ liệu chiến dịch này đã sử dụng mã độc ransomware hay không, do các hệ thống bị tác động đã được phát hiện và loại bỏ kịp thời. Dù chỉ có một số lượng hạn chế trong ngành công nghiệp ô tô ở Mỹ bị ảnh hưởng, các cơ quan bảo mật đã nhận diện một số tên miền độc hại giống với tên miền trong chiến dịch này. Đây là dấu hiệu cho thấy có khả năng nhóm APT FIN7 đang chuẩn bị một chiến dịch quy mô lớn hơn.

Dưới đây là một số IoC được ghi nhận

advanced-ip-sccanner[.]com	myscannappo[.]info
myipscanner[.]com	myscannappo[.]online
theipscanner[.]com	181[.]215.69[.]24
ipscanneronline[.]com	166[.]1.160[.]118
ipscannershop[.]com	185[.]39.204[.]179
myscannappo[.]com	109[.]107.171[.]62
38[.]180.1[.]17	0

Nguồn: https://thehackernews.com/2024/04/fin7-cybercrime-group-targeting-us-auto.html

Tin tức An toàn thông tin

"Cảnh báo: Khai thác lỗ hổng an toàn thông tin nghiêm trọng trên Atlassian để phát tán mã độc Ransomware Cerber."

Các nhóm tấn công đang khai thác máy chủ Atlassian không đủ bảo mật để triển khai biến thể Linux của mã độc Ransomware Cerber (C3RB3R). Việc khai thác lỗ hổng CVE-2023-22518 (điểm CVSS: 9.1) có mức độ ảnh hưởng nghiêm trọng trên "Atlassian Confluence Data Center and Server". Lỗ hổng này cho phép đối tượng tấn công đặt lại cấu hình Confluence và tạo tài khoản quản trị. Kết quả là, đối tượng tấn công chiếm quyền kiểm soát hệ thống bị lây nhiễm, gây ảnh hưởng tới tính bí mật, toàn vẹn và sẵn có của dịch vụ.

Đã có thông tin cho biết rằng các nhóm tấn công có động cơ tài chính đã khai thác lỗ hổng này để cài đặt plugin webshell Effulence. Plugin này cho phép thực thi câu lệnh tùy ý và tải xuống payload Cerber. Do ứng dụng Confluence mặc định thực thi dưới tài khoản "confluence" (có quyền hạn thấp) nên đối tượng chỉ có thể mã hóa các file sở hữu bởi tài khoản này.

Việc khai thác lỗ hổng CVE-2023-22518 để phát tán mã độc Cerber đã được cảnh báo từ tháng 11/2023. Payload chính của mã độc sử dụng ngôn ngữ C++ làm loader cho các mã độc C++ bổ trợ, sau đó tự xóa khỏi thiết bị. Payload cũng bao gồm "agttydck.bat", được thực thi để tải xuống bộ mã hóa cùng tên. Hàm agttydck có chức năng kiểm tra quyền hạn cho mã độc trước khi ghi vào file /tmp/ck.log.

Mã độc này sử dụng payload viết bằng C++ để rà soát thư mục gốc và mã hóa dữ liệu thành định dạng .LOCK3D. Đồng thời, nó tạo một note trên mỗi thư mục bị mã hóa. Điều đặc biệt là trong chiến dịch này, phần lớn mã độc đã chuyển sang sử dụng ngôn ngữ lập trình đa nền tảng như Golang và Rust, nhưng mã độc này vẫn duy trì việc sử dụng C++.

Trong bối cảnh này, các chủng mã độc ransomware như Evil Ant, HelloFire, L00KUPRU, Muliaka, Napoli, Red CryptoApp, Risen, và SEXi đã được phát hiện trên máy chủ Windows và VMware ESXi.

Ngoài ra, các nhóm tấn công Ransomware cũng sử dụng mã nguồn của ransomware LockBit để tạo biến thể như Lambda (hoặc Synapse), Mordor, và Zgut. Phân tích cho thấy, file builder của LockBit 3.0 bị lộ lọt, tiết lộ đặc điểm "đơn giản tới mức báo động", cho phép tạo biến thể mới và bổ sung chức năng phức tạp cho mã độc.

Nguồn: https://thehackernews.com/2024/04/critical-atlassian-flaw-exploited-to.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 **1.013** lỗ hổng, trong đó có 220 lỗ hổng mức Cao, 370 lỗ hổng mức Trung bình, 32 lỗ hổng mức Thấp và 391 lỗ hổng chưa đánh giá. Trong đó có ít nhất 165 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 tới các sản phẩm của NorthStar C2, Microsoft, giao thức UDP, cụ thể như sau:

- CVE-2024-28741 (**Điểm CVSS - Chưa xác định**): Là lỗ hổng XSS tồn tại trên EginDemirbilek NorthStar C2 v1 cho phép đối tượng tấn công thực thi câu lệnh tùy ý trên thành phần "login.php" của sản phẩm. Hiện lỗ hổng vẫn đang trong giai đoạn phân tích và có điểm SVRS (SOCRadar Vulnerability Risk Score) là 30, cho thấy nó có mối đe dọa mức độ trung bình. Hiện lỗ hổng đã có mã khai thác và đang được khai thác trong thực tế.
- CVE-2024-21412 (**Điểm CVSS: 8.1 – Cao**): Lỗ hổng tồn tại trên Internet Shortcut Files của Microsoft cho phép đối tượng tấn công vượt qua biện pháp bảo mật, qua đó thực thi mã tùy ý trên thiết bị người dùng. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm APT như Evilnum, TA428, lockbit,...
- CVE-2024-2169 (**Điểm CVSS - Chưa xác định**): Lỗ hổng gây ảnh hưởng tới giao thức UDP trên các dịch vụ tầng ứng dụng, khiến cho sản phẩm bị chịu ảnh hưởng của tấn công Network Loops. Đối tượng tấn công có thể khai thác lỗ hổng để thực hiện tấn công từ chối dịch vụ hoặc gây ảnh hưởng tới tài nguyên máy chủ. Hiện lỗ hổng đã có mã khai thác và đang bị khai tác trong thực tế.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-28741	- Điểm CVSS: Chưa xác định - Ảnh hưởng: EginDemirbilek NorthStar C2 - 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-2024-28741
2	CVE-2024-21412	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2022 - Mô tả: Lỗ hổng cho phép đối tượng vượt qua biện pháp bảo mật - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-21412
3	CVE-2024-2169	- Điểm CVSS: Chưa xác định - Ảnh hưởng: Giao thức UDP - Mô tả: Lỗ hổng cho phép đối tượng thực hiện tấn công từ chối dịch vụ. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-2169
4	CVE-2024-20359	- Điểm CVSS: 6.0 (Trung bình) - Ảnh hưởng: Cisco Adaptive Security Appliance (ASA), Cisco Firepower Threat Defense (FTD) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý trên hệ thống bị ảnh hưởng - Lỗ hổng đã có mã khai thác đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-20359
5	CVE-2024-21111	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Oracle VM VirtualBox - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-21111

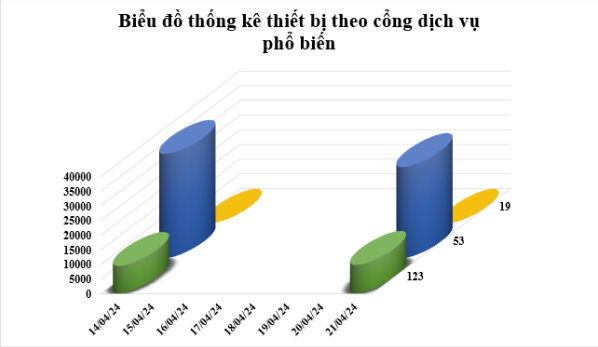
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-3400	- Điểm CVSS: 10 (Nghiêm trọng) - Ảnh hưởng: Palo Alto Networks PAN-OS - Mô tả: Lỗ hổng cho phép đối tượng thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong trong thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3400
7	CVE-2024-4040	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: CrushFTP - 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-2024-4040
8	CVE-2024-21338	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows 10, Windows Server 2022 - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền - 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-2024-21338
9	CVE-2024-3094	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: Tukaani XZ - 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 thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-3094
10	CVE-2024-27198	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: JetBrains TeamCity - Mô tả: Lỗ hổng cho phép đối tượng tấn công bỏ qua xác thực và thực hiện các tác vụ quản trị trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi nhóm tấn công Kimsuky.	https://nvd.nist.gov/vuln/detail/CVE-2024-27198

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 **40.763** (giảm so với tuần trước **44.886**) 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.

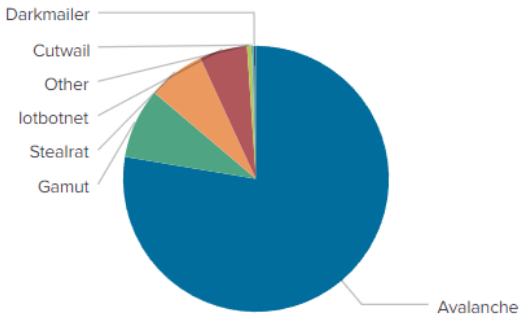


Tấn công Web

Trong tuần, có **83** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 50 trường hợp tấn công lừa đảo (Phishing), 33 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

184.105.192.2	differentia.ru
216.218.185.162	disorderstatus.ru
216.218.135.114	atomictrivia.ru
178.62.201.34	amnsreiuojy.ru
104.131.68.180	restlesz.su
64.71.166.50	hzmksreiuojy.ru
45.77.249.79	xjpakmdcfuqe.biz
184.105.76.250	xjpakmdcfuqe.in
64.71.188.178	xjpakmdcfuqe.ru
restless.su	xjpakmdcfuqe.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **286** 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 các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử,...

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

STT	Website lừa đảo	Ghi chú
1	https://vietgcv[.]cc	Website giả mạo Bộ Thông tin và Truyền thông
2	https://hdtinchap[.]com	Website giả mạo Công ty Tài chính TNHH HD SAISON
3	https://dichvucong[.]dancuso[.]com	Website giả mạo Dịch vụ công Quốc Gia
4	http://dichvucong[.]hhlpa[.]com	Website giả mạo Dịch vụ công Quốc Gia
5	https://lotttemart[.]store	Website giả mạo LOTTE
6	https://clzl[.]pro	Website giả mạo MoMo
7	https://vdbank[.]com[.]vn	Website giả mạo Ngân hàng Phát triển Việt Nam
8	https://sotuyenvcb[.]vietcombanker[.]com	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
9	https://nganhangsaison[.]org/	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
10	https://nang-han-muc-vcs1-khcn-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	http://vipcard-vib[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
12	https://tpbank[.]chamsocthekhachang-truc-tuyen[.]com/	Website giả mạo Ngân hàng TMCP Tiên Phong
13	https://shinhan[.]chamsoccanhankhachhangthe-tructuyen[.]online	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
14	https://canhanshinhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
15	https://www[.]vnambzuon36sc[.]vip/	Website giả mạo sàn TMĐT Amazon
16	http://sp6788[.]com	Website giả mạo sàn TMĐT Shopee
17	https://vn68822s[.]com/	Website giả mạo sàn TMĐT Shopee
18	https://sp77888[.]com/	Website giả mạo sàn TMĐT Shopee
19	https://tdkd07[.]com	Website giả mạo sàn TMĐT Tiki
20	https://vn147258p[.]com	Website giả mạo sàn TMĐTAmazon

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