NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 38 (16/09/2024 – 22/09/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Mã độc botnet "Raptor Train" tấn công hơn 200.000 thiết bị IoT trên toàn cầu.

- **Cảnh báo:** GitLab khắc phục lỗ hổng Nghiêm trọng trong phiên bản CE và EE.

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: 244** 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

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Mã độc botnet "Raptor Train" tấn công hơn 200.000 thiết bị IoT trên toàn cầu"

Gần đây, các chuyên gia bảo mật đã phát hiện một botnet mới chưa từng được ghi nhận trước đây. Botnet này nhắm vào các thiết bị IoT và hệ thống mạng của các doanh nghiệp nhỏ (SOHO), được sử dụng bởi nhóm APT Trung Quốc có tên Flax Typhoon (hay còn gọi là Ethereal Panda hoặc RedJuliett).

Botnet này có tên là Raptor Train, bắt đầu hoạt động từ tháng 05/2020 và đạt đỉnh vào tháng 06/2023 với 60.000 thiết bị bị lây nhiễm. Đến nay, hơn 200.000 thiết bị, bao gồm router SOHO, NVR/DVR, máy chủ NAS và camera IP, đã bị ảnh hưởng bởi mã độc này, khiến Raptor Train thành một trong những botnet IoT lớn nhất của Trung Quốc. Hạ tầng của botnet này được xây dựng theo cấu trúc ba tầng (tier) như sau

- Tier 1: Các thiết bị IoT/SOHO bị ảnh hưởng bởi mã độc
- Tier 2: Các máy chủ khai thác, máy chủ chứa payload và máy chủ C&C.
- Tier 3: Các node quản trị tập trung và một ứng dụng đa nền tảng Electron có tên Sparrow (hay Node Comprehensive Control Tool, gọi tắt NCCT)

Quy trình hoạt động của botnet diễn ra như sau: các tác vụ bot được khởi động từ các node quản trị "Sparrow" ở tier 3, sau đó được điều hướng qua các máy chủ C2 ở tier 2 và cuối cùng gửi đến các bot ở tier 1. Các thiết bị bị tấn công trong mạng botnet này bao gồm camera IP, DVR và máy chủ NAS từ nhiều thương hiệu nổi tiếng như ActionTec, ASUS, DrayTek, Fujitsu, Hikvision, Mikrotik, Mobotix, Panasonic, QNAP, Ruckus Wireless, Shenzhen TVT, Synology, Tenda, TOTOLINK, TP-LINK và Zyxel. Đa số các thiết bị tier 1 của botnet nằm ở Mỹ, Đài Loan, Việt Nam, Brazil, Hồng Kông và Thổ Nhĩ Kỳ. Những thiết bị này có thời gian hoạt động trung bình 17,44 ngày, cho thấy nhóm tấn công có khả năng tái lây nhiễm chúng nhờ khai thác nhiều lỗ hổng bảo mật trên thiết bị SOHO và IoT, mặc dù mã độc không duy trì được sau khi khởi động lại. Điều này cho thấy sự tự tin vào khả năng tái lây nhiễm của nhóm tấn công.

Nguồn: https://thehackernews.com/2024/09/new-raptor-train-iot-botnet-compromises.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Mã độc botnet "Raptor Train" tấn công hơn 200.000 thiết bị IoT trên toàn cầu"

Mã độc lây nhiễm các bot tier 1 được gọi là Nosedive, một biến thể tùy chỉnh của botnet Mirai, phát tán qua máy chủ payload ở tier 2. Mã độc này có khả năng thực thi lệnh, tải lên và tải xuống file, cũng như triển khai tấn công DDoS, cho phép đối tượng tấn công điều khiển thiết bị lây nhiễm mà không bị phát hiện.

Các node tier 2 được thay đổi vị trí khoảng 75 ngày một lần, chủ yếu nằm ở các quốc gia như Mỹ, Singapore, Vương quốc Anh, Nhật Bản và Hàn Quốc. Số lượng node C&C đã tăng khoảng 1-5 kể từ năm 2020 tới 2022 và đạt tối thiểu 60 node trong khoảng thời gian từ giữa tháng 06/2024 đến tháng 08/2024. Ngoài vai trò là máy chủ khai thác, các node tier 2 này còn được sử dụng để phát tán mã độc và hỗ trợ hoạt động do thám các mục tiêu tấn công.

Từ giữa năm 2020 đến nay, đã ghi nhận ít nhất bốn chiến dịch tấn công liên quan đến botnet "Raptor Train", mỗi chiến dịch sử dụng một domain root khác nhau và nhắm tới các thiết bị cụ thể:

- Crossbill (Tháng 05/2020 – Tháng 04/2022): Sử dụng domain C&C k3121.com
- Finch (Tháng 07/2022 – Tháng 06/2023): Sử dụng domain C&C b2047.com
- Canary (Tháng 05/2023 – Tháng 08/2023): Sử dụng domain C&C b2047.com nhưng bổ sung thêm các dropper đa giai đoạn.
- Oriole (Tháng 06/2023 – Tháng 09/2024): Sử dụng domain C&C w8510.com

Chiến dịch tấn công Canary đặc biệt nhằm vào các sản phẩm của Actiontec, Hikivision, Shenzhen TVT và ASUS. Nó sử dụng chuỗi lây nhiễm đa giai đoạn để tải xuống một bash script đầu tiên, kết nối tới máy chủ payload ở tier 2 để lấy mã độc Nosedive và bash script thứ hai. Mỗi 60 phút, script này sẽ tiếp tục tải xuống và thực thi một script thứ ba.

Domain C&C w8510.com trong chiến dịch Oriole nằm trong bảng xếp hạng domain phổ biến của Cisco Umbrella vào ngày 03/06/2024 và lọt vào top 1 triệu domain của Cloudflare Radar vào ngày 07/08/2024. Điều này có thể dẫn đến việc domain được tự động whitelist, cho phép các bot duy trì kết nối mà không bị phát hiện.

Cho đến nay, chưa ghi nhận cuộc tấn công DDoS nào từ botnet "Raptor Train", nhưng có bằng chứng cho thấy botnet này đã tấn công các tổ chức ở Mỹ và Đài Loan trong các lĩnh vực quốc phòng, chính phủ, giáo dục, viễn thông và công nghệ thông tin.

Nguồn: https://thehackernews.com/2024/09/new-raptor-train-iot-botnet-compromises.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Mã độc botnet "Raptor Train" tấn công hơn 200.000 thiết bị IoT trên toàn cầu"

Ngoài ra, có khả năng các bot của "Raptor Train" đã khai thác lỗ hổng trên máy chủ Atlassian Confluence và sản phẩm Ivanti Connect Secure (ICS) trong cùng hệ thống mạng để mở rộng tấn công.

Các chuyên gia bảo mật cho rằng botnet Raptor Train có liên quan đến nhóm APT Flax Typhoon vì chúng cùng nhắm tới các tổ chức ở Đài Loan, Đông Nam Á, Bắc Mỹ và Châu Phi. Sự tương đồng này thể hiện qua việc sử dụng ngôn ngữ Trung Quốc và các kỹ thuật tấn công tương tự.

Một số IoC được ghi nhận:

114[.]255[.]70[.]20	45[.]13[.]199[.]84	92[.]38[.]185[.]44	45[.]80[.]215[.]155	ecvkiehs[.]com
5[.]188[.]33[.]135	45[.]13[.]199[.]96	45[.]135[.]117[.]131	89[.]44[.]198[.]195	hfsdln[.]com
202[.]182[.]109[.]151	45[.]13[.]199[.]104	85[.]90[.]216[.]110	45[.]80[.]215[.]152	osiso[.]com
5[.]188[.]33[.]135	45[.]13[.]199[.]45	37[.]61[.]229[.]17	202[.]182[.]109[.]151	bcdkwwuah[.]com
5[.]188[.]33[.]228	45[.]135[.]117[.]136	37[.]9[.]35[.]89	89[.]44[.]198[.]254	cvmnomvxm[.]com
185[.]14[.]45[.]160	45[.]10[.]58[.]133	85[.]90[.]216[.]116	91[.]216[.]190[.]2	cvgeuwo[.]com
185[.]207[.]154[.]253	45[.]10[.]58[.]130	37[.]61[.]229[.]15	91[.]216[.]190[.]80	lofeuq[.]com
14[.]1[.]98[.]223	85[.]90[.]216[.]111	92[.]38[.]185[.]46	23[.]236[.]68[.]213	lznmihdej[.]com
223[.]98[.]159[.]112	5[.]8[.]33[.]26	45[.]80[.]215[.]186	23[.]236[.]69[.]82	fajxtg[.]com
210[.]61[.]186[.]117	45[.]10[.]58[.]128	85[.]90[.]216[.]115	23[.]236[.]68[.]161	grntjr[.]com
104[.]244[.]89[.]157	195[.]234[.]62[.]197	45[.]10[.]58[.]132	23[.]236[.]69[.]110	oploz[.]com
114[.]255[.]70[.]30	45[.]92[.]70[.]68	92[.]38[.]185[.]45	23[.]236[.]68[.]229	mudvw[.]com
195[.]234[.]62[.]188	5[.]45[.]184[.]68	45[.]92[.]70[.]71	hy92[.]com	amdord[.]com
195[.]234[.]62[.]192	195[.]234[.]62[.]198	207[.]148[.]122[.]69	hy830[.]com	mvxnspcqr[.]com
85[.]90[.]216[.]69	92[.]38[.]185[.]47	91[.]216[.]190[.]154	hy529[.]com	adjsn[.]com
195[.]234[.]62[.]184	92[.]38[.]185[.]43	23[.]236[.]68[.]193	hy229[.]com	ttcyci[.]com
89[.]44[.]198[.]200	85[.]90[.]216[.]112	91[.]216[.]190[.]247	hy324[.]com	glxxet[.]com
207[.]148[.]68[.]131	45[.]10[.]58[.]129	91[.]216[.]190[.]74	hy1025[.]com	nmfagp[.]com
108[.]61[.]177[.]81	5[.]181[.]27[.]219	45[.]80[.]215[.]47	hy42[.]com	rnjca[.]com
45[.]80[.]215[.]149	139[.]180[.]137[.]219	92[.]223[.]30[.]232	hy619[.]com	woaba[.]com
45[.]92[.]70[.]111	149[.]248[.]51[.]22	92[.]223[.]30[.]241	hy424[.]com	bxgtbv[.]com
45[.]13[.]199[.]140	65[.]20[.]97[.]251	202[.]182[.]109[.]151	hy811[.]com	ykcmewapc[.]com
abpi[.]b2047[.]com	iycwqot[.]com	mail[.]k3121[.]com	wmllxwkg[.]w8510[.]com	obqlibg[.]com

Nguồn: https://thehackernews.com/2024/09/new-raptor-train-iot-botnet-compromises.html

Tin tức An toàn thông tin

"Cảnh báo: GitLab khắc phục lỗ hổng Nghiêm trọng trong phiên bản CE và EE"

Gần đây, GitLab đã phát hành bản vá cho lỗ hổng nghiêm trọng cho phép đối tượng tấn công vượt qua xác thực SAML, ảnh hưởng đến phiên bản Community Edition (CE) và Enterprise Edition (EE) của sản phẩm.

Lỗ hổng này, mã CVE-2024-45409 (Điểm CVSS: 10.0), nằm trong thư viện ruby-saml, cho phép đối tượng tấn công đăng nhập bằng tài khoản người dùng bất kỳ trong hệ thống bị ảnh hưởng. Nguyên nhân là do thư viện không thực hiện kiểm tra chữ ký của SAML Response một cách chính xác. SAML (Security Assertion Markup Language) là giao thức cho phép đăng nhập một lần (SSO) và trao đổi dữ liệu xác thực, ủy quyền giữa nhiều ứng dụng và trang web. Đối tượng tấn công có thể lợi dụng một tài liệu SAML đã được ký từ trước để giả mạo SAML Response/Assertion với nội dung tùy chỉnh, từ đó đăng nhập trái phép vào hệ thống.

Ngoài ra, lỗ hổng này cũng ảnh hưởng đến thư viện omniauth-saml nhưng đã được khắc phục trong bản cập nhật 2.2.1 bằng cách nâng cấp thư viện ruby-saml lên phiên bản 1.17. Bản vá này đã được tích hợp vào các phiên bản GitLab như 17.3.3, 17.2.7, 17.1.8, 17.0.8 và 16.11.10.

Trong trường hợp chưa thể cập nhật ngay, GitLab khuyến nghị người dùng tắt tùy chọn bỏ qua xác thực hai yếu tố khi sử dụng SAML và bật tính năng xác thực hai yếu tố (2FA) cho tất cả tài khoản.

Mặc dù GitLab chưa phát hiện trường hợp nào lỗ hổng bị khai thác thực tế, các chuyên gia bảo mật đã chỉ ra một số dấu hiệu cho thấy đang có đối tượng nỗ lực khai thác lỗ hổng này. Nếu khai thác thành công, hệ thống sẽ ghi lại các sự kiện liên quan đến SAML trong log, bao gồm cả giá trị extern_id mà đối tượng tấn công sử dụng.

Trong bối cảnh này, Cơ quan An ninh mạng và Cơ sở hạ tầng Hoa Kỳ (CISA) đã thêm 5 lỗ hổng bảo mật mới vào danh sách Known Exploited Vulnerabilities (KEV), trong đó có lỗ hổng nghiêm trọng CVE-2024-27348 (Điểm CVSS: 9.8) trên Apache HugeGraph-Server. Các cơ quan thuộc Nhánh Hành chính Liên bang (FCEB) được khuyến nghị khắc phục các lỗ hổng này trước ngày 9 tháng 10 năm 2024 để bảo vệ mạng lưới khỏi các mối đe dọa.

Nguồn: https://thehackernews.com/2024/09/gitlab-patches-critical-saml.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 **706** lỗ hổng, trong đó có 304 lỗ hổng mức Cao, 304 lỗ hổng mức Trung bình, 10 lỗ hổng mức Thấp và 88 lỗ hổng chưa đánh giá. Trong đó có ít nhất 85 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

Trong đó, đáng chú ý có **03** lỗ hổng ảnh hưởng các sản phẩm của VMware, Windows và WhatsUp, cụ thể là như sau:

- **CVE-2024-38812 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên VMware vCenter Server tại giao thức DCERPC, đối tượng tấn công có thể khai thác lỗ hổng sử dụng các gói tin độc hại, qua đó dẫn tới tấn công thực thi mã từ xa. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024-43461 (Điểm CVSS: 8.8 – Cao):** Lỗ hổng tồn tại trên Windows MSHTML Platform của Windows 10, Windows 11 cho phép đối tượng tấn công giả mạo website để đánh lừa người dùng cung cấp thông tin quan trọng. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- **CVE-2024-6670 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên WhatsUp Gold là lỗi SQL Injection cho phép đối tượng tấn công truy cập và đọc được mật khẩu mã hóa của người dùng. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-38812	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: VMware vCenter Server - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - 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-2024-38812
2	CVE-2024-43461	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - Mô tả: Lỗ hổng cho phép đối tượng tấn công giả mạo website, đánh lừa người dùng cung cấp thông tin quan trọng. - 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-2024-43461
3	CVE-2024-6670	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: WhatsUp Gold. - 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-2024-6670
4	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 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-2024-23692
5	CVE-2024-2188	- Điểm CVSS: 6.1 (Trung bình) - Ảnh hưởng: TP-Link Archer AX50 firmware - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi XSS. - 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-2024-2188

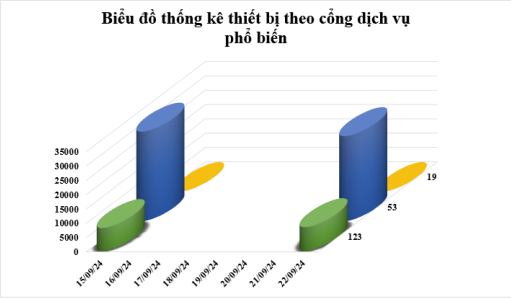
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-7965	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - 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-2024-7965
7	CVE-2024-8190	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: Ivanti Cloud Services - 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-2024-8190
8	CVE-2024-24919	- Điểm CVSS: 8.6 (Cao) - Ảnh hưởng: Check Point Security Gateways - 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-2024-24919
9	CVE-2024-38112	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Microsoft Windows 10, Windows 11 - Mô tả: lỗ hổng cho phép đối tượng tấn công thực hiện tấn công Spoofing. - 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-2024-38112
10	CVE-2024-45414	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Router hãng ZTE. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong môi trường thực tế bởi các nhóm tấn công	https://nvd.nist.gov/vuln/detail/CVE-2024-45414

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 **38.187** (giảm so với tuần trước **39.438**) 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.

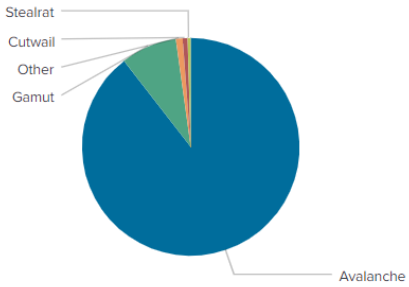


Tấn công Web

Trong tuần, có **75** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 64 trường hợp tấn công lừa đảo (Phishing), 11 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

hzmksreiuojy.ru	butterflyjobs.com
xjpakmdcfuqe.biz	db2017417b23.zapto.org
restlesz.su	rbdwa.com
xjpakmdcfuqe.com	kxtmstjs.org
xjpakmdcfuqe.ru	keeklagqpvg.com
xjpakmdcfuqe.in	kbvnpjijrahsgchor.org
restless.su	jtqqzvqrd.net
andall.servicesql.info	healthnasdaqfeature.com
spaines.pw	gfkpbebwqwhlginna.org
hzmksreiuojy.ru	elitiorecfreetoo.cc

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **244** 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	vssid[.]svgov[.]cc	Website giả mạo Bảo hiểm Xã hội Việt Nam
2	https://giaohangtietkiem247[.]top	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	https://vngiao[.]hangtietkiem[.]online	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://giaohangtietkiemvietnam[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	https://org[.]govqp[.]com	Website giả mạo Cục Đăng kiểm Việt Nam
6	dichvucong[.]bcavnvnvngov[.]com	Website giả mạo Dịch vụ công Quốc Gia
7	https://www[.]ebayu[.]top	Website giả mạo sàn TMĐT Ebay
8	https://github-scanner[.]com	Website giả mạo Github
9	https://play[.]appgoogle[.]cc	Website giả mạo Google
10	https://hethongnoibo[.]bio[.]link	Website giả mạo sàn TMĐT Lazada
11	https://baovietcv[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
12	https://www[.]baovietvc[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
13	ocb[.]chamsocthekhachhang-uudai-tructuyen-thang9[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phương Đông
14	https://tienichshiinhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
15	https://sendovn[.]shop	Website giả mạo sàn TMĐT Sendo
16	www[.]shopeeace[.]com	Website giả mạo sàn TMĐT Shopee
17	nzu66938s[.]com	Website giả mạo sàn TMĐT Shopee
18	https://kpd63519s[.]com	Website giả mạo sàn TMĐT Shopee
19	https://muasamtiki24h[.]com	Website giả mạo sàn TMĐT Tiki
20	https://vnpttechnology[.]weebly[.]com	Website giả mạo VNPT- Tập đoàn Bưu chính Viễn thông Việt Nam

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