NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 33 (12/08/2024 – 18/08/2024)

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm tấn công có liên quan tới Black Basta thực hiện chiến dịch phát tán mã độc SystemBC.

- **Cảnh báo:** Phát hiện lỗ hổng RCE trong TCP/IP trên Windows ảnh hưởng đến hệ thống IPv6 mà không cần tương tác từ người dùng.

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: 582** 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: Nhóm tấn công có liên quan tới Black Basta thực hiện chiến dịch phát tán mã độc SystemBC.”

Một chiến dịch tấn công theo hình thức social engineering đã được phát hiện và được nghi ngờ có liên hệ với nhóm sử dụng ransomware Black Basta. Mục tiêu của chiến dịch là đánh cắp thông tin xác thực và phát tán mã độc SystemBC. Kẻ tấn công đã gửi một lượng lớn email chứa mồi nhử, sau đó gọi điện cho người dùng để hướng dẫn cách xử lý.

Chuỗi tấn công bắt đầu bằng việc lừa người dùng tải xuống và cài đặt phần mềm hợp pháp AnyDesk, cho phép đối tượng tấn công truy cập từ xa vào thiết bị và triển khai các payload độc hại nhằm thu thập dữ liệu nhạy cảm.

Trong chiến dịch này, đối tượng tấn công sử dụng file thực thi có tên “AntiSpam.exe”, giả mạo là công cụ lọc email spam và thúc giục người dùng nhập thông tin đăng nhập Windows để hoàn tất cập nhật.

Tiếp theo, đối tượng tấn công thực thi các tệp binary, DLL, và script PowerShell có chứa một HTTP beacon viết bằng Golang để kết nối với máy chủ từ xa, cùng với một proxy SOCKS và mã độc SystemBC.

Theo các chuyên gia bảo mật, để giảm thiểu rủi ro, người dùng nên chặn tất cả các giải pháp truy cập từ xa trên máy tính và cảnh giác với các cuộc gọi hoặc tin nhắn bất thường tự nhận là từ nhân viên IT nội bộ.

Thông tin về chiến dịch này được công bố trong bối cảnh nhiều mã độc khác như SocGholish (FakeUpdates), GootLoader, và Raspberry Robin đang là những bộ nạp mã độc phổ biến nhất trong năm 2024. Những mã độc này thường được sử dụng để triển khai ransomware và được bán trên các diễn đàn Dark web theo mô hình trả phí hàng tháng.

Nguồn: https://thehackernews.com/2024/08/black-basta-linked-attackers-targets.html

Tin tức An toàn thông tin

"Chiến dịch tấn công APT: Nhóm tấn công có liên quan tới Black Basta thực hiện chiến dịch phát tán mã độc SystemBC."

Chiến dịch trên chỉ là một phần của loạt tấn công lừa đảo và social engineering được phát hiện trong tuần qua. Một số nhóm tấn công khác còn sử dụng mã QR giả mạo để gây hại, bao gồm:

- Chiến dịch ClearFake sử dụng website để phát tán mã độc .NET dưới dạng cập nhật Google Chrome.
- Tấn công lừa đảo với nội dung tuyển dụng để phát tán mã độc như AsyncRAT, Pure HVNC, XWorm và Venom RAT thông qua shellcode loader viết bằng Python.
- Chiến dịch sử dụng website giả mạo ngân hàng tại Anh để phát tán phần mềm AnyDesk tới người dùng Windows và macOS, qua đó đánh cắp dữ liệu.
- Website giả mạo WinRAR phát tán ransomware, mã độc đào tiền ảo và mã độc đánh cắp dữ liệu Kematian Stealer.
- Chiến dịch drive-by-download sử dụng quảng cáo độc hại và các website bị xâm nhập để phân phối mã độc NetSupport RAT.
- Chiến dịch quảng cáo mã độc trên mạng xã hội, chiếm dụng tài khoản Facebook để quảng bá website chỉnh ảnh AI, lừa người dùng tải xuống công cụ ITarian nhằm truy cập hệ thống và phát tán mã độc Lumma Stealer.

Một số IoC được ghi nhận:

spamicrosoft[.]com	91.142.74[.]28
37.221.126[.]202	191.142.74[.]28
91.196.70[.]160	195.2.70[.]38
halagifts[.]com	falseaudiencekd[.]shop
217.15.175[.]191	feighminoritsjda[.]shop
preservedmoment[.]com	justifycanddidatewd[.]shop
45.155.249[.]97	marathonbeedksow[.]shop
77.238.224[.]56	pleasurenarrowsdla[.]shop
77.238.229[.]63	raiseboltskdlwpow[.]shop
77.238.250[.]123	richardfloresp oew[.]shop
77.238.245[.]233	strwawrunnygjwu[.]shop

Nguồn: https://thehackernews.com/2024/08/black-basta-linked-attackers-targets.html

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Cảnh báo: Phát hiện lỗ hổng RCE trong TCP/IP trên Windows ảnh hưởng đến hệ thống IPv6 mà không cần tương tác từ người dùng."

Trong tuần qua, Microsoft đã phát hành bản vá cho một lỗ hổng nghiêm trọng trong giao thức TCP/IP trên hệ thống Windows, cho phép thực thi mã từ xa (RCE) với mã định danh CVE-2024-38063. Lỗ hổng này tồn tại trên mọi hệ thống Windows có IPv6 được bật mặc định, bao gồm Windows 10, Windows 11 và các phiên bản Windows Server.

Lỗ hổng CVE-2024-38063 phát sinh do lỗi Integer Underflow, cho phép đối tượng tấn công gây ra tràn bộ đệm và thực thi mã tùy ý trên hệ thống mục tiêu. Đáng chú ý, việc chặn IPv6 trên tường lửa của Windows không đủ để ngăn chặn lỗ hổng này bị khai thác, vì lỗi xảy ra trước khi tường lửa xử lý thông tin.

Microsoft cảnh báo rằng lỗ hổng có thể bị khai thác từ xa thông qua các cuộc tấn công có mức độ phức tạp thấp, bằng cách gửi liên tục các gói tin IPv6 chứa mã độc. Hãng cũng đánh giá đây là lỗ hổng "dễ bị khai thác," cho phép đối tượng tấn công tạo mã khai thác để tấn công liên tục. Nếu chưa thể cập nhật bản vá, Microsoft khuyến nghị người dùng nên tạm thời vô hiệu hóa IPv6 để tránh bị ảnh hưởng.

Một cơ quan bảo mật khác cũng nhận định rằng lỗ hổng này có thể được biến thành mã độc dạng worm, vì kẻ tấn công có thể thực thi mã từ xa với quyền truy cập cao sau khi khai thác thành công.

Trong những năm gần đây, Microsoft đã khắc phục nhiều lỗ hổng liên quan đến IPv6, bao gồm hai lỗ hổng TCP/IP (CVE-2020-16898 và CVE-2020-16899) có thể bị khai thác để thực thi mã từ xa và tấn công từ chối dịch vụ thông qua các gói tin ICMPv6 Router Advertisement độc hại. Ngoài ra, lỗ hổng phân mảnh IPv6 (CVE-2021-24086) đã làm ảnh hưởng đến mọi phiên bản Windows với nguy cơ bị tấn công DoS, và lỗ hổng CVE-2023-28231 trên DHCPv6 cũng cho phép đối tượng tấn công thực thi mã từ xa.

Mặc dù chưa có ghi nhận về việc lỗ hổng này bị khai thác trong các chiến dịch tấn công diện rộng, người dùng vẫn nên cập nhật bản vá càng sớm càng tốt để giảm thiểu rủi ro bị tấn công.

Nguồn: https://www.bleepingcomputer.com/news/microsoft/zero-click-windows-tcp-ip-rce-impacts-all-systems-with-ipv6-enabled-patch-now/

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 **458** lỗ hổng, trong đó có 214 lỗ hổng mức Cao, 160 lỗ hổng mức Trung bình, 13 lỗ hổng mức Thấp và 71 lỗ hổng chưa đánh giá. Trong đó có ít nhất 90 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 1Password và Microsoft, cụ thể là như sau:

- **CVE-2018-0824 (Điểm CVSS: 8.8 - Cao):** Lỗ hổng tồn tại trên "Microsoft COM for Windows" cho phép đối tượng tấn công thực thi mã từ xa thông qua lỗi xử lý đối tượng tuần tự thất bại. Hiện lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế.
- **CVE-2024-42219 (Điểm CVSS: 7.0 – Cao):** Lỗ hổng tồn tại trên ứng dụng 1Password cho hệ điều hành macOS, xảy ra do quá trình xác thực liên lạc giữa các tiến trình XPC thất bại. Cho phép đối tượng tấn công truy cập và trích xuất các thông tin lưu trong ứng dụng. Hiện lỗ hổng chưa có mã khai thác và chưa có ghi nhận khai thác trong môi trường thực tế bởi các nhóm tấn công.
- **CVE-2024-42218 (Điểm CVSS: 6.3 – Trung bình):** Lỗ hổng tồn tại trên ứng dụng 1Password cho hệ điều hành macOS. Đối tượng tấn công có thể khai thác lỗ hổng bằng cách vượt qua các biện pháp bảo mật của macOS, qua đó cho phép đối tượng tấn công truy cập và trích xuất các thông tin lưu trong ứng dụng. Hiện lỗ hổng chưa có mã khai thác và chưa có ghi nhận 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-2018-0824	- Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Microsoft Windows 7, Windows 8 Windows 10, Windows 11, Windows Server 2012. - 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-2018-0824
2	CVE-2024-42219	- Điểm CVSS: 7.0 (Cao) - Ảnh hưởng: 1Password - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện 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-2024-42219
3	CVE-2024-42218	- Điểm CVSS: 6.3 (Trung bình) - Ảnh hưởng: 1Password - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện 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-2024-42218
4	CVE-2024-38077	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: Windows Server 2022, Windows Server 2012, Windows Server 2016, Windows Server 2019. - 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-2024-38077
5	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

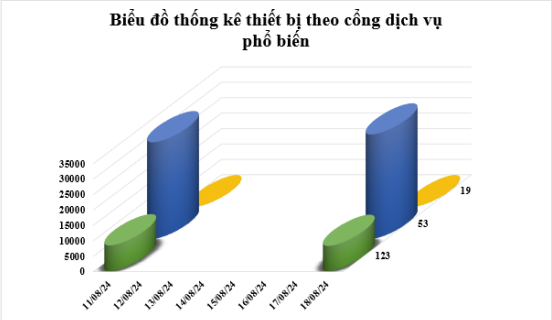
TOP 10 lỗ hổng đáng chú ý trong tuần

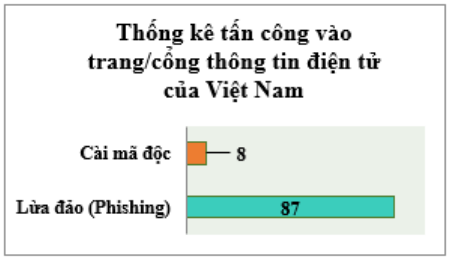
TT	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
6	CVE-2024-27198	- Điểm CVSS: 9.8 (Nghiêm trọng) - Ảnh hưởng: JetBrains TeamCity - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong môi trường thực tế bởi các nhóm tấn công.	https://nvd.nist.gov/vuln/detail/CVE-2024-27198
7	CVE-2024-36877	- Điểm CVSS: 8.2 (Cao) - Ảnh hưởng: Bo mạch chủ dòng series Z và series B của hãng Micro-Star International (MSI). - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý, 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-2024-36877
8	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
9	CVE-2024-21733	- Điểm CVSS: 5.3 (Trung bình) - Ảnh hưởng: Apache Tomcat - Mô tả: Lỗ hổng cho phép đối tượng 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-2024-21733
10	CVE-2024-36424	- Điểm CVSS: 5.5 (Trung bình) - Ảnh hưởng: K7 Ultimate Security. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - 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-2024-36424

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 **42.096** (tăng so với tuần trước **39.745**) 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.



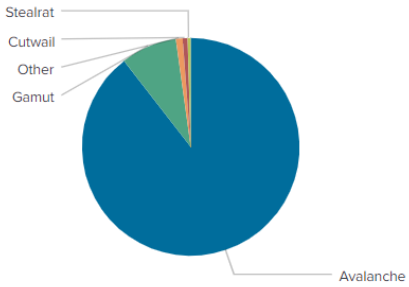


Tấn công Web

Trong tuần, có **95** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 87 trường hợp tấn công lừa đảo (Phishing), 8 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	griefcube.cc
amnsreiuojy.ru	uyhgqunqkxnx.pw
hzmksreiuojy.ru	xiaoe.com
xjpakmdcfuqe.biz	vqelhmqyuphr.info
restlesz.su	rikip.com
xjpakmdcfuqe.com	mildwave.com
xjpakmdcfuqe.in	maxisurf.net
xjpakmdcfuqe.ru	ljjskttqximu.in

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **582** 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://amazonl4[.]com	Website giả mạo Amazon
2	https://www[.]giaohangtietkiem247[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	https://www[.]cct-giaohangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://vn-eid[.]com	Website giả mạo Dịch vụ công Quốc Gia
5	https://dichvucong[.]snggov[.]com	Website giả mạo Dịch vụ công Quốc Gia
6	https://dienmayxanh389[.]com	Website giả mạo Điện máy xanh
7	https://acb[.]chamsocthekhachhang-tructuyen-thang8[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
8	https://acb[.]chamsockhachhang-uudaithetructuyen-thang8[.]online	Website giả mạo Ngân hàng TMCP Á Châu
9	https://www[.]baovietin[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
10	https://www[.]baovietvay[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
11	https://hotro0nline28[.]com	Website giả mạo Ngân hàng TMCP Quân đội
12	https://taichineximbak[.]com	Website giả mạo Ngân Hàng TMCP Xuất Nhập Khẩu Việt Nam
13	https://sendotv[.]shop	Website giả mạo sàn TMĐT Sendo
14	https://www[.]vnsendotv[.]vip	Website giả mạo sàn TMĐT Sendo
15	https://nuk36952s[.]com	Website giả mạo sàn TMĐT Shopee
16	https://sp61889p[.]com	Website giả mạo sàn TMĐT Shopee
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