NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 31 (29/07/2024 – 04/08/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT XDSpy tấn công các cơ quan tại Nga và Moldova bằng chiến dịch tấn công lừa đảo.

- **Cảnh báo:** Nguy cơ đe dọa Linux Kernel bằng hình thức tấn công cross-cache SLUBStick.

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: 1.073** 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 APT XDSpy tấn công các cơ quan tại Nga và Moldova bằng chiến dịch tấn công lừa đảo"

Các cơ quan tại Nga và Moldova gần đây đã trở thành mục tiêu của một chiến dịch tấn công lừa đảo do nhóm XDSpy thực hiện. Thông tin này được một cơ quan bảo mật xác định trong tháng 07/2024 và ghi nhận mục tiêu của chiến dịch là phát tán mã độc DSDownloader.

Nhóm XDSpy là một nhóm tấn công không rõ nguồn gốc lần đầu được ghi nhận vào tháng 02/2020, được cho là có liên quan tới các chiến dịch tấn công nhằm đánh cắp dữ liệu của các tổ chức chính phủ tại Đông Âu và vùng Balkan kể từ năm 2011.

Chuỗi tấn công của nhóm XDSpy sử dụng các email spear-phishing để lây nhiễm hệ thống với mã độc XDDown có nhiệm vụ tải xuống các plugin bổ trợ với chức năng thu thập thông tin hệ thống, liệt kê file trong ổ C, theo dõi các ổ rời, trích xuất file trên hệ thống và thu thập mật khẩu. Trong năm qua, XDSpy đã nhắm vào các tổ chức tại Nga, sử dụng dropper ngôn ngữ C# có tên UTask với nhiệm vụ tải xuống module dưới dạng file thực thi để tiếp tục tải thêm các payload độc hại từ máy chủ C&C.

Trong chiến dịch tấn công lần này, XDSpy sử dụng email lừa đảo với nội dung liên quan tới các thỏa thuận để phát tán file RAR có chứa một file thực thi hợp pháp và một file DLL độc hại. File DLL này được thực thi bằng kỹ thuật DLL side-loading, sử dụng file thực thi đi kèm. Sau khi thực thi, mã độc DSDownloader sẽ được tải xuống và thực thi, qua đó mở ra một file giả mạo có vai trò đánh lạc hướng người dùng trong lúc mã độc tải xuống mã độc bổ trợ từ máy chủ C&C. Ngoài ra, payload này không còn khả dụng để tải xuống vào thời điểm phân tích.

Nguồn: https://thehackernews.com/2024/07/cyber-espionage-group-xdspy-targets.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT XDSpy tấn công các cơ quan tại Nga và Moldova bằng chiến dịch tấn công lừa đảo"

Thông tin về chiến dịch tấn công của XDSpy được công bố trong bối cảnh một cơ quan bảo mật tại Ukraine cảnh báo về sự gia tăng đột biến của các cuộc tấn công lừa đảo do nhóm UAC-0057 (hay còn gọi là GhostWriter, UNC1151) thực hiện. Nhóm này sử dụng mã độc PicassoLoader để cài đặt Cobalt Strike Beacon trên các hệ thống bị tấn công.

Ngoài ra, chiến dịch của XDSpy còn được tiết lộ sau khi phát hiện một chiến dịch mới của nhóm Turla, sử dụng file .LNK độc hại làm backdoor không file để thực thi các script PowerShell từ một máy chủ hợp pháp đã bị xâm nhập, từ đó vô hiệu hóa các tính năng bảo mật của hệ thống bị tấn công.

Một số IoC được ghi nhận:

protej[.] org	nashtab[.] org	obshchiye-resursy[.] com
sbordokumentov[.] com	89.114.69[.] 65	89.114.69[.] 48
82.221.129[.] 24	185.56.136[.] 50	159.100.6[.] 5
hxxps://protej[.] org/zpwidnydav/?e&n=bVq7NwlXhjYOMT	hxxps://protej[.] org/zpwidnydav/?e&n=bVq7NwlXhjYOMT	hxxps://protej[.] org/zpwidnydav/?n=wHFbIDNW9YutX
hxxps://nashtab[.] org/biyasqbuk4/?e&n=GuVZoipdI2UIxk	hxxps://nashtab[.] org/pqwebyug3/?n=PDVXCGFwWnCaNv	hxxps://obshchiye-resursy[.] com/zpwidnydav/?e&n=V1Z82iODc5twdu
hxxps://obshchiye-resursy[.] com/zpwidnydav/?n=Jo9EDoZiYATO77	hxxps://sbordokumentov[.] com/snirboubd/?n=vAR1Xp9BG2nStq	hxxps://sbordokumentov[.] com/snirboubd/?n=ygTQMPQdzlcZ9E

Nguồn: https://thehackernews.com/2024/07/cyber-espionage-group-xdspy-targets.html

Tin tức An toàn thông tin

"Cảnh báo: Nguy cơ đe dọa Linux Kernel bằng hình thức tấn công cross-cache SLUBStick"

Gần đây, các chuyên gia bảo mật đã phát hiện một hình thức tấn công cross-cache mới trên Linux Kernel có tên SLUBStick, với tỷ lệ thành công lên đến 99% trong việc chuyển đổi lỗi heap hạn chế thành khả năng đọc/ghi bộ nhớ tùy ý, từ đó cho phép leo thang đặc quyền hoặc thoát khỏi các môi trường container.

Phát hiện này được thực hiện trên các phiên bản Linux Kernel 5.9 và 6.2, với việc sử dụng 09 lỗ hổng CVE khác nhau trên cả hệ thống 32-bit và 64-bit.

Đặc biệt, hình thức tấn công này vẫn hoạt động hiệu quả ngay cả khi các phương pháp bảo mật hiện đại như Supervisor Mode Execution Prevention (SMEP), Supervisor Mode Access Prevention (SMAP), và Kernel Address Space Layout Randomization (KASLR) đang được kích hoạt.

Chi tiết về SLUBStick sẽ được trình bày trong hội nghị "Usenix Security Symposium" vào tháng 8 năm 2024, nơi các nhà nghiên cứu sẽ minh họa khả năng nâng cao đặc quyền và thoát khỏi môi trường container trên hệ thống Linux với các cơ chế bảo mật tiên tiến.

Chi tiết về SLUBStick

Linux Kernel quản lý bộ nhớ một cách hiệu quả và an toàn bằng cách phân bổ và giải phóng các khối bộ nhớ gọi là "slabs" cho các cấu trúc dữ liệu khác nhau. Tuy nhiên, quá trình quản lý bộ nhớ này có thể tồn tại lỗi, cho phép đối tượng tấn công thao túng cấu trúc dữ liệu, dẫn đến các cuộc tấn công cross-cache. SLUBStick khai thác các lỗ hổng heap như double-free, user-after-free, hoặc ghi ngoài giới hạn để thao túng quá trình cấp phát bộ nhớ. Các lỗ hổng này bao gồm: CVE-2023-21400, CVE-2023-3609, CVE-2022-32250, CVE-2022-29582, CVE-2022-27666, CVE-2022-2588, CVE-2022-0995, CVE-2021-4157, và CVE-2021-3492.

Nguồn: https://www.bleepingcomputer.com/news/security/linux-kernel-impacted-by-new-slubstick-cross-cache-attack/

Tin tức An toàn thông tin

"Cảnh báo: Nguy cơ đe dọa Linux Kernel bằng hình thức tấn công cross-cache SLUBStick"

Tiếp theo, SLUBStick sử dụng một kênh phụ thời gian (timing side channel) để xác định chính xác thời điểm phân bổ bộ nhớ, cho phép đối tượng tấn công dự đoán và kiểm soát việc tái sử dụng bộ nhớ. Quá trình chuyển đổi lỗi heap thành khả năng đọc/ghi bộ nhớ tùy ý được thực hiện qua ba bước:

1. Giải phóng các khối bộ nhớ cụ thể và chờ kernel tái sử dụng chúng.
2. Cấp phát lại các khối này một cách có kiểm soát, đảm bảo chúng được sử dụng cho các cấu trúc dữ liệu quan trọng như bảng trang.
3. Khi các khối bộ nhớ đã được chiếm dụng, đối tượng tấn công ghi đè các mục nhập bảng trang, từ đó có thể đọc và ghi vào bất kỳ vị trí bộ nhớ nào.

Ảnh hưởng thực tiễn

SLUBStick yêu cầu quyền truy cập cục bộ vào máy mục tiêu với khả năng thực thi mã, và cần tồn tại lỗi heap trên Linux kernel để khai thác và đạt được quyền truy cập đọc/ghi bộ nhớ. Mặc dù điều này có thể khiến tấn công có vẻ không thực tế, nhưng nó cung cấp lợi ích đáng kể cho các đối tượng tấn công. SLUBStick không chỉ cho phép leo thang đặc quyền, vượt qua các bảo mật kernel, và thoát khỏi môi trường kiểm thử, mà còn có thể là một phần trong chuỗi tấn công phức tạp.

Nguồn: https://www.bleepingcomputer.com/news/security/linux-kernel-impacted-by-new-slubstick-cross-cache-attack/

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 **404** lỗ hổng, trong đó có 139 lỗ hổng mức Cao, 160 lỗ hổng mức Trung bình, 11 lỗ hổng mức Thấp và 94 lỗ hổng chưa đánh giá. Trong đó có ít nhất 55 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 Acronis, VMware và Microsoft, cụ thể là như sau:

- **CVE-2023-45249 (Điểm CVSS: 9.8 – Nghiêm trọng):** Lỗ hổng tồn tại trên Acronis Cyber Infrastructure do việc sử dụng mật khẩu mặc định cho giải pháp, 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 môi trường thực tế bởi các nhóm tấn công.
- **CVE-2024-37085 (Điểm CVSS: 7.2 – Cao):** Lỗ hổng tồn tại trên VMware ESXi cho phép đối tượng tấn công với quyền Active Directory phù hợp có thể bỏ qua bước xác thực của hệ thống, qua đó truy cập và thực hiện các hành vi trái phép. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế trong các chiến dịch tấn công Ransomware bởi các nhóm tấn công Storm-1567, babuk, LockBit, lockbit.
- **CVE-2024-21338 (Điểm CVSS: 7.8 – Cao)**: Lỗ hổng tồn tại trên Microsoft Windows 11, Windows 10 trên tầng Kernel, cho phép đối tượng tấn công leo thang đặc quyền hệ thống. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường 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-2023-45249	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Acronis Cyber Infrastructure - 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-2023-45249
2	CVE-2024-37085	- Điểm CVSS: 7.2 (Cao) - Ảnh hưởng: VMware ESXi - 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-2024-37085
3	CVE-2024-21338	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft Windows 11, Windows 10 - 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
4	CVE-2024-30088	- Điểm CVSS: 7.0 (Cao) - Ảnh hưởng: Microsoft Windows 10. - 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-2024-30088
5	CVE-2024-21413	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Microsoft Outlook - 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-2024-21413

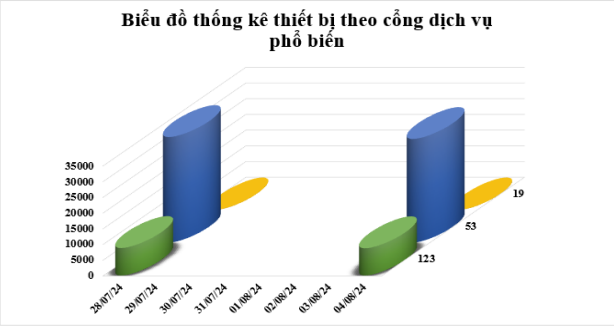
TOP 10 lỗ hổng đáng chú ý trong tuần

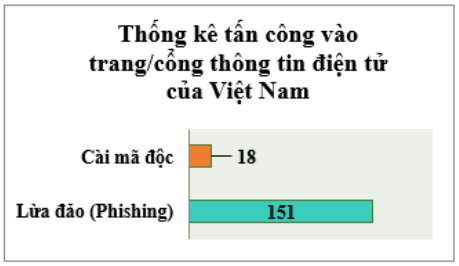
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-36401	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: GeoServer, GeoTools - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-36401
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-2024-4879	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: ServiceNow. - 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-2024-4879
9	CVE-2024-4577	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Ngôn ngữ lập trình PHP. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, 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-2024-4577
10	CVE-2024-41110	- Điểm CVSS: 9.9 (Nghiêm trọng) - Ảnh hưởng: Docker Engine. - 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-2024-41110

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 **41.696** (tăng so với tuần trước **41.090**) 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.



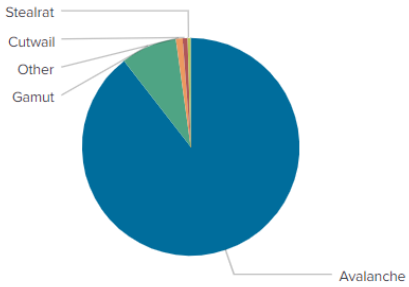


Tấn công Web

Trong tuần, có **169** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 151 trường hợp tấn công lừa đảo (Phishing), 18 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	andall.servicesql.info
disorderstatus.ru	griefcube.cc
atomictrivia.ru	aurasport.net
amnsreiuojy.ru	elitiorecfreetoo.cc
hzmksreiuojy.ru	ufecrlurtnee.space
xjpakmdcfuqe.biz	qiwiy.com
restlesz.su	ljjskttqximu.in
xjpakmdcfuqe.com	ideal-abuse-kind.com
xjpakmdcfuqe.in	htlummla.org
xjpakmdcfuqe.ru	andall.servicesql.info

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **1.073** 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://www[.]govn[.]cc	Website giả mạo Bộ Công An
2	nappthe[.]vn	Website giả mạo Công Ty Cổ Phần Giải Trí Và Thể Thao Điện Tử Việt Nam
3	https://ggiao[.]hangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://giiao[.]hangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	https://vgiao[.]hangtietkiem[.]com/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
6	bachhoaxanhh[.]com	Website giả mạo Công ty cổ phần Thương mại Bách Hóa Xanh
7	https://homecredit[.]hethongvaynhanh247[.]com/	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
8	https://nqsncoau[.]buzz/	Website giả mạo Cty tài chính tnhh ngân hàng việt nam thịnh vượng smbc
9	https://dienmayxanhctv24[.]com	Website giả mạo Điện máy xanh
10	https://thisinhthanhlich2024[.]com	Website giả mạo Facebook
11	https://baovietn[.]vip	Website giả mạo Ngân hàng TMCP Bảo Việt
12	https://vnsehotro[.]com	Website giả mạo Ngân hàng TMCP Quân đội
13	https://mbbkh-canhan[.]com	Website giả mạo Ngân hàng TMCP Quân đội
14	https://mmbonline01[.]com	Website giả mạo Ngân hàng TMCP Quân đội
15	https://vib[.]cham-soc-the-truc-tuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
16	https://www[.]shopeesopp[.]com	Website giả mạo sàn TMĐT Shopee
17	https://tdke03[.]com	Website giả mạo sàn TMĐT Tiki
18	https://kyaj11[.]com	Website giả mạo sàn TMĐT Tiki
19	https://chinhphu[.]thongtincutru[.]org	Website giả mạo Văn phòng Chính phủ
20	https://vnviettel[.]com	Website giả mạo Viettel

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