NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 20 (13/05/2024 – 19/05/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT Turla tấn công Bộ Ngoại giao Châu Âu bằng mã độc backdoor LunarWeb và LunarMail.

- **Cảnh báo:** VMware phát hành bản vá cho các lỗ hổng an toàn thông tin nghiêm trọng trên phần mềm Workstation và Fusion.

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: 271** 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 Turla tấn công Bộ Ngoại giao Châu Âu bằng mã độc backdoor LunarWeb và LunarMail"

Bộ Ngoại giao tại Châu Âu cùng ba cơ quan đại diện của họ tại Trung Đông đã bị tấn công bởi hai mã độc backdoor LunarWeb và LunarMail.

Tổ chức bảo mật ESET đã phát hiện ra chiến dịch này có liên quan đến nhóm APT Turla. Đây là một nhóm tấn công được hậu thuẫn bởi Nga và còn có các tên gọi khác như: Iron Hunter, Pensive Ursa, Secret Blizzard, Snake, Uroburos, và Venomous Bear.

Phân tích cho thấy LunarWeb được triển khai trên máy chủ, sử dụng HTTP/HTTPS làm giao thức liên lạc với máy chủ C&C và giả mạo các gói tin yêu cầu hợp pháp. Trong khi đó, LunarMail được triển khai trên các máy trạm của nhân viên và duy trì kết nối dưới dạng tiện ích mở rộng trên Outlook, sử dụng email làm phương thức liên lạc với máy chủ C&C. Các bằng chứng cũng cho thấy hai mã độc Lunar này đã được sử dụng trong các chiến dịch từ năm 2020, hoặc thậm chí sớm hơn.

Vector xâm nhập Bộ Ngoại giao hiện chưa được xác định nhưng các chuyên gia cho rằng có liên quan đến tấn công spear-phishing và khai thác phần mềm Zabbix cấu hình không bảo mật. Nhóm Turla bắt đầu chuỗi tấn công bằng trang ASP.NET độc hại để giải mã hai khối dữ liệu nhúng, bao gồm trình tải LunarLoader và mã độc backdoor LunarWeb. Khi trang web được yêu cầu, chờ mật khẩu trong cookie SMSKey; sau khi nhập sẽ thu về khóa mã hóa để giải mã payload. Nhóm Turla đã sử dụng thông tin xác thực đánh cắp để di chuyển trong hệ thống.

Nguồn: https://thehackernews.com/2024/05/turla-group-deploys-lunarweb-and.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT Turla tấn công Bộ Ngoại giao Châu Âu bằng mã độc backdoor LunarWeb và LunarMail"

Mã độc LunarMail được phát tán qua file Microsoft Word độc hại gửi qua email spear-phishing, bao gồm cả LunarLoader và mã độc này. Về chức năng, LunarWeb có khả năng thu thập thông tin hệ thống máy chủ và duyệt câu lệnh ẩn trong các file .JPG, .GIF được gửi từ máy chủ C&C, sau đó trích xuất dữ liệu gửi về cho máy chủ dưới dạng nén và mã hóa. Ngoài ra, mã độc còn giả mạo lưu lượng để tránh phát hiện.

Máy chủ C&C trong chiến dịch chỉ thị mã độc LunarWeb thực thi các lệnh shell và PowerShell, thực hiện mã Lua, đọc/ghi file, và lưu trữ các đường dẫn được chỉ định. Đối với LunarMail, chức năng giữa hai mã độc này tương đồng, nhưng điểm khác biệt lớn nhất là LunarMail tận dụng Outlook và sử dụng email làm phương thức liên lạc tới máy chủ C&C bằng cách tìm kiếm các email nhất định chứa file PNG. Một số câu lệnh chỉ có trên mã độc LunarMail cho phép nó tạo profile Outlook để sử dụng làm C&C, tạo tiến trình ngẫu nhiên và chụp ảnh màn hình. Kết quả của các lệnh được lưu và nhúng vào file .PNG hoặc .PDF, sau đó gửi tới email của nhóm tấn công.

Mã độc LunarMail có một số điểm chung với mã độc LightNeuron, cũng là một backdoor được Turla sử dụng, dùng email làm phương thức kết nối tới máy chủ C&C.

Một số IoC được ghi nhận:

45.33.24[.]145	45.79.93[.]87
65.109.179[.]67	74.50.80[.]35
82.165.158[.]86	82.223.55[.]220
139.162.23[.]113	158.220.102[.]80
161.97.74[.]237	176.57.150[.]252
212.57.35[.]174	212.57.35[.]176

Nguồn: https://thehackernews.com/2024/05/turla-group-deploys-lunarweb-and.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: VMware phát hành bản vá cho các lỗ hổng an toàn thông tin nghiêm trọng trên phần mềm Workstation và Fusion"

Nhiều lỗ hổng an toàn thông tin đã được công bố chi tiết trên Vmware Workstation và Fusion, cho phép đối tượng tấn công khi khai thác thành công có thể truy cập và thực hiện các hành vi trái phép, thực hiện tấn công từ chối dịch vụ và thực thi mã từ xa.

Bốn lỗ hổng an toàn thông tin này gây ảnh hưởng tới Workstation phiên bản 17.x và Fusion phiên bản 13.x sẽ được vá trong phiên bản 17.5.2 và 13.5.2.

Thông tin về bốn lỗ hổng cụ thể là như sau:

- **CVE-2024-22267 (Điểm CVSS: 9.3)** – Là lỗ hổng use-after-free tồn tại trên thiết bị Bluetooth có thể bị khai thác bởi các đối tượng tấn công có quyền truy cập cục bộ trên máy ảo để thực thi mã tùy ý dưới tiến trình VMX của máy ảo.
- **CVE-2024-22268 (Điểm CVSS: 7.1) –** Lỗ hổng tràn bộ đệm Heap tồn tại trên chức năng Shader có thể bị khai thác bởi các đối tượng tấn công có quyền truy cập tới máy ảo với chức năng đồ họa 3D được bật để thực hiện tấn công từ chối dịch vụ.
- **CVE-2024-22269 (Điểm CVSS: 7.1)** – Lỗ hổng gây lộ lọt thông tin trên thiết bị Bluetooth có thể bị khai thác bởi các đối tượng tấn công có quyền truy cập cục bộ trên máy ảo để đọc thông tin lưu trên bộ nhớ hypervisor của máy ảo.
- **CVE-2024-22270 (Điểm CVSS: 7.1)** – Lỗ hổng gây lộ lọt thông tin tồn tại trên chức năng Host Guest File Sharing (HGFS) có thể bị khai thác bởi các đối tượng tấn công có quyền truy cập cục bộ trên máy ảo để đọc thông tin lưu trên bộ nhớ hypervisor của máy ảo.

Nguồn: https://thehackernews.com/2024/05/vmware-patches-severe-security-flaws-in.html

Tin tức An toàn thông tin

"Cảnh báo: VMware phát hành bản vá cho các lỗ hổng an toàn thông tin nghiêm trọng trên phần mềm Workstation và Fusion"

Trong trường hợp không thể cập nhật bản vá, người dùng được khuyến nghị tắt chức năng Bluetooth và 3D acceleration trên máy ảo. Đối với lỗ hổng **CVE-2024-22270**, hiện chưa có biện pháp khắc phục nào khác ngoài việc cập nhật lên phiên bản vá mới nhất. Đáng chú ý, các lỗ hổng CVE-2024-22267, CVE-2024-22269, và CVE-2024-22270 đã được chứng minh bởi hai cơ quan bảo mật STAR Labs SG và Theori trong cuộc thi Pwn2Own diễn ra tại Vancouver vào tháng 03/2024.

Thông tin về bốn lỗ hổng này được công bố trong bối cảnh hai tháng sau khi VMware phát hành bản vá cho bốn lỗ hổng an toàn thông tin khác ảnh hưởng đến ESXi, Workstation, và Fusion. Đặc biệt, **CVE-2024-22252 (Điểm CVSS: 9.3)** và **CVE-2024-22253 (Điểm CVSS: 8.4)** là hai lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa.

Nguồn: https://thehackernews.com/2024/05/vmware-patches-severe-security-flaws-in.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 **446** lỗ hổng, trong đó có 69 lỗ hổng mức Cao, 134 lỗ hổng mức Trung bình, 32 lỗ hổng mức Thấp và 211 lỗ hổng chưa đánh giá. Trong đó có ít nhất 117 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 giao thức DHCP, các sản phẩm của Google, Ivanti, cụ thể là như sau:

- CVE-2024-4761 (**Điểm CVSS: Chưa xác định**): Lỗi ghi ngoài bộ nhớ tồn tại trên Google Chrome các phiên bản cũ hơn 124.0.6367.207. Lỗ hổng cho phép đối tượng tấn công khai thác lỗi này thông qua trang HTML độc hại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.
- CVE-2024-3661 **(Điểm CVSS: 7.6 – Trung bình**): Lỗ hổng tồn tịa trên giao thức DHCP cho phép đối tượng tấn công nằm trong cùng mạng với người dùng có thể đọc, gây gián đoạn, chỉnh sửa lưu lượng mạng mặc cho hệ thống mạng được bảo vệ bởi VPN. Quá trình khai thác diễn ra thành công do DCHP có thể thêm luồng điều hướng (route) vào bảng routing table của client thông qua lựa chọn classless static route (121). Các biện pháp bảo mất VPN dựa vào route để điều hướng lưu lượng mạng sẽ bị lộ lọt dữ liệu thông qua interface vật lý. Hiện lỗ hổng này đang bị khai thác trong thực tế.
- CVE-2023-46805 (**Điểm CVSS: 8.2 - Cao**): Lỗ hổng tồn tại trên Ivanti ICS cho phép đối tượng tấn công truy cập vào tài nguyên hạn chế một cách trái phép bằng cách bỏ qua xác thực kiểm soát. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công UTA0178, cactus, Storm-1567, akira, RAZOR TIGER, SideWinder, và SideCopy.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2024-4761	- Điểm CVSS: Chưa xác định - Ảnh hưởng: Google Chrome - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi ghi ngoài bộ nhớ. - 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-2024-4761
2	CVE-2024-3661	- Điểm CVSS: 7.6 (Cao) - Ảnh hưởng: giao thức DHCP - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép, gây ảnh hưởng tới hệ thống mạng vốn được bảo vệ bởi VPN. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-3661
3	CVE-2023-46805	- Điểm CVSS: 8.2 (Cao) - Ảnh hưởng: Ivanti ICS - 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-2023-46805
4	CVE-2024-4671	- Điểm CVSS: 9.6 (Nghiêm trọng) - Ảnh hưởng: Google Chrome - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép thông qua việc khai thác lỗi use-after-free. - 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-2024-4671
5	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

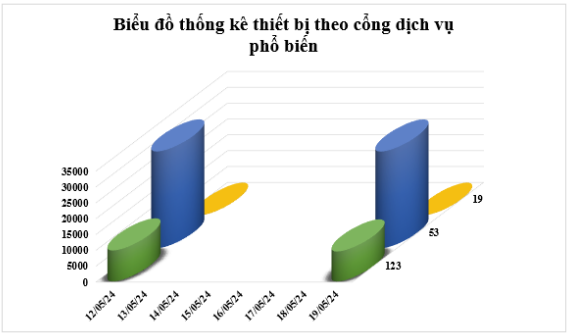
TOP 10 lỗ hổng đáng chú ý trong tuần

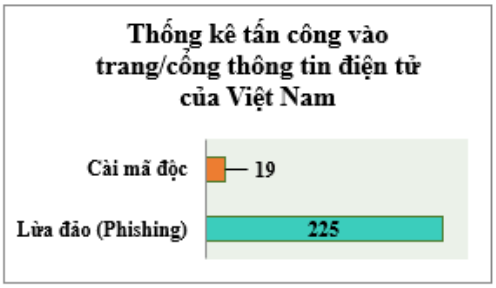
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-30051	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows 10, Windows 11 - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền trên hệ thống. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-30051
7	CVE-2024-21887	- Điểm CVSS: 9.1 (Nghiêm trọng) - Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Lỗ hổng đã có mã khai thác đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công như UTA0178, cactus, Storm-1567 hay akira.	https://nvd.nist.gov/vuln/detail/CVE-2024-21887
8	CVE-2024-26026	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: BIP-IP Next Central Manager API - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện truy vấn SQL trái phép, từ đó truy cập và thực hiện 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-2024-26026
9	CVE-2024-21793	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: BIP-IP Next Central Manager API - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-21793
10	CVE-2024-30040	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows 10 - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý trên hệ thống, vượt qua biện pháp bảo mật. - 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-2024-30040

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 **40.030** (giảm so với tuần trước **40.375**) 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.



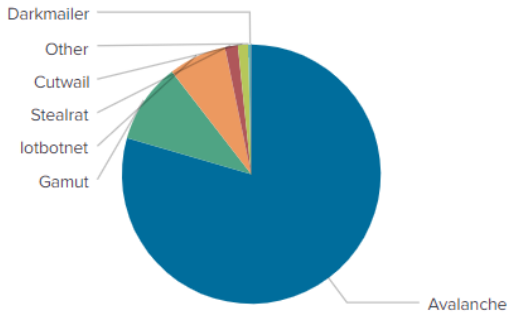


Tấn công Web

Trong tuần, có **244** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 225 trường hợp tấn công lừa đảo (Phishing), 19 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	xjpakmdcfuqe.com
disorderstatus.ru	xjpakmdcfuqe.ru
atomictrivia.ru	andall.servicesql.info
amnsreiuojy.ru	db2017417b23.zapto.org
restlesz.su	restless.su
hzmksreiuojy.ru	wacmovfcbufaweutk.org
xjpakmdcfuqe.biz	mildwave.com
xjpakmdcfuqe.in	jvlohdjcfqjikuhas.com
76236osm1.ru	griefcube.cc
differentia.ru	facialwaxmaxfaxlax3.com

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **271** 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[.]amazonl0[.]com/	Website giả mạo sàn TMĐT Amazon
2	https://bachoaxanhh[.]com	Website giả mạo Công ty cổ phần Thương mại Bách Hóa Xanh
3	https://aeeonmaili[.]shop/	Website giả mạo Công ty TNHH Aeon Việt Nam
4	https://vn-ebay[.]quxlpuj[.]cn/	Website giả mạo sàn TMĐT Ebay
5	https://www[.]hethongdonhang[.]com/	Website giả mạo sàn TMĐT Lazada
6	https://la7890[.]cc/	Website giả mạo sàn TMĐT Lazada
7	https://khoi-khach-hang-ca-nhan-uu-tien-vni[.]com/	Website giả mạo Ngân hàng MBbank
8	https://ocb[.]chamsocthekhachhang-uudai-tructuyen[.]com/	Website giả mạo Ngân hàng TMCP Phương Đông
9	https://mydiamon-han-muc-ca-nhan-vni[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
10	vib[.]chamsocuudaithekhachhang-tructuyen[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	vib[.]chamsockhachhangtheuudai-tructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
12	kh-cn-mrd-f5-tpbank[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
13	https://tpbankvn[.]workplace[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
14	https://miles-card-vpbank[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
15	https://shinhanbank[.]vnfiba[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
16	https://vnsendo[.]net/	Website giả mạo sàn TMĐT Sendo
17	https://www[.]vnsendo[.]net/	Website giả mạo sàn TMĐT Sendo
18	https://sp5188[.]com	Website giả mạo sàn TMĐT Shopee
19	https://sp56788[.]com/	Website giả mạo sàn TMĐT Shopee
20	https://www[.]shopee123[.]vip	Website giả mạo sàn TMĐT Shopee

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