TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG QUỐC GIA

NCSC VN
National Cyber Security Center

# CẢNH BÁO TUẦN

SỐ 32 (09/08/2021 – 15/08/2021)

**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 xác nhận thêm 1 lỗ hổng bảo mật mới Windows Print Spooler

- **Chiến dịch tấn công APT:** Nhóm tấn công mạng UNC215 nhằm mục tiêu vào các tổ chức của Israel

## ĐIỂM YẾU, LỖ HỔNG

- **639** 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 xác nhận thêm 1 lỗ hổng bảo mật mới Windows Print Spooler

Sau khi phát hành danh sách bản vá vào tháng 8 năm 2021, Microsoft đã công bố thêm thông tin mới của một lỗ hổng khác (CVE-2021-36958) trong Print Spooler. Lỗ hổng này đã được một chuyên gia bảo mật công bố từ giữa tháng 7/2021 và đã có mã khai thác công khai.

Microsoft cho biết CVE-2021-36958 là một lỗ hổng thực thi mã từ xa tồn tại khi dịch vụ Windows Print Spooler thực hiện không đúng các hoạt động tệp đặc quyền, có điểm CVSS: 7.3 (cao). Khai thác thành công lỗ hổng này, cho phép đối tượng tấn công thực thi mã tùy ý với các đặc quyền hệ thống, từ đó có thể chiếm quyền điều khiển toàn bộ hệ thống mục tiêu.

Tại thời điểm hiện tại chưa có bản vá cho lỗ hổng bảo mật này. Thay vào đó, Microsoft đã đưa ra biện pháp khắc phục để giảm thiểu rủi ro khai thác bằng cách vô hiệu hóa dịch vụ Print Spooler. Quý đơn vị tham khảo tại:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958

*Nguồn:* https://www.helpnetsecurity.com/2021/08/13/cve-2021-36958/?web_view=true


# Nhóm tấn công mạng UNC215 nhằm mục tiêu vào các tổ chức của Israel

UNC215 là nhóm tấn công mạng từ Trung Quốc nhằm mục tiêu vào các tổ chức của Israel. Các cuộc tấn công này đã nhằm vào các dịch vụ CNTT, các tổ chức chính phủ và các công ty viễn thông kể từ năm 2019.

Để có quyền truy cập bao đầu vào máy mục tiêu, đối tượng tấn công đã khai thác lỗ hổng SharePoint (CVE-2019-0604). Sau đó, nhóm này thu thập thông tin xác thực và rà quét nội bộ để phát hiện các hệ thống quan trọng trong mạng của mục tiêu.

Mỗi giai đoạn của các cuộc tấn công đều thực hiện xóa dấu vết khỏi các máy bị nhiễm nhằm tránh việc bị phát hiện. Để thực hiện cuộc tấn công, nhóm này cũng đã sử dụng các công cụ tấn công như cửa hậu FOCUSFJORD, bộ cấy ghép tùy chỉnh HyperBro, webshel SeASHAARPEE.

Một số chuyên gia cho rằng các hoạt động gián điệp mạng của Trung Quốc ở Trung Đông và Trung Á có thể là các bước để bảo vệ các khoản đầu tư khổng lồ của Trung Quốc vào sáng kiến Vành đai và Con đường (BRI) ở các khu vực đó. Và khi dự án tiến triển, các nhóm gián điệp như UNC215 dự kiến sẽ tiếp tục các cuộc tấn công nhằm vào các cơ sở hạ tầng quan trọng ở Israel và Trung Đông.

*Nguồn:* https://cyware.com/news/unc215-impersonated-an-iranian-group-to-target-israeli-organizations-2b079a24

# 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 639 lỗ hổng, trong đó có 24 lỗ hổng mức cao, 61 lỗ hổng mức trung bình, 24 lỗ hổng mức thấp và 530 lỗ hổng chưa đánh giá. Trong đó có ít nhất 49 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 44 lỗ hổng trong sản phẩm của Microsoft, Nhóm 28 lỗ hổng trong sản phẩm của Netgear, Nhóm 22 lỗ hổng trong Linux kernel, Nhóm 16 lỗ hổng trong các Wordpress Plugin, Nhóm 15 lỗ hổng trong các sản phẩm Intel, Nhóm 12 lỗ hổng trong các extension cho Typo3, Nhóm 11 lỗ hổng trong các sản phẩm của Dell. 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:***

*- Microsoft: CVE-2021-26428, CVE-2021-36943,...*

*- Netgear: CVE-2021-38537, CVE-2021-38530,...*

*- Linux: CVE-2021-38160, CVE-2021-38202,...*

*- Wordpress: CVE-2021-34660, CVE-2021-24520,...*

*- Intel: CVE-2021-0008, CVE-2021-0009,...*

*- Typo3: CVE-2021-36790, CVE-2021-36787,...*

*- Dell: CVE-2021-21564, CVE-2021-21585,...*

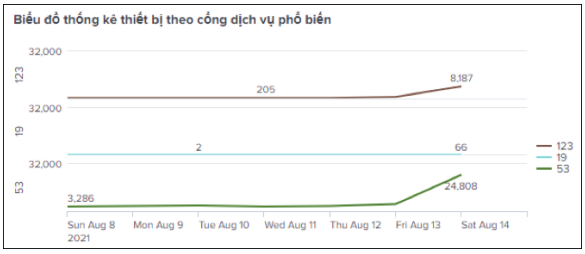
# Thông tin điểm yếu, lỗ hổng

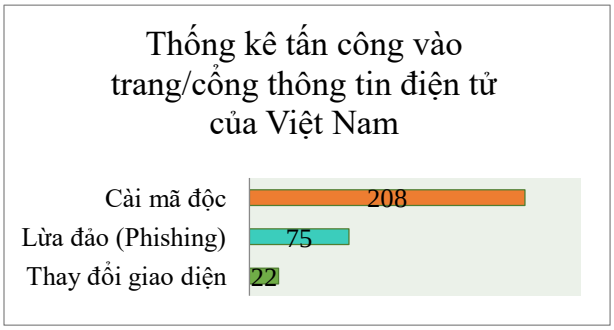
| TT | Sản phẩm/ dịch vụ | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|---|
| **1** | Microsoft | CVE-2021-26428<br>CVE-2021-36943<br>CVE-2021-36949<br>… | Nhóm 44 lỗ hổng trong sản phẩm của Microsoft (Azure, Windows,…) cho phép đối tượng tấn công thu thập thông tin, thực thi mã từ xa, leo thang đặc quyền, tấn công từ chối dịch vụ, tấn công giả mạo LSA. | Đã có thông tin xác nhận và bản vá |
| **2** | Netgear | CVE-2021-38537<br>CVE-2021-38530<br>CVE-2021-38515<br>… | Nhóm 28 lỗ hổng trong sản phẩm của Netgear (RBK40, RBK20,…) cho phép đối tượng tấn công thực hiện tấn công giả mạo XSS, command injection, tấn công từ chối dịch vụ. | Đã có thông tin xác nhận và bản vá |
| **3** | Linux | CVE-2021-38160<br>CVE-2021-38202<br>CVE-2021-38166<br>… | Nhóm 22 lỗ hổng trong Linux kernel cho phép đối tượng tấn công truy cập trái phép, tấn công từ chối dịch vụ, leo thang quyền. | Đã có thông tin xác nhận và bản vá |
| **4** | Wordpress | CVE-2021-34660<br>CVE-2021-24520<br>CVE-2021-24304<br>… | Nhóm 16 lỗ hổng trong các Wordpress Plugin (WP Fusion Lite WordPress plugin,…) cho phép đối tượng tấn công truy cập trái phép, thực thi mã tùy ý, tấn công giả mạo XSS, SSRF, SQL injection. | Đã có thông tin xác nhận và bản vá |
| **5** | Intel | CVE-2021-0008<br>CVE-2021-0009<br>CVE-2021-0005<br>… | Nhóm 15 lỗ hổng trong các sản phẩm Intel (Intel(R) Ethernet Adapters 800 Series Controllers,…) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ, leo thang đặc quyền. | Đã có thông tin xác nhận và bản vá |
| **6** | Typo3 | CVE-2021-36790<br>CVE-2021-36787<br>CVE-2021-36791<br>… | Nhóm 12 lỗ hổng trong các extension cho Typo3 (Yoast SEO, Miniorange Saml,…) cho phép đối tượng tấn công thu thập thông tin, tấn công giả mạo XSS, tấn công từ chối dịch vụ, tấn công SQL injection. | Đã có thông tin xác nhận và bản vá |
| **7** | Dell | CVE-2021-21564<br>CVE-2021-21585<br>CVE-2021-21584<br>… | Nhóm 11 lỗ hổng trong các sản phẩm của Dell (OpenManage Enterprise,…) cho phép đối tượng tấn công truy cập trái phép, thực thi mã tùy ý, thu thập thông tin, leo thang 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 **57,762** (tăng so với tuần trước **55,224**) 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.



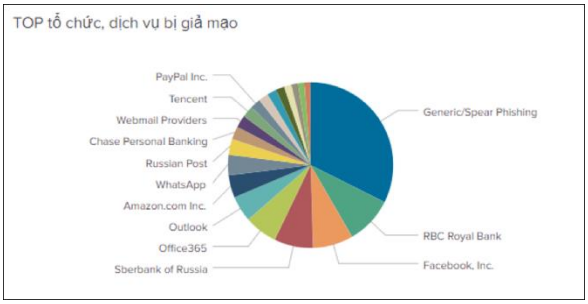




### *Tấn công Phishing*

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 có 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 319 trường hợp tấn công vào trang/cổng thông tin điện tử của Việt Nam: 23 trường hợp tấn công thay đổi giao diện, 82 trường hợp tấn công lừa đảo (Phishing), 214 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 36 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 như lừa đảo giả mạo website của ngân hàng, lừa đảo liên quan đến COVID…..

Dưới đây một số trường hợp điển hình người dùng cần nâng cao cảnh giác trong các trường hợp tương tự.

| STT | Website lừa đảo | Ghi chú |
|---|---|---|
| 1 | https://www.vay60s.com/ | Website lừa đảo kiếm tiền, vay tiền online. |
| 2 | https://shopee585.com/index/user/login.html<br>https://shopee88.vip/ope/ | Giả mạo website shopee lừa đảo nạp tiền vào để hoàn thành đơn hàng hưởng hoa hồng. |
| 3 | https://taikhoannhanqua.com/nhan-qua-tang-shopee-thang-08/ | Website lừa đảo không chính thống của shopee |
| 4 | http://207.148.115.161/ | Giả mạo trang báo Công An Nhân Dân. |
| 5 | https://lis666.sinh5.com/ | Giả mạo website của NYSE lừa đảo chiếm đoạt tài sản |

# 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