NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 34 (19/08/2024 – 25/08/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công Triều Tiên triển khai trojan MoonPeak trong chiến dịch tấn công mạng mới nhất.

- **Cảnh báo:** Google đã phát hành bản vá khẩn cấp cho Chrome nhằm sửa lỗ hổng zero-day thứ 9 bị khai thác trong năm 2024.

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: 537** trường hợp lừa đảo do người dùng Internet Việt Nam thông báo.

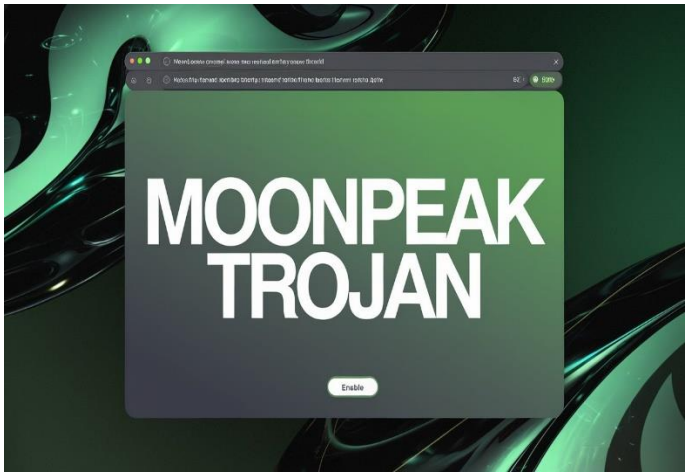
4. Tài liệu lưu trữ

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 Triều Tiên triển khai trojan MoonPeak trong chiến dịch tấn công mới"



Một loại trojan truy cập từ xa (RAT) mới có tên MoonPeak đã được phát hiện, do một nhóm đối tượng tấn công hậu thuẫn bởi Triều Tiên triển khai trong chiến dịch tấn công mạng mới nhất. Theo ghi nhận từ Cisco Talos, chiến dịch này được gán mã UAT-5394 và có những điểm tương đồng về mặt chiến thuật với nhóm APT Kimsuky, một nhóm đối tượng tấn công quốc gia đã được biết đến trước đó.

Mã độc MoonPeak vẫn đang trong quá trình phát triển, đây là một biến thể của mã độc Xeno RAT mã nguồn mở. Trước đây, Xeno RAT đã được sử dụng trong các chiến dịch lừa đảo, với mục tiêu tải xuống các payload từ các dịch vụ đám mây do đối tượng tấn công kiểm soát như Dropbox, Google Drive, và Microsoft OneDrive.

Một số tính năng chính của Xeno RAT bao gồm khả năng cài đặt các plugin bổ sung, thực thi và ngắt các tiến trình, cũng như kết nối tới máy chủ điều khiển C&C. Phân tích sự tương đồng giữa hai nhóm tấn công cho thấy UAT-5394 có thể chính là nhóm Kimsuky (hoặc một phân nhóm của nó) hoặc là một nhóm đối tượng tấn công khác tại Triều Tiên, đang sử dụng các công cụ từ Kimsuky trong chiến dịch của mình.

Trong chiến dịch này, nhóm đối tượng tấn công đã triển khai hạ tầng mới, bao gồm các máy chủ C&C, các trang lưu trữ payload, và các máy ảo thử nghiệm. Máy chủ C&C lưu trữ các mã độc để tải xuống, sau đó được sử dụng để truy cập và thiết lập cơ sở hạ tầng mới, hỗ trợ cho sự phát tán của MoonPeak. Trong một số trường hợp, nhóm đối tượng tấn công này còn truy cập vào các máy chủ đã có từ trước để cập nhật payload và thu thập thông tin từ các hệ thống bị nhiễm MoonPeak.

Sự thay đổi này đánh dấu bước chuyển hướng của nhóm đối tượng tấn công từ việc sử dụng các nhà cung cấp dịch vụ lưu trữ đám mây hợp pháp sang thiết lập và kiểm soát máy chủ riêng. Tuy nhiên, hiện tại vẫn chưa rõ mục tiêu cụ thể của chiến dịch này.

Nguồn: https://thehackernews.com/2024/08/north-korean-hackers-deploy-new.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm tấn công Triều Tiên triển khai trojan MoonPeak trong chiến dịch tấn công mạng mới"

Đáng chú ý, sự phát triển liên tục của MoonPeak đi đôi với việc triển khai cơ sở hạ tầng mới bởi nhóm đối tượng tấn công và mỗi phiên bản của mã độc đều được trang bị các kỹ thuật ẩn mình nhằm làm khó khăn quá trình phân tích, cùng với việc thay đổi giao thức liên lạc để ngăn chặn truy cập trái phép. Nói cách khác, nhóm đối tượng tấn công đã thiết kế MoonPeak sao cho mỗi biến thể của mã độc chỉ hoạt động với phiên bản máy chủ C&C tương ứng.

Các chuyên gia bảo mật nhận định rằng, việc nhóm UAT-5394 liên tục triển khai và nâng cấp mã độc như trường hợp của MoonPeak cho thấy nhóm này đang tiếp tục bổ sung và cải thiện các công cụ tấn công trong hệ thống của mình. Tốc độ triển khai cơ sở hạ tầng mới nhanh chóng cũng là dấu hiệu cho thấy UAT-5394 đang nỗ lực mở rộng phạm vi chiến dịch tấn công, bổ sung thêm các điểm lây nhiễm và máy chủ C&C mới.

Một số IoC được ghi nhận:

167[.]88[.]173[.]173	95[.]164[.]86[.]148
80[.]71[.]157[.]55	84[.]247[.]179[.]77
45[.]87[.]153[.]79	45[.]95[.]11[.]52
104[.]194[.]152[.]251	yoiroyse[.]store
pumaria[.]store	27[.]255[.]81[.]118
212[.]224[.]107[.]244	27[.]255[.]80[.]162
nmailhostserver[.]store	210[.]92[.]18[.]169
91[.]194[.]161[.]109	nsonlines[.]store

Nguồn: https://thehackernews.com/2024/08/north-korean-hackers-deploy-new.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Google đã phát hành bản vá khẩn cấp cho Chrome nhằm sửa lỗ hổng Zero-day thứ 9 bị khai thác trong năm 2024"

Gần đây, Google đã phát hành bản cập nhật bảo mật khẩn cấp để vá lỗ hổng Zero-day CVE-2024-7971, được phát hiện là đã bị khai thác trong các cuộc tấn công thực tế. Lỗ hổng này là một lỗi "type confusion" trong engine V8 JavaScript của Chrome cho phép đối tượng tấn công gây ra sự cố trình duyệt sau khi dữ liệu được đưa vào bộ nhớ bị hiểu sai và có thể thực thi mã tùy ý trên thiết bị chưa được vá.

Hiện nay, lỗ hổng này đã được khắc phục trong phiên bản 128.0.6613.84/.85 cho Windows/macOS và 128.0.6613.84 cho Linux. Các bản cập nhật sẽ được phát hành tự động cho người dùng trong vài tuần tới. Để đẩy nhanh quá trình cập nhật, người dùng có thể vào menu của Chrome, chọn "Trợ giúp" sau đó chọn "Giới thiệu về Google Chrome" để cập nhật và chọn "Khởi động lại" để cài đặt trình duyệt.

Google đã xác nhận lỗ hổng CVE-2024-7971 đã bị khai thác trong thực tế. Tuy nhiên, để đảm bảo rằng đa số người dùng đã kịp cập nhật bản vá, Google tạm thời chưa tiết lộ thông tin chi tiết

Việc này nhằm ngăn chặn các đối tượng tấn công khác lợi dụng lỗ hổng trước khi mọi người đều được bảo vệ.

CVE-2024-7971 là lỗ hổng zero-day thứ 9 được vá bởi Google trong năm 2024, với danh sách cụ thể như sau:

- **CVE-2024-0519**: Lỗ hổng truy cập bộ nhớ ngoài vùng cho phép trong engine V8 JavaScript, cho phép đối tượng tấn công khai thác heap corruption thông qua trang HTML độc hại, dẫn đến truy cập thông tin trái phép.
- **CVE-2024-2887**: Lỗ hổng type confusion trên tiêu chuẩn WebAssembly, cho phép thực thi mã từ xa qua trang HTML độc hại.
- **CVE-2024-2887**: Lỗ hổng use-after-free trong WebCodecs API, cho phép đối tượng tấn công thực hiện đọc/ghi tùy ý qua trang HTML độc hại, dẫn đến thực thi mã từ xa.
- **CVE-2024-3159**: Lỗ hổng đọc ngoài vùng trong engine V8 JavaScript, dẫn đến khai thác heap corruption và truy cập thông tin trái phép.
- **CVE-2024-4671**: Lỗ hổng Use-after-free tồn tại trên thành phần Visuals có chức năng hiển thị nội dung cho browser.
- **CVE-2024-4761**: Lỗ hổng ghi ngoài vùng cho phép tồn tại trên engine V8 Javascript của Chrome, cho phép đối tượng tấn công thực thi mã Javascript trên ứng dụng.
- **CVE-2024-4947**: Lỗ hổng type confusion trên engine V8 Javascript của Chrome cho phép đối tượng tấn công thực thi mã từ xa.
- **CVE-2024-5274**: Lỗ hổng type confusion trên engine V8 Javascript của Chrome cho phép đối tượng tấn công thực thi mã từ xa, dẫn đến sự cố trình duyệt hoặc hỏng dữ liệu.

Nguồn: https://www.bleepingcomputer.com/news/security/google-fixes-tenth-actively-exploited-chrome-zero-day-in-2024/

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 **993** lỗ hổng, trong đó có 399 lỗ hổng mức Cao, 365 lỗ hổng mức Trung bình, 37 lỗ hổng mức Thấp và 192 lỗ hổng chưa đánh giá. Trong đó có ít nhất 114 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 FreeBSD, Ivanti và Microsoft, cụ thể là như sau:

- **CVE-2024-7589 (Điểm CVSS: 8.1 - Cao):** Lỗ hổng tồn tại trên FreeBSD cho phép đối tượng tấn công thực thi mã từ xa dưới quyền root. Xảy ra do lỗi trên sshd(8) cho phép chương trình gọi lên hàm ghi log không đạt chuẩn async-signal-safe. Hiện lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024-7593 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên Ivanti Virtual Traffic Manager (vTM) cho phép đối tượng tấn công không được xác thực có thể bỏ qua bước xác thực tại admin panel do sai sót trong khâu triển khai thuật toán xác thực. Qua đó, cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. Hiện lỗ hổng chưa có mã khai thác và chưa có ghi nhận bị khai thác trong thực tế bởi các nhóm tấn công.
- **CVE-2024-38063 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên Windows TCP/IP 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.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-7589	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: FreeBSD - 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-2024-7589
2	CVE-2024-7593	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Ivanti Virtual Traffic Manager (vTM). - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - 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-2024-7593
3	CVE-2024-38063	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Microsoft Windows 10, Windows 11. - 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-2024-38063
4	CVE-2024-7971	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Google Chrome - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - 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-2024-7971
5	CVE-2024-38856	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Apache OFBiz. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, 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-2024-38856

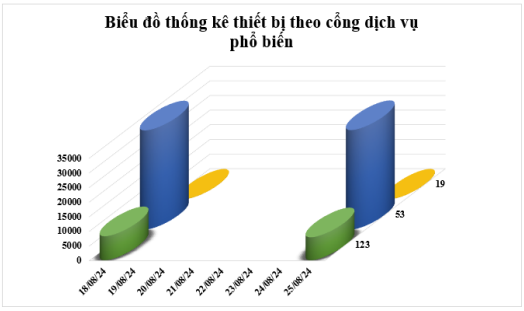
TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-23897	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Jenkins - Mô tả: Lỗ hổng cho phép đối tương 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-2024-23897
7	CVE-2024-6387	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: OpenSSH - 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-2024-6387
8	CVE-2024-28000	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: LiteSpeed Technologies LiteSpeed Cache - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền trên hệ thống. - 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-2024-28000
9	CVE-2024-22263	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Spring Cloud Data Flow - Mô tả: Lỗ hổng cho phép đối tương tấn công truy cập và thực thi 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-2024-22263
10	CVE-2024-3183	- Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: FreeIPA - Mô tả: Lỗ hổng cho phép đối tương 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-2024-3183

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 **41.844** (giảm so với tuần trước **42.096**) 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.

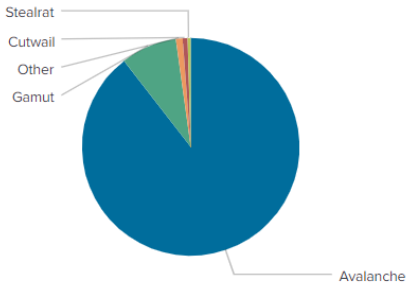


Tấn công Web

Trong tuần, có **85** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 74 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

differentia.ru	restless.su
disorderstatus.ru	andall.servicesql.info
atomictrivia.ru	elitiorecfreetoo.cc
amnsreiuojy.ru	griefcube.cc
hzmksreiuojy.ru	focusdate.com
xjpakmdcfuqe.biz	wrapn.net
restlesz.su	wildrive.com
xjpakmdcfuqe.com	upushjxglaroiqnii.org
xjpakmdcfuqe.ru	hpowixs.info
xjpakmdcfuqe.in	facialwaxmaxfaxlax3.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **537** 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://dichvu[.]congtygiaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
2	https://giaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	https://lazada68[.]com	Website giả mạo sàn TMĐT Lazada
4	https://acb[.]chamsocthekhachhang-tructuyen-thang8[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
5	https://acb[.]chamsockhachhang-uudaithetructuyen-thang8[.]online	Website giả mạo Ngân hàng TMCP Á Châu
6	https://www[.]baovietin[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
7	https://sendotv[.]shop	Website giả mạo sàn TMĐT Sendo
8	https://www[.]vnsendotv[.]vip	Website giả mạo sàn TMĐT Sendo
9	https://558-558-559[.]com	Website giả mạo sàn TMĐT Shopee
10	nzx65821s[.]com	Website giả mạo sàn TMĐT Shopee
11	https://nuk36952s[.]com	Website giả mạo sàn TMĐT Shopee
12	https://sp61889p[.]com	Website giả mạo sàn TMĐT Shopee
13	https://sjfku11[.]com	Website giả mạo sàn TMĐT Tiki
14	https://hethongtikicareers24h[.]com	Website giả mạo sàn TMĐT Tiki
15	https://hethongtikicareers24[.]com	Website giả mạo sàn TMĐT Tiki
16	https://sjfku88[.]com	Website giả mạo sàn TMĐT Tiki
17	https://sdfsshop1[.]com	Website giả mạo sàn TMĐT Tiki
18	https://www[.]tikivn84[.]com	Website giả mạo sàn TMĐT Tiki
19	https://tikimuasam24h[.]com	Website giả mạo sàn TMĐT Tiki
20	https://chinhphu[.]dulieucutru[.]org	Website giả mạo Văn phòng Chính phủ

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