TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

NCSC VN
National Cyber Security Center

CẢNH BÁO TUẦN

SỐ 37 (13/09/2021 – 19/09/2021)

Thông tin liên hệ: Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 – ais.@mic.gov.vn

Tầng 16, số 115 Trần Duy Hưng, quận Cầu Giấy, Tp.Hà Nội

NCSC VN
National Cyber Security Center

NỘI DUNG TUẦN

"NỖ LỰC ĐỂ KHÔNG GIAN MẠNG VIỆT NAM LUÔN AN TOÀN, LÀNH MẠNH"

TIN CẢNH BÁO

- **Cảnh báo:** Microsoft công bố danh sách bản vá tháng 9/2021 cho các lỗ hổng bảo mật quan trọng

- **Chiến dịch tấn công APT:** Nhóm tấn công mạng APT C-36 sử dụng email lừa đảo để phát tán mã độc RAT

ĐIỂM YẾU, LỖ HỔNG

- **453** lỗ hổng được công bố và cập nhật.

- **07** lỗ hổng, nhóm lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam.

SỐ LIỆU, THỐNG KÊ

- Tấn công DRDoS
- Tấn công Web
- Tấn công lừa đảo người dùng Việt Nam

Hot News!

Tài liệu lưu trữ:

Chuyên mục **Báo cáo định kỳ** tại địa chỉ:

https://service.khonggianmang.vn

TIN CẢNH BÁO

Cảnh báo: Microsoft công bố danh sách bản vá tháng 9/2021 cho các lỗ hổng bảo mật quan trọng

Giữa tháng 9 năm 2021, Microsoft đã công bố danh sách bản vá cho 60 lỗ hổng bảo mật bao gồm 4 lỗ hổng mức nghiêm trọng và 56 lỗ hổng mức cao trên các sản phẩm của mình. Trong đó có một số bản vá đáng chú ý cho các lỗ hổng bảo mật như sau:

Lỗ hổng bảo mật CVE-2021-40444 có mức ảnh hưởng nghiêm trọng trong Microsoft Windows với điểm CVSS 8,8, cho phép đối tượng tấn công thực thi mã từ xa, đang được khai thác tích cực trong thời gian qua. Kẻ tấn công tạo tài liệu Microsoft Office có chứa trình điều khiển ActiveX độc hại.

Lỗ hổng bảo mật EoP CVE-2021-36968 có mức ảnh hưởng cao trong Windows DNS với điểm CVSS 7,8, cho phép đối tượng tấn công nâng cao đặc quyền trên hệ thống mục tiêu.

03 lỗ hổng bảo mật CVE-2021-38667, CVE-2021-38671 và CVE-2021-40447 có mức ảnh hưởng cao trong Windows Print Spooler với điểm CVSS 7,8. Trong đó, CVE-2021-38671 là lỗ hổng được đánh giá là có nhiều khả năng bị khai thác hơn.

03 lỗ hổng bảo mật CVE-2021-36955, CVE-2021-36963 và CVE-2021-38633 trong Windows Common Log File System Driver (CLFS) cho phép kẻ tấn công nâng cao đặc quyền trên hệ thống mục tiêu. Microsoft đánh giá đây là những lỗ hổng dễ bị khai thác, là mục tiêu lớn đối với các đối tượng tấn công.

02 lỗ hổng bảo mật CVE-2021-36975 và CVE-2021-38639 trên Win32k có mức ảnh hưởng cao với điểm CVSS 7,8. Những kẻ tấn công khai thác lỗ hổng này để nâng cao đặc quyền trên hệ thống mục tiêu. Vì Win32k là thành phần cốt lõi của Windows, nên người dùng cần cập nhật bản vá sớm.

Danh sách các bản vá cho các lỗ hổng của Microsoft tham khảo tại:

https://msrc.microsoft.com/update-guide/releaseNote/2021-Sep

Nguồn: https://www.tenable.com/blog/microsoft-s-september-2021-patch-tuesday-addresses-60-cves-cve-2021-40444

Nhóm tấn công mạng APT C-36 sử dụng email lừa đảo để phát tán mã độc RAT

Gần đây, các chuyên gia bảo mật phát hiện 1 chiến dịch tấn công của nhóm APT C-36 nhằm mục tiêu vào Nam Mỹ. Nhóm đã sử dụng nhiều phần mềm độc hại khác nhau như njRAT, BitRAT, Async RAT và Lime RAT.

Hầu hết các mục tiêu đều ở Colombia, tuy nhiên một số có trụ sở tại Ecuador, Tây Ban Nha và Panama. Nhóm này nhằm mục tiêu chủ yếu vào các lĩnh vực tài chính, chính phủ và y tế. Một số mục tiêu khác được quan sát thấy là lĩnh vực năng lượng, dầu khí và viễn thông.

APT C-36 sử dụng email lừa đảo, giả danh các email từ tổng cục thuế và hải quan Colombia. Nội dung email liên quan đến việc tịch thu một tài khoản ngân hàng, còn thông tin các chi tiết khác được cung cấp bên trong tệp đính kèm email. Một số email lừa đảo khác, người nhận được yêu cầu mở file đính kèm có tên là picture[.]jpg với mật khẩu file là “foto”. Các file đính kèm độc hại này có dạng PDF/DOCX, trong đó bao gồm một liên kết. Khi người nhận nhấp vào liên kết đó, sẽ bị chuyển hướng đến trang web lưu trữ một loại tệp tin. Tệp tin này có chứa phần mềm độc hại BitRAT và sẽ tự động tải xuống máy mục tiêu.

Nguồn: https://cyware.com/news/apt-c-36-drops-commodity-rats-for-financial-gains-27ecf47a

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 453 lỗ hổng, trong đó có 02 lỗ hổng mức cao, 19 lỗ hổng mức trung bình, 0 lỗ hổng mức thấp và 432 lỗ hổng chưa đánh giá. Trong đó có ít nhất 110 lỗ hổng cho phép chèn và thực thi mã lệnh.

Hệ thống kỹ thuật của Cục ATTT chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có 07 lỗ hổng/nhóm lỗ hổng trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam: Nhóm 209 lỗ hổng trong các sản phẩm của Apple, Nhóm 46 lỗ hổng trong WordPress, Nhóm 20 lỗ hổng trong phần mềm Google, Nhóm 13 lỗ hổng trong các sản phẩm của Cisco, Nhóm 12 lỗ hổng trong Aruba Networks, Nhóm 10 lỗ hổng trong phần mềm Adobe, Nhóm 09 lỗ hổng trong phần mềm Nextcloud. Thông tin chi tiết về một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

Một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam:

- Apache: CVE-2021-39275, CVE-2021-34798,...

- IBM: CVE-2021-29825, CVE-2021-29752,...

- Zohocorp: CVE-2021-37422, CVE-2021-37423,...

- BIG-IP: CVE-2021-23038, CVE-2021-23042,...

- Jitsi: CVE-2021-39205, CVE-2021-39215

- McAfee: CVE-2021-31845, CVE-2021-31844,...

- Microsoft: CVE-2021-36956, CVE-2021-40440,...

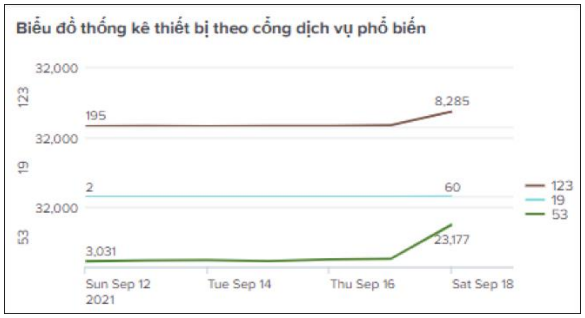
Thông tin điểm yếu, lỗ hổng

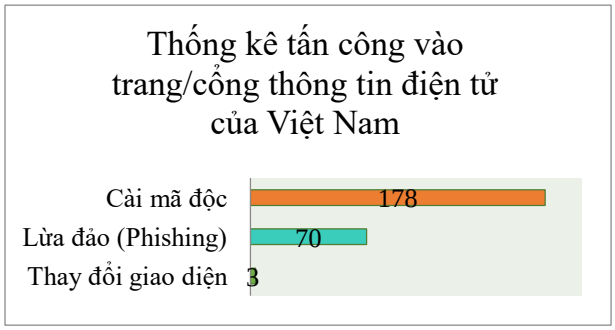
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Apache	CVE-2021-39275 CVE-2021-34798 CVE-2021-39239 …	Nhóm 07 lỗ hổng trong phần mềm Apache (Apache HTTP Server, Apache Jena) cho phép đối tượng tấn công thực thi mã từ xa	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2021-29825 CVE-2021-29752 CVE-2021-29763 …	Nhóm 11 lỗ hổng trong sản phẩm của IBM (IBM Db2) cho phép đối tượng tấn công thu thập thông tin, nâng cao đặc quyền, tấn công giả mạo XSS.	Đã có thông tin xác nhận và bản vá
3	Zohocorp	CVE-2021-37422 CVE-2021-37423 CVE-2021-37414	Nhóm 03 lỗ hổng trong sản phẩm của Zohocorp (Zoho ManageEngine ADSelfService Plus, Zoho ManageEngine DesktopCentral) cho phép đối tượng tấn công thực hiện tấn công SQL Injection.	Đã có thông tin xác nhận và bản vá
4	BIG-IP	CVE-2021-23038 CVE-2021-23042 CVE-2021-23040 …	Nhóm 29 lỗ hổng trong các sản phẩm của BIG-IP (BIG-IP AFM,…) cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền, tấn công giả mạo XSS	Đã có thông tin xác nhận và bản vá
5	Jitsi	CVE-2021-39205 CVE-2021-39215	Nhóm 02 lỗ hổng trong phần mềm Jitsi (Jitsi Meet) cho phép đối tượng tấn công thực hiện tấn công giả mạo XSS.	Chưa có thông tin xác nhận và bản vá
6	McAfee	CVE-2021-31845 CVE-2021-31844 CVE-2021-31842 …	Nhóm 04 lỗ hổng trong sản phẩm của McAfee (McAfee Data Loss Prevention (DLP) Endpoint, McAfee Endpoint Security (ENS),…) cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền.	Đã có thông tin xác nhận và bản vá
7	Microsoft	CVE-2021-36956 CVE-2021-40440 CVE-2021-38655 …	Nhóm 62 lỗ hổng trong sản phẩm của Microsoft (Microsoft Edge, Microsoft Excel, Office,…) cho phép đối tượng tấn công thu thập thông tin, thực thi mã từ xa, tấn công giả mạo XSS, nâng cao đặc quyền, tấn công từ chối dịch vụ	Đã có thông tin xác nhận và bản vá

Thống kê nguy cơ, các cuộc tấn công tại 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 **55,331** (tăng so với tuần trước **53,246**) 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.



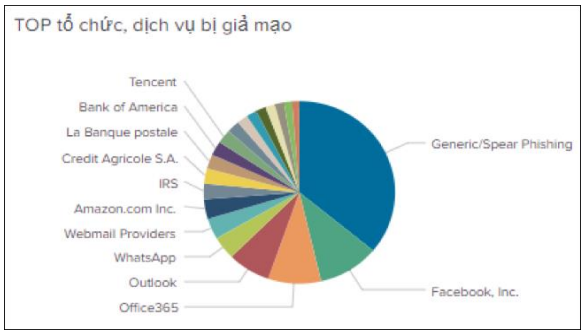


Tấn công Phishing

Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như: Các mạng xã hội, ngân hàng, thư điện tử .v.v… Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và tính phí) như các mạng xã hội, Paypment, Apple, Paypal ..v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

Tấn công Web

Trong tuần, có 251 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 03 trường hợp tấn công thay đổi giao diện, 70 trường hợp tấn công lừa đảo (Phishing), 178 trường hợp tấn công cài cắm mã độc.



Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

differentia.ru	a.asense.in
disorderstatus.ru	ww2.bbbjdnxbgp3.ru
atomictrivia.ru	a.deltaheavy.ru
morphed.ru	sdk.asense.in
ydbnsrt.me	soplifan.ru

New

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có 102 phản ánh trường hợp lừa đảo do người dùng Internet Việt Nam thông báo 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 website của ngân hàng, lừa đảo liên quan đến COVID…

Dưới đây là một số trường hợp người dùng cần nâng cao cảnh giác.

STT	Website lừa đảo	Ghi chú
1	https://chanle247.com/ https://cltxuytin.win/ https://momoloto.club/ https://chanletaixiu.net/ https://chanlemomo.win/ https://x102.net/ http://cluytin.win/ https://nsomomo.com/ http://clmmvip.com/ https://chamlemm.online Thanhphomomo.com	Web lừa đảo cờ bạc qua ví điện tử Momo
2	ipnbd19.com	Lừa đảo mua bán trực tuyến Shopee
3	www.ufapj.com/sccb www.rkceb.com/sccb www.mxsccb.com https://www.fasccb.com/	Giả mạo ngân hàng SCB
4	https://tiki-88.com/index/ctrl/deposited	Website giả mạo sàn TMĐT Tiki
5	https://aquank.com/ez3	Ứng dụng cho vay lừa đảo
6	http://www.lddianci.com/	Giả mạo website Báo Thế giới&Việt Nam
7	truongtonducthang.edu.vn https://www.tu.edu.vn	Giả mạo website trường Đại học Tôn Đức Thắng
8	https://cs6162.com/	Ứng dụng lừa đảo mua bán

Khuyến nghị đối với các cơ quan, đơn vị

1. Đối với các nguy cơ, cảnh báo đã được đề cập trong phần **Tin cảnh báo** 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 **Nguy cơ tấn công mạng từ điểm yếu lỗ hổng**, 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, những đơn vị đã có tài khoản trên "Hệ thống Cảnh báo điểm yếu và rà soát lỗ hổng bảo mật tự động" tại địa chỉ https://service.khonggianmang.vn, quản trị viên có thể thêm các sản phẩm đang sử dụng để giám sát và nhận cảnh báo ngay khi có lỗ hổng mới phát sinh.

***

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.

***

4. 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.

***

Thông tin liên hệ:

Trung tâm Giám sát an toàn không gian mạng quốc gia

024.3209.1616 - ais@mic.gov.vn