NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 19 (06/05/2024 – 12/05/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT FIN7 sử dụng các quảng cáo độc hại trên Google để phát tán mã độc NetSupport RAT.

- **Cảnh báo:** Google đã vá lỗ hổng an toàn thông tin Zero-Day thứ năm trên Chrome trong năm nay.

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: 259** 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 FIN7 sử dụng các quảng cáo độc hại trên Google để phát tán mã độc NetSupport RAT."

Một nhóm APT có động cơ tài chính, được biết đến với tên gọi FIN7, đã bị phát hiện sử dụng các quảng cáo Google giả mạo các thương hiệu nổi tiếng để phát tán mã độc NetSupport RAT thông qua bộ cài đặt MSIX. Các thương hiệu bị giả mạo bao gồm AnyDesk, WinSCP, BlackRock, Asana, Concur, The Wall Street Journal, Workable, và Google Meet.

Nhóm APT FIN7, còn được biết đến với các tên gọi khác như Carbon Spider và Sangria Tempest, đã bắt đầu hoạt động từ năm 2013. Ban đầu, nhóm này tập trung vào việc tấn công các thiết bị PoS để đánh cắp dữ liệu thanh toán, sau đó mở rộng hoạt động để tấn công các tổ chức lớn hơn thông qua các chiến dịch ransomware.

Trong suốt thời gian hoạt động, FIN7 đã phát triển và củng cố các kỹ thuật tấn công của mình, bao gồm sử dụng các loại mã độc như BIRDWATCH, Carbanak, DICELOADER, POWERPLANT, POWERTRASH, và TERMITE,...

Đáng chú ý, FIN7 thường sử dụng hình thức tấn công spear-phishing để phát tán mã độc đến hệ thống/mạng lưới của nạn nhân. Gần đây, nhóm này đã bắt đầu sử dụng kỹ thuật quảng cáo độc hại (malvertising) làm bước đầu trong chuỗi tấn công.

Vào tháng 12/2023, Microsoft đã ghi nhận việc FIN7 lợi dụng quảng cáo trên Google để lừa người dùng tải xuống gói cài đặt MSIX độc hại, từ đó thực thi mã độc NetSupport RAT và Gracewire.

Microsoft cũng đã phát hiện rằng nhóm FIN7 đã lợi dụng quảng cáo trên Google để đánh lừa người dùng tải xuống gói cài đặt MSIX chứa mã độc. Hành động này dẫn đến việc thực thi POWERTRASH, một dropper PowerShell, nhằm phát tán mã độc NetSupport RAT và Gracewire trên hệ thống của nạn nhân.

Nguồn: https://thehackernews.com/2024/05/fin7-hacker-group-leverages-malicious.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm APT FIN7 sử dụng các quảng cáo độc hại trên Google để phát tán mã độc NetSupport RAT."

Việc sử dụng MSIX làm phương tiện phát tán mã độc đã khiến Microsoft phải vô hiệu hóa giao thức này, do khả năng bỏ qua các cơ chế bảo mật như Microsoft Defender SmartScreen.

Trong chiến dịch vào tháng 04/2024 bởi eSentire, người dùng truy cập vào trang web lừa đảo qua quảng cáo sẽ nhận thấy một thông báo xuất hiện trên màn hình, thúc đẩy họ tải xuống một tiện ích mở rộng trình duyệt giả mạo. Thực chất của tiện ích này là một tập tin MSIX chứa script PowerShell được thiết kế để thu thập thông tin hệ thống và kết nối đến máy chủ từ xa để tải xuống một đoạn mã PowerShell mã hóa khác. Đoạn mã thứ hai này được sử dụng để tải xuống và thực thi mã độc NetSupport RAT. Hơn nữa, mã độc RAT còn được dùng để tải xuống các phần mềm độc hại bổ sung như DICELOADER thông qua script Python.

Chiến dịch tấn công bằng quảng cáo độc hại của FIN7 diễn ra cùng lúc với làn sóng tấn công vào các đối tác doanh nghiệp của nhóm SocGholish. Nhóm SocGholish sử dụng các kỹ thuật tấn công living-off-the-land nhằm thu thập thông tin xác thực và sơ đồ hóa mô hình kết nối nội bộ giữa các doanh nghiệp.

Bên cạnh đó, cũng ghi nhận thông tin nhóm FIN7 có liên quan đến các chiến dịch tấn công vào Windows và Microsoft Office để phát tán mã độc RAT và mã độc đào tiền ảo thông qua các phiên bản tải lậu của phần mềm.

Một số IoC được ghi nhận:

cdn41[.]space	cdn46[.]space
cdn45[.]space	cdn35[.]space
cdn30[.]space	cdn34[.]space
cdn32[.]space	cdn43[.]space
cdn37[.]space	cdn42[.]space
cdn27[.]space	cdn25[.]space
cdn36[.]space	cdn33[.]space
cdn40[.]click	cdn31[.]space
cdn38[.]space	eprst431[.]boo
cdn1124[.]net	cdn1701[.]com
193[.]124[.]24[.]51:443	38[.]135[.]52[.]151:273
5[.]8[.]63[.]140	185[.]174[.]102[.]62
109[.]107[.]170[.]126	193[.]233[.]206[.]23
7-zip[.]cfd	asana[.]wf
advancedipscannerapp[.]com	winscp-install[.]com

Nguồn: https://thehackernews.com/2024/05/fin7-hacker-group-leverages-malicious.html

Tin tức An toàn thông tin

"Cảnh báo: Google đã vá lỗ hổng an toàn thông tin Zero-Day thứ năm trên Chrome trong năm nay."

Google đã phát hành bản vá bảo mật cho trình duyệt Chrome để vá lỗ hổng an toàn thông tin zero-day thứ năm đã bị khai thác trong môi trường thực tế kể từ đầu năm nay. Lỗ hổng này có mã CVE-2024-4671, là một lỗi "Use After Free" (tạm dịch: "Sử dụng sau khi giải phóng bộ nhớ"). Đây là một loại lỗi liên quan đến bộ nhớ, có thể khiến bộ nhớ bị hỏng hoặc cho phép sửa đổi dữ liệu trong bộ nhớ, dẫn đến việc người dùng bị tước bỏ hoàn toàn các đặc quyền trên hệ thống hoặc phần mềm bị ảnh hưởng. Lỗ hổng tồn tại trên thành phần Visuals, chịu trách nhiệm xử lý việc kết xuất và hiển thị nội dung trên trình duyệt.

Lỗ hổng này đã bị khai thác trong môi trường thực tế và hiện đã được khắc phục trong phiên bản 124.0.6367.201/.202 cho Mac/Windows và phiên bản 124.0.6367.201 cho Linux. Đối với người dùng thuộc kênh "Extended Stable", lỗ hổng sẽ được vá trong phiên bản 124.0.6367.201 cho Mac và Windows.

Chrome thường tự động cập nhật khi có bản vá bảo mật mới nhưng người dùng có thể kiểm tra phiên bản mình đang sử dụng bằng cách vào Cài đặt > Giới thiệu về Chrome (Settings > About Chrome).

Đây là lỗ hổng thứ năm được phát hiện trên trình duyệt Google Chrome kể từ đầu năm nay, với các lỗ hổng khác được phát hiện trong cuộc thi Pwn2Own diễn ra vào tháng 3/2024 tại Vancouver.

Nguồn: https://www.bleepingcomputer.com/news/security/google-fixes-fifth-chrome-zero-day-vulnerability-exploited-in-attacks-in-2024/?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Google đã vá lỗ hổng an toàn thông tin Zero-Day thứ năm trên Chrome trong năm nay."

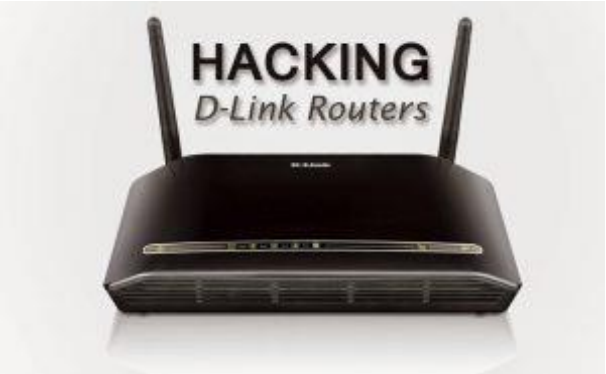
Danh sách các lỗ hổng zero-day đã được phát hiện cụ thể là như sau:

- **CVE-2024-0519:** Lỗ hổng truy cập bộ nhớ ngoài giới hạn trong engine V8 JavaScript của Chrome, cho phép đối tượng tấn công từ xa khai thác lỗi heap thông qua trang HTML độc hại, dẫn đến việc truy cập trái phép các thông tin nhạy cảm.
- **CVE-2024-2887:** Lỗ hổng nhầm lẫn phân loại tồn tại trên tiêu chuẩn WebAssembly (Wasm), cho phép đối tượng tấn công thực thi mã từ xa (RCE) thông qua trang HTML độc hại.
- **CVE-2024-2886:** Lỗ hổng Use After Free tồn tại trong WebCodecs API, cho phép mã hóa và giải mã âm thanh và video. Đối tượng tấn công có thể thực thi mã từ xa khi khai thác lỗ hổng thông qua trang HTML độc hại.
- **CVE-2024-3159:** Lỗ hổng cho phép đọc ngoài phạm vi, tồn tại trong engine V8 JavaScript của Chrome. Đối tượng tấn công có thể truy cập các dữ liệu nằm ngoài phân vùng bộ nhớ đệm, từ đó dẫn đến lỗi heap cho phép đối tượng tấn công trích xuất thông tin nhạy cảm từ hệ thống.

Nguồn: https://www.bleepingcomputer.com/news/security/google-fixes-fifth-chrome-zero-day-vulnerability-exploited-in-attacks-in-2024/?&web_view=true

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 các sản phẩm của D-Link, GitLab và giao thức DHCP, cụ thể như sau:

- **CVE-2015-2041 (Điểm CVSS: 10.0 – Nghiêm trọng)**: Lỗ hổng an toàn thông tin tồn tại trên firmware của thiết bị "D-Link DIR-645 Wired/Wireless Router Rev. Ax" cho phép đối tượng tấn công thực thi mã tùy ý thông qua interface HNAP. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế bởi các nhóm tấn công như Lazarus Group, TeamnTNT và Kinsing; đáng chú ý, trong tháng 04/2024, lỗ hổng này đã bị khai thác bởi botnet Goldoon.
- **CVE-2023-7028 (Điểm CVSS: 7.5 – Cao)**: Lỗ hổng tồn tại trên GitLab CE/EE cho phép đối tượng tấn công đặt lại mật khẩu người dùng sử dụng email không liên kết với tài khoản, từ đó chiếm dụng tài khoản của người dùng. 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.

TOP 10 lỗ hổng đáng chú ý trong tuần

TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	CVE-2015-2051	- Điểm CVSS: 10.0 (Nghiêm trọng) - Ảnh hưởng: D-Link DIR-645. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - 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-2015-2051
2	CVE-2023-7028	- Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: GitLab CE/EE - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép trên tài khoản người dùng. - 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-2023-7028
3	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
4	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
5	CVE-2024-27322	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Ngôn ngữ lập trình R - 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-2024-27322

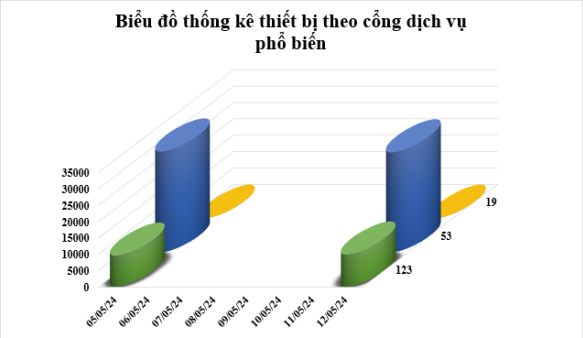
TOP 10 lỗ hổng đáng chú ý trong tuần

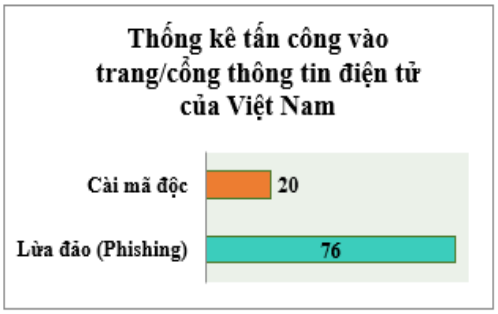
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-21111	- Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Oracle VM VirtualBox - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Lỗ hổng đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công và chỉ ảnh hưởng tới phiên bản trên hệ điều hành Windows.	https://nvd.nist.gov/vuln/detail/CVE-2024-21111
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-2024-31497	- Điểm CVSS: 5.9 (Trung bình) - Ảnh hưởng: PuTTY - 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 đang bị khai thác trong môi trường thực tế bởi các nhóm tấn	https://nvd.nist.gov/vuln/detail/CVE-2024-31497

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 **40.375** (tăng so với tuần trước **40.281**) 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.



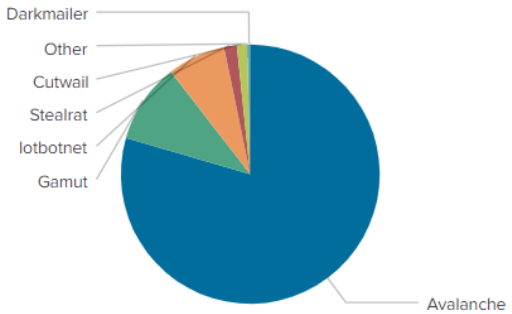


Tấn công Web

Trong tuần, có **96** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 76 trường hợp tấn công lừa đảo (Phishing), 20 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	restless.su
atomictrivia.ru	facialwaxmaxfaxlax3.com
amnsreiuojy.ru	griefcube.cc
hzmksreiuojy.ru	db2017417b23.zapto.org
restlesz.su	uyhgqunqkxnx.pw
xjpakmdcfuqe.biz	focusdate.com
xjpakmdcfuqe.in	zzbtj.lcrgk.com
xjpakmdcfuqe.ru	zmtqozq.info
xjpakmdcfuqe.com	yjxvtkxjqvirdvbgh.org

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **259** 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[.]hdsaison-app[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
2	hdsaison-vn[.]com	Website giả mạoCông ty Tài chính TNHH HD SAISON
3	https://trungtam-dienmayxanh[.]com	Website giả mạo Điện máy xanh
4	https://dienmayxanh542[.]com	Website giả mạo Điện máy xanh
5	https://c[.]vn-ebayn[.]vip	Website giả mạo sàn TMĐT Ebay
6	https://ebayasean[.]com	Website giả mạo sàn TMĐT Ebay
7	https://lazada[.]bbc6666[.]com	Website giả mạo sàn TMĐT Lazada
8	http://vieetcombiank[.]com	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
9	https://mbdkb[.]com	Website giả mạo Ngân hàng TMCP Quân đội
10	vib-mydiamon-khcn-uutien-vnc1[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
11	khcn-my-diamon-han-muc-uu-tien[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
12	http://vib[.]hanmucvn[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
13	http://vib[.]tanghanmuc-vn[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
14	https://tpbank[.]chamsockhachhang-uudaitructuyen[.]online	Website giả mạo Ngân hàng TMCP Tiên Phong
15	kh-cn-mrd-f5-tpbank[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
16	http://mail[.]labtpb[.]online	Website giả mạo Ngân hàng TMCP Tiên Phong
17	https://miles-card-vpbank[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
18	vpb[.]nanghanmucvisa-vn[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
19	http://vpb[.]tang-han-muc-the-visa-vn[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
20	https://vnsendo[.]info	Website giả mạo sàn TMĐT Sendo

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