NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

CẢNH BÁO TUẦN

Số 09 (26/02/2024 – 03/03/2024)

s

NỘI DUNG TUẦN

1. Tin tức An toàn thông tin

- **Chiến dịch tấn công APT:** Nhóm APT người Trung Quốc khai thác lỗ hổng Zero-day trên Ivanti để triển khai mã độc

- **Cảnh báo:** Hàng triệu mã xác thực hai bước (2FA) của Google, WhatsApp, Facebook bị lộ lọt trên không gian mạng.

2. Điểm yếu, lỗ hổng

- **1.014** 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.

3. Số liệu, thống kê

- **Tấn công DRDoS**

- **Tấn công Web**

- **Tấn công lừa đảo người dùng Việt Nam: 254** 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

"Nhóm APT người Trung Quốc khai thác lỗ hổng Zero-day trên Ivanti để triển khai mã độc."

Các nhóm APT có liên kết tới Trung Quốc đang cố duy trì trạng thái lây nhiễm sau khi khai thác thành công lỗ hổng an toàn thông tin trên Ivanti Connect Secure VPN kể cả sau khi thiết bị reset về trạng thái mặc định, cập nhật hệ thống hay bản vá.

Nhóm APT UNC5325 thành thạo về kỹ thuật "living-off-the-land" (sử dụng các công cụ sẵn có trên hệ thống như PowerShell để thực hiện tấn công). Cụ thể hơn, nhóm này đang sử dụng mã độc như LittleLamb.WoolTea để duy trì trạng thái lây nhiễm.

Ivanti đã công bố 5 lỗ hổng khác nhau kể từ 10/01, trong đó bao gồm CVE-2024-21893, lỗ hổng SSRF trong thành phần SAML của Ivanti Connect Secure, Ivanti Policy Secure và Ivanti Neurons cho thiết bị ZTA. Việc khai thác thành công lỗ hổng đã cho phép UNC5325 truy cập trái phép vào các tài nguyên hạn chế.

Một cơ quan bảo mật đã liên kết UNC5325 với một nhóm APT khác là UNC3886 do điểm tương đồng về chiến thuật, kỹ thuật và quá trình tấn công. Nhóm UNC3886 được tình nghi là một nhóm gián điệp không gian mạng người Trung Quốc cũng sử dụng các lỗ hổng Zero-day nhằm vào cơ sơ công nghiệp quốc phòng, tổ chức công nghệ và viễn thông đặt tại Mỹ và khu vực châu Á Thái Bình Dương.

Trong chiến dịch tấn công, UNC5325 đã triển khai biến thể của webshell BushWalk để đọc file tùy ý và tránh bị phát hiện. Đối tượng còn lợi dụng các thành phần vốn có của Ivanti như plugin SparkGateway để triển khai backdoor, qua đó xâm nhập sâu hơn vào hệ thống bị ảnh hưởng. Bằng cách chèn các object chung vào SparkGateway, đối tượng đã tạo đường dẫn cho các khai thác sau này.

UNC5325 còn sử dụng cơ chế backup dữ liệu hệ thống và căn thời điểm hành động vào lúc cập nhật để bí mật nhúng mã độc vào hệ thống sau khi được cập nhật. Một thủ đoạn khác để duy trì trạng thái lây nhiễm được sử dụng là phân tích chi tiết phần cứng của thiết bị rồi điều chỉnh quá trình reset về trạng thái mặc định để vẫn còn tồn tại sau khi reset. Tuy nhiên, nỗ lực để tồn tại sau khi reset về trạng thái mặc định của nhóm này chưa thành công.

Nguồn: https://www.bankinfosecurity.com/chinese-group-runs-highly-persistent-ivanti-0-day-exploits-a-24471?&web_view=true

NCSC VN
National Cyber Security Center

Tin tức An toàn thông tin

"Hàng triệu mã xác thực hai bước (2FA) của Google, WhatsApp, Facebook bị lộ lọt trên không gian mạng."

Các chuyên gia bảo mật đã từng đưa ra khuyến cáo người dùng không nên sử dụng tin nhắn SMS cho việc nhận mã 2FA do chúng dễ bị chặn bắt hoặc xâm phạm. Gần đây, các chuyên gia đã phát hiện ra một cơ sở dữ liệu không bảo mật có chứa hàng triệu các mã 2FA, và có thể dễ dàng đọc được bởi những đối tượng truy cập vào cơ sở dữ liệu.

Cụ thể hơn, cơ sở dữ liệu có thể dễ dàng truy cập được trên Internet này đã không được đặt mật khẩu. Các đối tượng biết được địa chỉ IP của cơ sở dữ liệu có thể dễ dàng truy cập vào sử dụng bất kì trình duyệt web thông thường nào trên không gian mạng. Qua quá trình điều tra, cơ sở dữ liệu đã được phát hiện là thuộc sở hữu của YX International, một công ty châu Á cung cấp dịch vụ điều hướng tin nhắn SMS, cùng một số dịch vụ khác. Hiện cơ sở dữ liệu này đã được phía công ty bảo mật lại sau khi được nhắc nhở.

Với lượng tin nhắn luân chuyển hàng ngày lên tới 5 triệu tin, cơ sở dữ liệu của YX International đã trở thành một mỏ vàng chứa thông tin quan trọng như: đường dẫn reset mật khẩu, mã 2FA cho Google, WhatsApp, Facebook và TikTok.

Trong phần lịch sử sử, tin nhắn cũ nhất ghi lại trên cơ sở dữ liệu là từ tháng 07/2023, việc thiếu sót mật khẩu để bảo mật cơ sở dữ liệu có thể gây chấn động cho nhiều người dùng, tuy nhiên, các chuyên gia cho rằng người dùng không cần quá bất an. Lí do chính là bản chất của các mã 2FA có thời hạn sử dụng rất ngắn, một đối tượng tấn công muốn lợi dụng việc lộ lọt của cơ sở dữ liệu này cần phải giám sát liên tục cả hoạt động của người dùng lẫn sự thay đổi trên cơ sở dữ liệu, điều này trong thực tế là rất hiếm xảy ra

Vậy người dùng có nên tiếp tục sử dụng tin nhắn SMS làm phương thức nhận mã 2FA?

Ý kiến của chuyên gia bảo mật đã cho rằng, với các mối đe dọa trên không gian mạng dần trở nên phức tạp và đa lớp, tài khoản người dùng cần phải được bảo mật một cách tương tự sử dụng các ứng dụng xác thực, khóa bảo mật vật lý và passkey; và người dùng nên cân nhắc các lựa chọn này nếu họ vẫn đang sử dụng mã 2FA nhận từ SMS hoặc thậm chí là không sử dụng 2FA.

Nguồn:https://www.forbes.com/sites/daveywinder/2024/03/04/millions-of-google-whatsapp-facebook-2fa-security-codes-leak-online/?ss=cybersecurity&sh=629f9cf774d1

NCSC VN
National Cyber Security Center

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 **1.014** lỗ hổng, trong đó có 125 lỗ hổng mức Cao, 300 lỗ hổng mức Trung bình, 33 lỗ hổng mức Thấp và 556 lỗ hổng chưa đánh giá. Trong đó có ít nhất 162 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 304 lỗ hổng trong Linux, Nhóm 02 lỗ hổng trong Google, Nhóm 03 lỗ hổng trong Microsoft, Nhóm 10 lỗ hổng trong Dell, Nhóm 08 lỗ hổng trong Adobe, Nhóm 06 lỗ hổng trong Cisco, Nhóm 22 lỗ hổng trong IBM. 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:

- Linux: CVE-2024-1784, CVE-2019-25160,...

- Google: CVE-2024-1938, CVE-2024-1939

- Microsoft: CVE-2024-26192, CVE-2024-21423,...

- Dell: CVE-2024-24903, CVE-2024-22457,...

- Adobe: CVE-2024-20765, CVE-2023-44341,...

- Cisco: CVE-2024-20267, CVE-2024-20321,...

- IBM: CVE-2022-43842, CVE-2023-25921,...

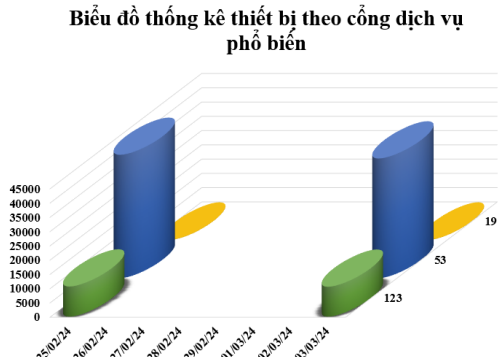
Thông tin điểm yếu, lỗ hổng

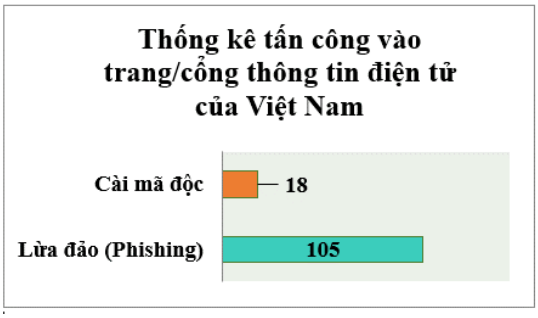
TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Linux	CVE-2024-1784 CVE-2019-25160 CVE-2019-25162 …	Nhóm 304 lỗ hổng trong Linux cho phép đối tượng tấn công thực hiện SQL Injection, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
2	Google	CVE-2024-1938 CVE-2024-1939	Nhóm 02 lỗ hổng trong Google cho phép đối tượng tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
3	Microsoft	CVE-2024-26192 CVE-2024-21423 CVE-2024-26188	Nhóm 03 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện tấn công truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Dell	CVE-2024-24903 CVE-2024-22457 CVE-2024-24904 …	Nhóm 10 lỗ hổng trong Dell cho phép đối tượng tấn công khai thác lỗ hổng XSS, thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa.	Chưa có thông tin xác nhận và bản vá
5	Adobe	CVE-2024-20765 CVE-2023-44341 CVE-2023-44342 …	Nhóm 08 lỗ hổng trong Adobe cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
6	Cisco	CVE-2024-20267 CVE-2024-20321 CVE-2024-20294 …	Nhóm 06 lỗ hổng trong Cisco cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
7	IBM	CVE-2022-43842 CVE-2023-25921 CVE-2023-25925 …	Nhóm 22 lỗ hổng trong IBM phép đối tượng tấn công thực hiện SQL Injection, thực thi mã từ xa, khai thác lỗ hổng XSS, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

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 **52.509** (giảm so với tuần trước **53.886**) 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.



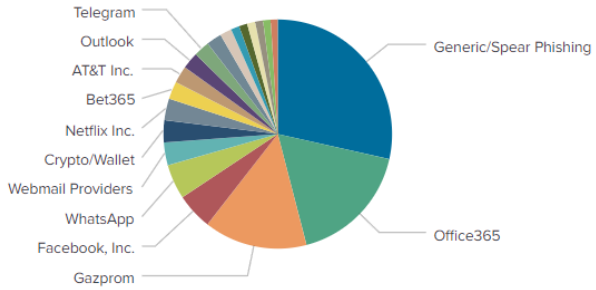


Tấn công Web

Trong tuần, có **128** trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 108 trường hợp tấn công lừa đảo (Phishing), 18 trường hợp tấn công cài cắm mã độc.

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, Payment, Apple, Paypal,v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để đánh cắp tài khoản.



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

differentia.ru: 8273 IP	hzmksreiuojy.ru: 130 IP
disorderstatus.ru: 4324 IP	xjpakmdcfuqe.biz: 149 IP
atomictrivia.ru: 1967 IP	xjpakmdcfuqe.com: 94 IP
amnsreiuojy.ru: 527 IP	xjpakmdcfuqe.ru: 89 IP
restlesz.su: 241 IP	xjpakmdcfuqe.in: 87 IP

Tấn công lừa đảo người dùng Việt Nam

Trong tuần đã có **254** 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 website của ngân hàng, các trang thương mại điện tử…

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

STT	Website lừa đảo	Ghi chú
1	amadbfk.shop	Website giả mạo sàn TMĐT Amazon
2	hgff11.com	Website giả mạo sàn TMĐT Tiki
3	scb.chamsockhachhang-truc-tuyen-the.online	Website giả mạo Ngân hàng TMCP Sài Gòn
4	soppe68.com vn88631p.com spmail86.com	Website giả mạo sàn TMĐT Shopee
5	cskh-vib-canhan.com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam

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, 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. 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**, Quý đơn vị cần chú ý quan tâm không truy cập vào các trang web được nêu để tránh nguy cơ bị tấn công lừa đảo, nâng cao nhận thức bản thân và tuyên truyền cho bạn bè, người thân và những người xung quanh tránh việc trở thành nạn nhân của những cuộc tấn công lừa đảo này.

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