viettel security

BÁO CÁO

TÌNH HÌNH NGUY CƠ ATTT

TẠI VIỆT NAM 6 THÁNG ĐẦU NĂM 2025

MỤC LỤC

I. TỔNG QUAN

II. THỐNG KÊ & PHÂN TÍCH CHI TIẾT

Phần I.
TỔNG QUAN

1. Xu hướng

Trong 6 tháng đầu năm 2025, Viettel Threat Intelligence đã ghi nhận nhiều nguy cơ an toàn thông tin mới xuất hiện có ảnh hưởng tới các tổ chức, doanh nghiệp tại Việt Nam. Một số nguy cơ nổi bật như sau:

~8.5 triệu

Tài khoản bị đánh cắp tại Việt Nam

Số lượng tài khoản lộ lọt tại Việt Nam chiếm **1.7%** trong tổng số tài khoản bị đánh cắp trên thế giới (489 triệu tài khoản).

Việc lộ lọt tài khoản đăng nhập vào các hệ thống quan trọng và nhạy cảm như hệ thống Email, SSO, VPN,... dẫn tới nguy cơ hệ thống doanh nghiệp bị phá hoại hoặc đánh cắp thông tin.

>3 TB

Dữ liệu bị mã hóa

Các biến thể ransomware và RAT tinh vi hơn.

Các ngành bị tấn công nhiều nhất gồm: Sản xuất – Công nghiệp, Công nghệ, Y tế – Dược phẩm, Giáo dục – Edtech và Tài chính – Ngân hàng.

67 lỗ hổng

Có khả năng cao ảnh hưởng tới hệ thống của các doanh nghiệp, tổ chức tại Việt Nam.

Các nhóm tấn công vẫn tích cực sử dụng các lỗ hổng đã phát hiện từ thời gian trước để tiến hành rà quét, khai thác trên các sản phẩm phổ biến trong môi trường doanh nghiệp.

Nhóm lĩnh vực mục tiêu: Tài chính – Ngân hàng (hệ thống thanh toán, dịch vụ ngân hàng trực tuyến, ví điện tử), Sản xuất, Năng lượng.

4,532

Tên miền lừa đảo

1,067

Trang giả mạo

Tấn công lừa đảo dựa trên AI & deepfake: số lượng các cuộc tấn công phishing sẽ gia tăng nhiều hơn và được tự động hóa toàn diện bằng AI.

Các phương thức lừa đảo qua email, SMS, vishing và deepfake voice/video sẽ được cá nhân hóa dựa trên dữ liệu mạng xã hội, khiến các hệ thống bảo mật truyền thống và người dùng khó phát hiện, tăng nguy cơ bỏ qua các cơ chế bảo mật.

>528,000

Cuộc tấn công DDoS

▲ Tăng 3% so với H1.2024

Nhóm lĩnh vực mục tiêu: Tài chính – Ngân hàng, Công nghệ, Giáo dục - Edtech, Dịch vụ giải trí số, Dịch vụ công.

Các cuộc tấn công đang có xu hướng được **điều chỉnh linh hoạt về thời gian và tần suất**, nhằm né tránh các cơ chế phòng thủ theo ngưỡng, cho thấy sự chuyển hướng từ "tấn công số lượng" kết hợp "tấn công chất lượng".

191

Vụ rao bán dữ liệu tại Việt Nam với:

- **Gần 3 tỷ** bản ghi
- **482GB** dữ liệu

▲ Tăng 3 lần so với H1.2024 về số lượng vụ lộ lọt

Sự bùng nổ của việc rao bán thông tin người dùng, dữ liệu hệ thống cùng nhiều dữ liệu nhạy cảm của các doanh nghiệp lớn gây ảnh hưởng trực tiếp đến thương hiệu, uy tín của tổ chức.

2. Dự báo

Trong 6 tháng cuối năm 2025, các mối đe dọa an toàn thông tin được dự báo sẽ tiếp tục gia tăng với các xu hướng chính sau:

AI và Deepfake sẽ thúc đẩy làn sóng tấn công mạng mới trong thời gian tới

Trong thời gian tới, các công cụ AI và công nghệ deepfake được dự báo sẽ trở thành yếu tố then chốt thúc đẩy làn sóng tấn công mạng tinh vi hơn, đặc biệt là trong hai lĩnh vực: tấn công lừa đảo (phishing) và tấn công mã độc. Số lượng các cuộc **tấn công phishing** sẽ gia tăng nhiều hơn và được tự động hóa toàn diện bằng các công cụ AI. Các phương thức lừa đảo qua email, SMS, vishing và deepfake voice/video sẽ được cá nhân hóa dựa trên dữ liệu mạng xã hội, khiến các hệ thống bảo mật truyền thống và người dùng khó phát hiện, tăng nguy cơ bỏ qua các cơ chế bảo mật.

Song song đó, các nhóm tấn công cũng tận dụng công cụ AI để tạo ra **mã độc thế hệ mới** với khả năng khó bị phát hiện hơn. Với sự trợ giúp của AI, mã độc có thể được thiết kế để **thích ứng linh hoạt, tự động thay đổi hành vi nhằm né tránh các công cụ phòng vệ** như antivirus, EDR hoặc sandbox. Điều này dẫn đến nguy cơ bùng phát các chiến dịch phát tán mã độc trên diện rộng trong thời gian tới, đặc biệt khi chi phí tạo và triển khai mã độc ngày càng thấp nhờ các công cụ AI.

Sự gia tăng của các vụ lộ lọt dữ liệu

Số lượng các vụ lộ lọt tiếp tục tăng lên. Đặc biệt, các vụ lộ lọt từ đối tác bên thứ ba do cấu hình sai hoặc bị đánh cắp dữ liệu đăng nhập ngày càng xuất hiện nhiều hơn.

IoT và Blockchain trở thành mục tiêu mới

Với sự gia tăng của các thiết bị IoT và hệ sinh thái Blockchain, tin tặc sẽ tập trung vào các thiết bị bảo mật kém và các nền tảng giao dịch tiền mã hóa, dẫn đến rủi ro lớn về tài chính và dữ liệu.

Ransomware dưới dạng dịch vụ (RaaS)

Ransomware sẽ tiếp tục phát triển, trở thành một dịch vụ phổ biến, cho phép những người không có kỹ năng kỹ thuật cũng có thể triển khai tấn công, đồng thời kết hợp các kỹ thuật mã hóa phức tạp hơn.

Tấn công không cần file (Fileless Malware)

Các cuộc tấn công sử dụng mã độc chạy trực tiếp trên bộ nhớ RAM hoặc các công cụ tích hợp sẵn như PowerShell sẽ gia tăng, khiến việc phát hiện và xử lý trở nên khó khăn hơn.

3. Khuyến nghị

Để đảm bảo các hoạt động sản xuất kinh doanh của doanh nghiệp, tổ chức được diễn ra liên tục, giảm thiểu rủi ro của nguy cơ ATTT, Viettel Threat Intelligence có một số khuyến nghị sau:

Theo dõi và giám sát liên tục các nguy cơ ATTT

- Triển khai các hoạt động giám sát & phản ứng ATTT liên tục 24/7 để phát hiện và phản ứng sớm với các cuộc tấn công vào hệ thống trước khi xảy ra các thiệt hại nặng nề.
- Triển khai các giải pháp Threat Intelligence để nhận biết và phản ứng sớm với các chiến dịch tấn công xâm nhập, tấn công mã hoá dữ liệu đang xảy ra trên môi trường mạng.
- Chủ động rà soát dấu hiệu nhận biết xâm nhập trên hệ thống, phát hiện và phản ứng sớm với các nhóm tấn công có chủ đích.
- Hợp tác, chia sẻ với các đơn vị bên ngoài: Thiết lập hợp tác với các nhà cung cấp dịch vụ an ninh mạng để nhận các thông tin nguy cơ và nhận hỗ trợ khi cần.

Quản lý các nguy cơ từ chuỗi cung ứng, đối tác bên thứ ba

- Đảm bảo đối tác và nhà cung cấp của công ty tuân thủ các tiêu chuẩn an ninh mạng.
- Đưa ra các yêu cầu bảo mật trong hợp đồng với đối tác, nhà cung cấp.

Liên tục nâng cấp, cải tiến các hệ thống công nghệ thông tin

- Rà soát, nâng cấp phiên bản các phần mềm, ứng dụng thường xuyên: Đảm bảo các hệ thống, ứng dụng được vá các lỗ hổng bảo mật kịp thời.
- Định kỳ rà soát, đánh giá An toàn thông tin toàn diện cho hạ tầng công nghệ thông tin của tổ chức.
- Sao lưu định kỳ dữ liệu: Thực hiện sao lưu dữ liệu định kỳ: Mã nguồn, hệ thống khách hàng, dữ liệu sản phẩm/dịch vụ ảnh hưởng đến hoạt động kinh doanh của tổ chức.
- Đầu tư các giải pháp bảo mật tiên tiến: External Attack Surface Management, zero trust access, các giải pháp quản trị an toàn (PAM/PIM).

Xây dựng văn hóa an toàn thông tin

- Đào tạo nhận thức: Tổ chức đào tạo, kiểm tra định kỳ cho nhân viên về các rủi ro, mối đe dọa về nguy cơ mất ATTT.
- Kiểm soát truy cập: Thiết lập các chính sách quản lý, kiểm soát truy cập với nguyên tắc quyền tối thiểu.

Phần II.

THỐNG KÊ & PHÂN TÍCH CHI TIẾT

1. Các dòng mã độc

Trong 6 tháng đầu năm 2025, hoạt động mã độc ghi nhận xu hướng gia tăng rõ rệt với nhiều chiến dịch tấn công có **mức độ tinh vi cao**, đặc biệt là các biến thể mã độc mã hóa tống tiền (ransomware) và RAT (Remote Access Trojan). Các mã độc này nhắm mục tiêu vào các doanh nghiệp, tổ chức tại nhiều khu vực, trong đó có Việt Nam.

Với sự hỗ trợ của các công cụ AI, tin tặc có thể tự động hóa quá trình phát triển mã độc, giúp rút ngắn thời gian và giảm chi phí tạo mới. Nhờ đó, số lượng mã độc mới được tạo ra được dự báo sẽ tiếp tục gia tăng mạnh trong thời gian tới. Trong 6 tháng đầu năm 2025, các ngành bị tấn công nhiều nhất bởi các dòng mã độc bao gồm: **Sản xuất - Công nghiệp, Công nghệ, Y tế - Dược phẩm, Giáo dục - Edtech và Tài chính - Ngân hàng**.

Mã độc mã hóa tống tiền (ransomware)

Tình hình ransomware tại Việt Nam trong nửa đầu năm 2025 tiếp tục diễn biến phức tạp với nhiều vụ tấn công **quy mô lớn**, **đa dạng mục tiêu** và **thiệt hại đáng kể**. Trong 6 tháng đầu năm 2025, các doanh nghiệp, tổ chức tại Việt Nam tiếp tục là mục tiêu tấn công của nhiều nhóm ransomware lớn trên thế giới. Đáng chú ý, có ít nhất 10 vụ tấn công ransomware lớn được ghi nhận, do các nhóm như Hunters, Ransomhub, Fog Ransomware,… thực hiện. Tổng lượng dữ liệu bị đánh cắp và rò rỉ công khai được ước tính lên đến **hơn 3 terabyte**. Các lĩnh vực bị ảnh hưởng bao gồm: **Sản xuất - Công nghiệp, Công nghệ, Y tế, Năng lượng, Dịch vụ công, Xây dựng, Dịch vụ**.

Bảng 1. Các vụ tấn công Ransomware nổi bật trong 6 tháng đầu năm 2025 được ghi nhận bởi Viettel Threat Intelligence

STT	Lĩnh vực	Nhóm tấn công	Số vụ	Thời gian tấn công
1	Y tế, Dịch vụ công, Sản xuất	Funksec	2	Tháng 01/2025
2	Năng lượng	Hunters	1	Tháng 01/2025
3	Sản xuất	RansomHub	1	Tháng 01/2025
4	Công nghệ	Fog ransomware	1	Tháng 02/2025
5	Công nghệ	Bianlian	1	Tháng 03/2025
6	Công nghệ	Crypto24	1	Tháng 04/2025
7	Xây dựng	J	1	Tháng 05/2025
8	Công nghiệp	Devman	1	Tháng 05/2025
9	Dịch vụ	Flocker	1	Tháng 06/2025

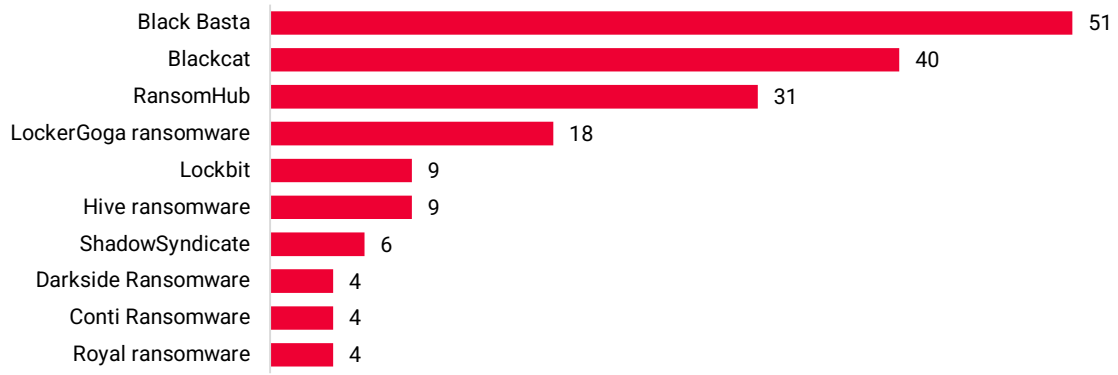
**Nguồn: Viettel Threat Intelligence*

*Thông tin phân tích chi tiết về các nguy cơ tấn công Ransomware được chia sẻ **độc quyền** trong các báo cáo chuyên sâu của Viettel Threat Intelligence tại https://platform.cyberintel.io/#/.*

1. Các dòng mã độc

Dưới đây là danh sách các Ransomware có nhiều kết nối tới trong 6 tháng đầu năm 2025:

Hình 1. Các Ransomware có số lượng IP kết nối đến nhiều nhất trong 6 tháng đầu năm 2025



Nguồn: Viettel Threat Intelligence

Dưới đây là danh sách các nhóm Ransomware hoạt động mạnh trong 6 tháng đầu năm 2025 theo Viettel Threat Intelligence ghi nhận:

Bảng 2. Các nhóm Ransomware hoạt động mạnh trong 6 tháng đầu năm 2025 theo Viettel Threat Intelligence ghi nhận

STT	Tên nhóm	Mô tả	Đối tượng ảnh hưởng
1	Funksec	Nhóm xuất hiện và hoạt động mạnh vào cuối năm 2024. Mục tiêu của FunkSec không chỉ là mã hóa dữ liệu mà còn đánh cắp và bán dữ liệu bị rò rỉ trên các thị trường chợ đen.	Doanh nghiệp và tổ chức
2	Lockbit	Nhóm hoạt động theo mô hình Ransomware-as-a Service (RaaS). Phiên bản mới Lockbit 4.0 với nhiều cải tiến về tốc độ mã hóa, khả năng lây lan và khả năng tùy biến cho nhiều đối tượng sử dụng.	Doanh nghiệp và tổ chức
3	Frog	Xuất hiện lần đầu tiên vào đầu tháng 5 năm 2024 và được phát hiện đang tích cực sử dụng thông tin đăng nhập mạng riêng ảo (VPN) bị xâm phạm để truy cập vào mạng của các tổ chức trong lĩnh vực Giáo dục.	Lĩnh vực Giáo dục
4	Lynx	Hoạt động theo mô hình Ransomware-as-a-Service (RaaS), Lynx sử dụng các chiến thuật tinh vi như tống tiền kép và mã hóa nâng cao.	Lĩnh vực Công nghiệp
5	Medusa	Hoạt động theo mô hình Ransomware-as-a Service (RaaS). Gần đây, BabyLockerKZ, một biến thể của mã độc MedusaLocker đã hoạt động mạnh và tấn công nhiều khu vực trên thế giới.	Người dùng Windows
6	Ransom Hub	Hoạt động theo mô hình Ransomware-as-a Service (RaaS). Nhóm thường nhắm vào các tổ chức lớn có khả năng trả tiền chuộc cao.	Doanh nghiệp và tổ chức

Nguồn: Viettel Threat Intelligence

1. Các dòng mã độc

Mã độc RAT (Remote Access Trojan)

Trong 6 tháng đầu năm 2025, mã độc RAT (Remote Access Trojan) là một mối đe dọa đáng lo ngại, với sự kết hợp nhiều RAT với nhau, đặc biệt khi các RAT ngày càng sử dụng AI và các kỹ thuật tiên tiến để tăng hiệu quả tấn công.

Mã độc RAT thường sử dụng các chiến thuật tinh vi để tránh phát hiện, bao gồm mã hóa lưu lượng C2, sử dụng các tiến trình hợp pháp, và tận dụng các lỗ hổng trong hệ thống chưa được vá. Sự gia tăng số lượng RAT mới và sự cải tiến thích nghi của các RAT cũ khiến cho tình hình mã độc trở nên phức tạp và khó dự đoán. Ngoài ra, với sự phát triển của AI agentic có thể làm tăng khả năng tự động hóa của RAT, cho phép chúng lập kế hoạch và thực hiện tấn công mà không cần sự can thiệp trực tiếp, điều này có thể dẫn đến sự gia tăng đáng kể trong số lượng và mức độ nghiêm trọng của các cuộc tấn công.

Bảng 3. Danh sách các mã độc RAT được Viettel Threat Intelligence phát hiện và đánh giá có ảnh hưởng lớn trong 6 tháng đầu năm 2025

STT	Tên mã độc	Mô tả
1	StilachiRAT	Mã độc mới được phát hiện với khả năng đánh cắp ví tiền điện tử, thông tin hệ thống.
2	Hiatus RAT	HiatusRAT nhắm mục tiêu vào các thiết bị Internet vạn vật (IoT) cho phép truy cập và điều khiển từ xa. Các mục tiêu bao gồm camera thông minh và hộp DVR.
3	WmRAT/Miya RAT	Mã độc RAT được nhóm APT Bitter sử dụng nhắm vào lĩnh vực dịch vụ công.
4	Remcos RAT	Mã độc với nhiều chức năng kiểm soát thiết bị. Gần đây mã độc sử dụng phương pháp lây lan mới, tấn công qua email và tệp đính kèm.
5	NetSupport RAT	Mã độc phát tán qua trang CAPTCHA giả mạo, có khả năng kiểm soát hệ thống từ xa.

**Nguồn: Viettel Threat Intelligence*

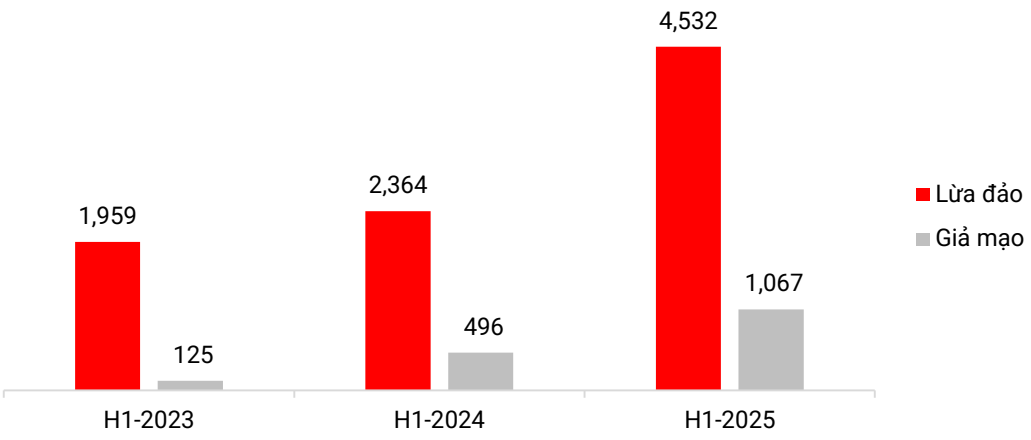
*Thông tin phân tích chi tiết về các nguy cơ tấn công RAT được chia sẻ **độc quyền** trong các báo cáo chuyên sâu của Viettel Threat Intelligence tại https://platform.cyberintel.io/#/.*

2. Lừa đảo, gian lận tài chính

*Các số liệu, biểu đồ trong mục **Lừa đảo, gian lận tài chính** được tổng hợp từ dữ liệu độc quyền của Viettel Threat Intelligence.*

Thống kê số lượng tên miền lừa đảo, giả mạo

Hình 2: Biểu đồ thống kê số lượng tên miền lừa đảo, giả mạo trong cùng kỳ các năm



**Nguồn: Viettel Threat Intelligence*

Theo thống kê của Viettel Threat Intelligence, trong 6 tháng đầu năm 2025 đã ghi nhận **4,532** tên miền lừa đảo nhắm vào người dùng, khách hàng của các tổ chức lớn tại Việt Nam. Số lượng tên miền lừa đảo **tăng hơn 90%** so với cùng kỳ năm 2024. Các hình thức lừa đảo diễn ra ngày càng phức tạp và tinh vi, liên tục mở rộng sang các nhóm mục tiêu mới: từ việc nhắm trực tiếp đến các khách hàng sử dụng dịch vụ của các tổ chức **Tài chính - Ngân hàng** sang các người dùng trong lĩnh vực **Dịch vụ công** thông qua hình thức giả mạo các cơ quan chức năng, kèm theo đó là sự gia tăng các vụ lừa đảo liên quan đến người dùng nhóm ngành **Bán lẻ - Thương mại điện tử**, **Năng lượng** và **Vận Tải**.

Ngoài ra, Viettel Threat Intelligence cũng đã phát hiện và cảnh báo **1,067** trang giả mạo, sử dụng trái phép thương hiệu của các tổ chức, doanh nghiệp tại Việt Nam, **tăng 115%** so với cùng kỳ 6 tháng đầu năm 2024.

Sự gia tăng liên tục số lượng tên miền lừa đảo, giả mạo nhắm vào người dùng, khách hàng của các tổ chức cũng như sử dụng trái phép các thương hiệu của các doanh nghiệp tại Việt Nam đặt ra những vấn đề cấp bách và thiết yếu liên quan đến công tác bảo vệ thương hiệu. Trước thực trạng đó, các doanh nghiệp cần chủ động triển khai các biện pháp giám sát, phát hiện và xử lý kịp thời các hành vi xâm phạm thương hiệu, lừa đảo người dùng, đồng thời nâng cao nhận thức để bảo vệ khách hàng cũng như hình ảnh và uy tín của doanh nghiệp trên không gian mạng.

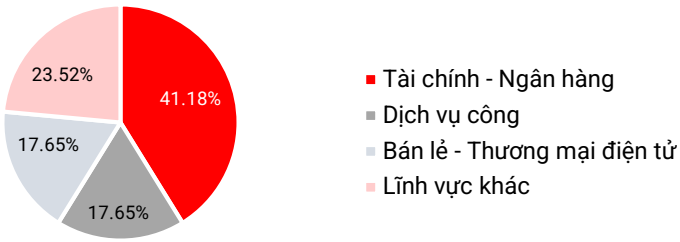
Một số hình thức lừa đảo phổ biến được các nhóm tội phạm mạng sử dụng trong các chiến dịch tấn công bao gồm:

- Lừa đảo, giả mạo các dịch vụ liên quan đến thẻ tín dụng.
- Giả mạo cơ quan chức năng để cài đặt ứng dụng Android độc hại trên các thiết bị di động.
- Lừa đảo hỗ trợ thu hồi vốn, thu hồi tiền bị treo.
- Giả mạo nhân viên giao hàng.
- Giả mạo nhân viên điện lực.
- Giả mạo tổ chức, cơ quan để lừa đảo thông qua tin tuyển dụng.

2. Lừa đảo, gian lận tài chính

Tấn công lừa đảo, giả mạo theo ngành

Hình 3: Tỉ lệ tấn công lừa đảo, giả mạo theo ngành



Nguồn: Viettel Threat Intelligence

Về phân bố theo nhóm ngành, ngành **Tài chính - Ngân hàng** vẫn là nhóm đứng đầu về các cuộc tấn công lừa đảo, giả mạo, chiếm tới 41.18% tổng số các cuộc tấn công.

Bảng 4. Các chiến dịch tấn công lừa đảo, giả mạo tiêu biểu được Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2025

Chiến dịch	Mô tả	Ảnh hưởng
Lừa đảo, giả mạo ứng dụng chứng khoán	Tin tặc mạo danh chuyên gia chứng khoán, mời nạn nhân tham gia nhóm đầu tư trên Telegram, Zalo và hướng dẫn cài đặt ứng dụng giả mạo. Sau đó tạo giao dịch ảo, hiển thị lợi nhuận cao bất thường để dụ nạn nhân nạp tiền và chiếm đoạt toàn bộ số tiền của nạn nhân.	Người dùng các tổ chức chứng khoán tại Việt Nam
Lừa đảo đặt tour, khách sạn giá rẻ qua mạng	Tin tặc mạo danh nhân viên công ty du lịch, tạo fanpage hoặc website giả mạo với giao diện bắt mắt, sau đó đăng quảng cáo tour, phòng khách sạn giá rẻ để thu hút nạn nhân. Khi nạn nhân liên hệ đặt cọc dịch vụ và chuyển tiền, tin tặc viện cớ sai sót trong giao dịch, yêu cầu chuyển thêm tiền để xác nhận đặt phòng, rồi chiếm đoạt toàn bộ số tiền và cắt đứt liên lạc.	Người dân Việt Nam
Lừa đảo, giả mạo nhân viên giao hàng	Tin tặc nhắn tin hoặc gọi điện báo giao hàng với những thông tin chính xác về họ tên, địa chỉ, mặt hàng, số tiền, đánh vào sự chủ quan của người mua sắm, từ đó chiếm đoạt tiền hàng.	Người dân Việt Nam
Mạo danh chương trình quyên góp tình nguyện của một số cơ quan chức năng, tổ chức, doanh nghiệp	Tin tặc mạo danh, lợi dụng danh nghĩa của một số cơ quan chức năng, doanh nghiệp, tổ chức uy tín để huy động sự ủng hộ từ các tổ chức, cá nhân trong và ngoài nước trên các nền tảng mạng xã hội.	Người dân, cơ quan, tổ chức, doanh nghiệp tham gia thiện nguyện tại Việt Nam
Lừa đảo giả mạo Công ty Điện lực	Tin tặc tự xưng là nhân viên Công ty Điện lực đề nghị số hóa hồ sơ điện để phục vụ thu tiền điện hàng tháng. Sau đó hướng dẫn người dùng cài đặt ứng dụng độc hại và đăng nhập tài khoản ngân hàng. Sau khi thực hiện thao tác, số tiền trong tài khoản ngân hàng sẽ lập tức bị mất.	Người dùng của các Công ty Điện lực
Mạo danh, lừa đảo khoá học kỹ năng mùa hè	Trong thời điểm các em học sinh nghỉ hè, các khoá kỹ năng được nhiều phụ huynh lựa chọn và đặt niềm tin. Lợi dụng nhu cầu này các đối tượng lừa đảo tạo fanpage giả để chiếm đoạt tiền.	Phụ huynh, học sinh tại Việt Nam
Giả mạo tuyển dụng của các cơ quan, doanh nghiệp tại Việt Nam	Tin tặc giả mạo trang tuyển dụng các cơ quan, doanh nghiệp tại Việt Nam tạo tên miền giả mạo dẫn đến trang Google Sheets. Từ đó lấy thông tin cá nhân của nạn nhân, và dùng các kịch bản tấn công khác nhau như cài app độc hại và đóng các loại phí để chiếm đoạt tài sản.	Người lao động tại Việt Nam

Nguồn: Viettel Threat Intelligence

2. Lừa đảo, gian lận tài chính

Bảng 4 (tiếp). Các chiến dịch tấn công lừa đảo, giả mạo tiêu biểu được Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2025

Chiến dịch	Mô tả	Ảnh hưởng
Giả mạo các sàn giao dịch chứng khoán tại Việt Nam	Tin tặc tạo ra các trang giả mạo giao diện các sàn giao dịch chứng khoán tại Việt Nam. Lợi dụng việc người dùng chủ quan đăng nhập vào các trang giả mạo này dẫn đến mất tài khoản.	Các tổ chức chứng khoán tại Việt Nam
Mạo danh nhân viên của nhà mạng	Tin tặc giả mạo nhân viên chăm sóc khách hàng của nhà mạng, gọi điện tư vấn ưu đãi hấp dẫn như gia hạn gói cước, tăng dung lượng Internet hoặc thời gian gọi. Sau khi lấy được lòng tin, chúng hướng dẫn nạn nhân truy cập ứng dụng của nhà mạng và cung cấp mã OTP để "hoàn tất thao tác". Sau đó, chiếm quyền kiểm soát tài khoản, chuyển tiền về tài khoản của tin tặc.	Người dùng cá nhân
Mạo danh nhân viên tại các hệ thống cửa hàng bán lẻ	Tin tặc gửi tin nhắn qua các nền tảng mạng xã hội, các nhóm thông báo trúng thưởng các phần quà giá trị như điện thoại, tivi, phiếu mua hàng để chiếm đoạt tài sản.	Người dùng cá nhân
Lừa đảo, giả mạo có liên quan tới thương hiệu của các tổ chức ngân hàng tại Việt Nam	Giả mạo dịch vụ ví điện tử: Yêu cầu nạn nhân truy cập các trang "ví điện tử" của ngân hàng để kiểm tra các khoản tiền giao dịch. Hướng dẫn nhập thông tin và mã OTP để chiếm đoạt tài sản của nạn nhân.	Người dùng của tất cả các ngân hàng tại Việt Nam
Lừa đảo thông qua hình thức vay tiền trực tuyến	Mạo danh nhân viên của ngân hàng, công ty tài chính để gọi điện, mời chào vay tiền trực tuyến. Chiếm đoạt các khoản tiền "phí" (phí bảo hiểm, phí khắc phục lỗi, phí thay đổi thông tin,...).	Người dùng các tổ chức tài chính vay tiêu dùng, các ngân hàng tại Việt Nam
Lừa đảo liên quan đến dịch vụ thẻ tín dụng của các tổ chức tài chính, ngân hàng tại Việt Nam	Lợi dụng nhu cầu sử dụng thẻ tín dụng ngày càng tăng, các đối tượng giả mạo nhân viên mời chào các dịch vụ nâng hạn mức, sang ngang thẻ, mở thẻ tín dụng,... nhằm thực hiện các hành vi lừa đảo, gian lận, chiếm đoạt tài sản của nạn nhân.	Người dùng của tất cả các ngân hàng tại Việt Nam
Giả mạo cơ quan chức năng để lừa người dùng cài đặt ứng dụng Android độc hại	Tin tặc mạo danh cán bộ cơ quan chức năng tại Việt Nam để hướng dẫn người dùng cài đặt ứng dụng độc hại trên điện thoại, sau đó chiếm quyền điều khiển điện thoại của nạn nhân, và thực hiện các hành vi chiếm đoạt tài sản.	Người dùng tại Việt Nam
Giả danh nhân viên điện lực	Cuộc gọi thông báo cắt điện do nợ tiền hoặc lỗi hệ thống, yêu cầu chuyển tiền ngay lập tức để tránh bị cắt, từ đó thực hiện các hành vi lừa đảo chiếm đoạt tài sản.	Người dùng các ứng dụng nộp tiền điện tại Việt Nam
Mạo danh công chức thuế	Tin tặc giả danh nhân viên thuế gọi điện thông báo nợ thuế hoặc yêu cầu cập nhật thông tin qua đường link giả mạo, nhằm đánh cắp dữ liệu cá nhân.	Người nộp thuế
Lừa đảo thông qua các chương trình khuyến mãi Tết	Lợi dụng thời điểm nhu cầu mua sắm và đi lại tăng cao, tin tặc sử dụng hình thức gọi điện mời mua vé xe, vé máy bay giá rẻ hoặc tham gia chương trình khuyến mãi Tết, yêu cầu chuyển khoản trước; từ đó thực hiện các hành vi chiếm đoạt tài sản.	Người dân Việt Nam
Giả mạo nhân viên ngân hàng	Tin tặc thu thập thông tin cá nhân và tài khoản ngân hàng của người dùng thông qua chợ đen giao dịch dữ liệu hoặc lộ lọt trên mạng xã hội. Tin tặc giả mạo nhân viên ngân hàng hỏi về giao dịch bất thường, hướng dẫn người dùng cài đặt ứng dụng độc hại hoặc quét QR chứa đường dẫn độc hại.	Người dùng của tất cả các ngân hàng tại Việt Nam

Nguồn: Viettel Threat Intelligence

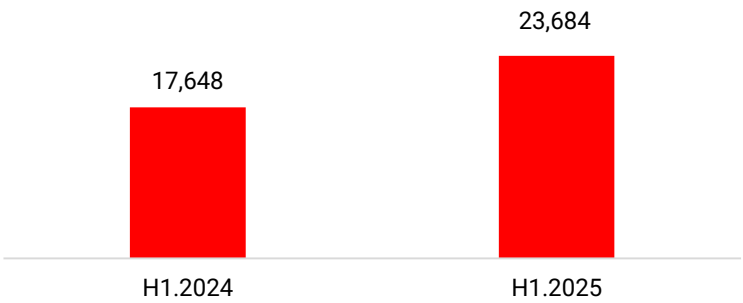
3. Tình hình lỗ hổng bảo mật

Viettel Threat Intelligence đã cảnh báo chi tiết về **67** lỗ hổng bảo mật trong các sản phẩm, phần mềm phổ biến được công bố trong 6 tháng đầu năm 2025 có nguy cơ ảnh hưởng đến các doanh nghiệp, tổ chức tại Việt Nam.

Bên cạnh đó, các nhóm tấn công vẫn tích cực sử dụng các lỗ hổng đã phát hiện từ thời gian trước để tiến hành rà quét, khai thác trên các sản phẩm phổ biến trong môi trường doanh nghiệp như: **CVE-2023-21931 và CVE-2023-21839** (Lỗ hổng thực thi mã tùy ý trên Oracle WebLogic Server), **CVE-2022-39952** (Lỗ hổng thực thi mã từ xa trên FortiNAC), **CVE-2021-44228** (Lỗ hổng thực thi mã từ xa trên Apache Log4j), **CVE-2021-41379** (Lỗ hổng leo thang đặc quyền trên Microsoft Windows), **CVE-2023-22515** (Lỗ hổng truy cập trái phép trên Confluence Data Center and Server), **CVE-2020-10148** (Lỗ hổng thực thi mã tùy ý trên SolarWinds Orion Platform),... Mã khai thác của các lỗ hổng này đều đã được công khai từ lâu trên không gian mạng khiến việc khai thác trở nên dễ dàng.

Các lỗ hổng mới xuất hiện trong 6 tháng đầu năm 2025

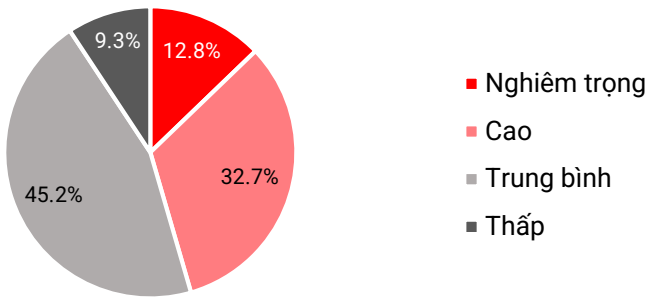
Hình 4: Số lượng lỗ hổng mới xuất hiện trong 6 tháng đầu năm 2024 và 6 tháng đầu năm 2025



Nguồn: Viettel Threat Intelligence

Trong 6 tháng đầu năm 2025, số lượng lỗ hổng ghi nhận trên thế giới có xu hướng tăng hơn 34% so với cùng kỳ năm ngoái.

Hình 5: Tỉ lệ lỗ hổng trong 6 tháng đầu năm 2025 theo mức độ



Nguồn: Viettel Threat Intelligence

Các lỗ hổng mức **Cao và Trung Bình** (theo hệ thống chấm điểm lỗ hổng phổ biến – CVSS 3.0) chiếm tỉ trọng lớn nhất với lần lượt là 32.7% và 45.2%. Trong khi đó, số lượng lỗ hổng mức **Nghiêm trọng** mặc dù chỉ chiếm 12.8% nhưng các lỗ hổng này đa số đều được các nhóm tin tặc sử dụng trong các chiến dịch tấn công thực tế, gây ảnh hưởng lớn tới các tổ chức.

3. Tình hình lỗ hổng bảo mật

Qua quá trình đánh giá và phân tích các lỗ hổng, Viettel Threat Intelligence đã đưa ra **67 cảnh báo liên quan đến lỗ hổng** có ảnh hưởng lớn tới các tổ chức, doanh nghiệp tại Việt Nam, cụ thể như sau:

Bảng 5. Thống kê số lượng lỗ hổng có nguy cơ ảnh hưởng lớn tới các tổ chức tại Việt Nam theo mức độ

Mức độ	Số lượng
Nghiêm trọng	3
Cao	21
Trung bình	42
Thấp	1

**Nguồn: Viettel Threat Intelligence*

Bảng 6. Danh sách các lỗ hổng nổi bật trong 6 tháng đầu năm 2025 được Viettel Threat Intelligence đánh giá là có ảnh hưởng lớn tới các tổ chức, doanh nghiệp tại Việt Nam

STT	CVE	Thông tin chung	Mức độ theo đánh giá của Viettel Threat Intelligence
1	CVE-2024-7097, CVE-2024-7096, CVE-2024-6914 và CVE-2024-7074	Nguy cơ khai thác các lỗ hổng trên các sản phẩm của WSO2: Khai thác lỗ hổng thành công, tin tặc không cần xác thực có thể tạo một tài khoản mới và dùng tài khoản này để reset password của tài khoản admin, dẫn đến nguy cơ chiếm quyền quản trị hệ thống. Viettel Threat Intelligence ghi nhận lỗ hổng này đã được khai thác trên thực tế.	Nghiêm trọng
2	CVE-2025-0282	Nguy cơ khai thác lỗ hổng cho phép thực thi mã từ xa trên Ivanti Connect Secure - giải pháp VPN được sử dụng phổ biến: Khai thác lỗ hổng thành công, tin tặc không cần xác thực có thể thực thi mã từ xa trên hệ thống mục tiêu. Viettel Threat Intelligence ghi nhận lỗ hổng này đã được khai thác trên thực tế.	Nghiêm trọng
3	CVE-2025-4427 và CVE-2025-4428	Nguy cơ khai thác các lỗ hổng CVE-2025-4427 và CVE-2025-4428 trên Ivanti Endpoint Manager Mobile (EPMM): Khai thác thành công cho phép tin tặc vượt qua cơ chế xác thực và thực thi mã từ xa trên hệ thống.	Nghiêm trọng
4	CVE-2024-55591	Nguy cơ khai thác lỗ hổng trên FortiOS và FortiProxy: Khai thác lỗ hổng thành công, tin tặc có thể vượt qua xác thực, lấy được quyền super admin và kiểm soát hệ thống mục tiêu. Viettel Threat Intelligence ghi nhận lỗ hổng này đã được khai thác trên thực tế.	Cao

3. Tình hình lỗ hổng bảo mật

Bảng 6 (tiếp). Danh sách các lỗ hổng nổi bật trong 6 tháng đầu năm 2025 được Viettel Threat Intelligence đánh giá là có ảnh hưởng lớn tới các tổ chức, doanh nghiệp tại Việt Nam

STT	Tên lỗ hổng	Thông tin chung	Mức độ đánh giá của Viettel Threat Intelligence
5	CVE-2024-49113 và CVE-2024-49112	Nguy cơ khai thác lỗ hổng trên hệ điều hành Microsoft Windows: Khai thác lỗ hổng thành công cho phép tin tặc gây ra tình trạng từ chối dịch vụ hoặc thực thi mã tùy ý trên máy chủ mà không cần xác thực.	Cao
6	CVE-2024-21182	Nguy cơ khai thác lỗ hổng Oracle WebLogic Server - máy chủ ứng dụng hàng đầu trên nền tảng Java: Khai thác lỗ hổng thành công, tin tặc không cần xác thực có thể thực thi mã tùy ý trên máy chủ thông qua giao thức T3, IIOP.	Cao
7	CVE-2024-50379	Nguy cơ khai thác lỗ hổng trên Apache Tomcat - một web server HTTP mã nguồn mở của Apache Software Foundation: Khai thác lỗ hổng này thành công, tin tặc có thể tải tệp lên hệ thống và thực thi mã từ xa.	Cao
8	CVE-2025-21298	Nguy cơ khai thác lỗ hổng CVE-2025-21298 trên Windows Object Linking and Embedding (OLE): Lỗ hổng tồn tại trong trình phân tích cú pháp RTF. Tin tặc có thể gửi các email đặc biệt tới máy chủ mục tiêu, người dùng mở email bằng Outlook hoặc hiển thị bản xem trước cho phép tin tặc thực thi mã từ xa.	Cao
9	CVE-2024-43639	Nguy cơ khai thác lỗ hổng CVE-2024-43639 trên Microsoft Windows Key Distribution Center (KDC) Proxy: Khai thác lỗ hổng thành công cho phép tin tặc thực thi mã tùy ý trong ngữ cảnh bảo mật của dịch vụ mục tiêu.	Cao
10	CVE-2025-24813	Nguy cơ khai thác lỗ hổng CVE-2025-24813 trên Apache Tomcat: Khai thác lỗ hổng thành công cho phép tin tặc thực thi mã từ xa, tiết lộ thông tin nhạy cảm hoặc làm hỏng dữ liệu của hệ thống.	Cao
11	ZDI-CAN-25373	Nguy cơ khai thác các lỗ hổng Zero-Day ZDI-CAN-25373 trên hệ điều hành Microsoft Windows: Khai thác lỗ hổng thành công cho phép tin tặc thực thi mã từ xa trên máy của nạn nhân. Để khai thác lỗ hổng, tin tặc cần đánh lừa người dùng tải và mở các tệp độc hại.	Cao

3. Tình hình lỗ hổng bảo mật

Bảng 6 (tiếp). Danh sách các lỗ hổng nổi bật trong 6 tháng đầu năm 2025 được Viettel Threat Intelligence đánh giá là có ảnh hưởng lớn tới các tổ chức, doanh nghiệp tại Việt Nam

STT	Tên lỗ hổng	Thông tin chung	Mức độ đánh giá của Viettel Threat Intelligence
12	CVE-2025-24071	Nguy cơ khai thác lỗ hổng CVE-2025-24071 trên hệ điều hành Windows khi giải nén tệp RAR/ZIP: Khai thác lỗ hổng thành công cho phép tin tặc thu thập mã băm NTLMv2 của người dùng.	Cao
13	CVE-2025-23120	Nguy cơ khai thác lỗ hổng CVE-2025-23120 trong phần mềm Veeam Backup & Replication: Khai thác lỗ hổng thành công cho phép tin tặc đã được xác thực thực thi mã từ xa với quyền SYSTEM trên máy chủ sao lưu.	Cao
14	CVE-2025-29824	Nguy cơ khai thác lỗ hổng CVE-2025-29824 trong Windows Common Log File System (CLFS): Tin tặc với đặc quyền thấp trên hệ thống có thể khai thác lỗ hổng này để leo thang đặc quyền lên NT AUTHORITY\SYSTEM. Lỗ hổng đã được sử dụng để khai thác trong thực tế.	Cao
15	CVE-2025-22457	Nguy cơ khai thác lỗ hổng thực thi mã từ xa trên Ivanti Connect Secure: Khai thác thành công, tin tặc không cần xác thực có thể khai thác lỗ hổng stack-based buffer overflow, từ đó thực thi mã từ xa trên hệ thống mục tiêu. Lỗ hổng đã được sử dụng trong các chiến dịch tấn công trong thực tế.	Cao
16	Lỗ hổng trên Telegram Windows	Nguy cơ khai thác lỗ hổng cho phép tin tặc đánh cắp thông tin liên quan đến địa chỉ IP public, NTLM Hash trên Telegram Windows: Khai thác yêu cầu người dùng mở tệp .m3u trên Telegram phiên bản trên Windows. Từ việc thu thập NTLM Hash, tin tặc có thể tấn công Pass-The-Hash, từ đó truy cập hệ thống Active Directory (AD) mục tiêu.	Cao
17	CVE-2025-2825	Nguy cơ khai thác lỗ hổng CVE-2025-2825 trên CrushFTP: Khai thác lỗ hổng thành công cho phép tin tặc vượt qua cơ chế xác thực và truy cập trái phép vào hệ thống. Lỗ hổng đã bị khai thác trong thực tế.	Cao
18	CVE-2025-1097, CVE-2025-1098, CVE-2025-24514 và CVE-2025-1974	Nguy cơ khai thác lỗ hổng CVE-2025-1097, CVE-2025-1098, CVE-2025-24514 và CVE-2025-1974 (được gọi chung là IngressNightmare) trên Ingress NGINX Controller của Kubernetes: Khai thác lỗ hổng thành công cho phép tin tặc thực thi mã từ xa mà không cần xác thực, truy cập secrets trong tất cả các namespace và tiềm ẩn khả năng chiếm quyền kiểm soát toàn bộ cluster.	Cao

3. Tình hình lỗ hổng bảo mật

Bảng 6 (tiếp). Danh sách các lỗ hổng nổi bật trong 6 tháng đầu năm 2025 được Viettel Threat Intelligence đánh giá là có ảnh hưởng lớn tới các tổ chức, doanh nghiệp tại Việt Nam

STT	Tên lỗ hổng	Thông tin chung	Mức độ đánh giá của Viettel Threat Intelligence
19	CVE-2025-26529	Nguy cơ khai thác lỗ hổng CVE-2025-26529 trong Moodle: Khai thác lỗ hổng thành công cho phép tin tặc thực hiện tấn công XSS (Cross-Site Scripting) được lưu trữ trong nhật ký quản trị, từ đó có thể chiếm quyền điều khiển tài khoản của quản trị viên.	Cao
20	CVE-2025-4525	Nguy cơ khai thác lỗ hổng CVE-2025-4525 trong ứng dụng Discord Windows Client: Tin tặc với đặc quyền thấp trên hệ thống có thể khai thác lỗ hổng và thực thi mã tùy ý trên hệ thống.	Cao
21	CVE-2025-27817	Nguy cơ khai thác lỗ hổng CVE-2025-27817 trên Apache Kafka Connect: Khai thác lỗ hổng thành công cho phép tin tặc đọc tùy ý các tệp tin trên máy chủ và thực hiện các cuộc tấn công SSRF (Server-Side Request Forgery) mà không cần xác thực.	Cao
22	CVE-2025-33053	Nguy cơ khai thác lỗ hổng thực thi mã từ xa trên Web Distributed Authoring and Versioning (WEBDAV) trên hệ điều hành Windows: Tin tặc lừa người dùng nhấp vào đường dẫn WebDAV độc hại thông qua email, tin nhắn,... Từ đó, tin tặc có thể thực thi mã từ xa trên hệ thống mục tiêu. Lỗ hổng đã được sử dụng trong các chiến dịch tấn công trong thực tế.	Cao
23	CVE-2025-20188	Nguy cơ khai thác lỗ hổng tải lên tệp tùy ý trên Cisco IOS XE Wireless Controller Software của Wireless LAN Controllers (WLCs): Tin tặc không cần xác thực có thể khai thác lỗ hổng hard-coded JSON Web Token (JWT), từ đó tải lên tệp, path traversal và thực thi mã từ xa trên hệ thống mục tiêu.	Cao
24	CVE-2025-32756	Nguy cơ khai thác lỗ hổng thực thi mã từ xa trên các sản phẩm của Fortinet bao gồm FortiCamera, FortiMail, FortiNDR, FortiRecorder, FortiVoice: Tin tặc không cần xác thực có thể khai thác lỗ hổng Stack-based Buffer Overflow, từ đó thực thi mã từ xa trên hệ thống mục tiêu.	Cao

**Nguồn: Viettel Threat Intelligence*

3. Tình hình lỗ hổng bảo mật

Các lỗ hổng được khai thác trong các chiến dịch tấn công thực tế

Ngoài các lỗ hổng mới được công bố trong 6 tháng đầu năm 2025, các nhóm tấn công vẫn tích cực sử dụng các lỗ hổng đã phát hiện từ thời gian trước để tiến hành rà quét, khai thác. Dưới đây là danh sách các lỗ hổng được sử dụng nhiều trong các chiến dịch tấn công thực tế mà Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2025:

Bảng 7. Danh sách các lỗ hổng được sử dụng nhiều trong các chiến dịch tấn công thực tế mà Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2025

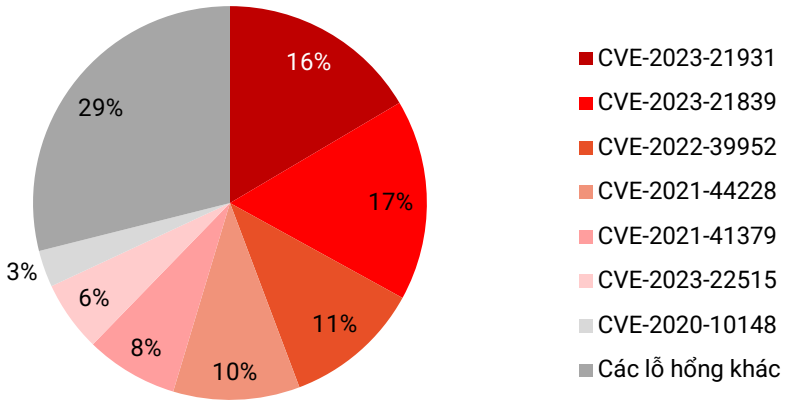
STT	Tên lỗ hổng	Thông tin chung	Mức độ đánh giá của Viettel Threat Intelligence
1	CVE-2023-21931 và CVE-2023-21839	Nguy cơ khai thác lỗ hổng CVE-2023-21931 và CVE-2023-21839 trên Oracle WebLogic Server - máy chủ ứng dụng hàng đầu trên nền tảng Java: Nguyên nhân của lỗ hổng là do máy chủ không xử lý an toàn khi deserialize dữ liệu truyền từ người dùng qua các giao thức T3, IIOP. Khai thác thành công, tin tặc có thể thực thi mã tùy ý trên hệ thống.	Cao
2	CVE-2022-39952	Nguy cơ khai thác CVE-2022-39952 trên các máy chủ Fortinet FortiNAC: Khai thác lỗ hổng thành công cho phép tin tặc tải lên tập tin tuỳ ý, từ đó thực thi mã trên máy chủ.	Nghiêm Trọng
3	CVE-2021-44228	Nguy cơ khai thác lỗ hổng Log4Shell trên thư viện Log4j - thư viện được sử dụng rất phổ biến: Khai thác lỗ hổng thành công cho phép tin tặc không cần xác thực có thể thực thi mã từ xa trên hệ thống mục tiêu.	Nghiêm Trọng
4	CVE-2021-41379	Nguy cơ khai thác lỗ hổng CVE-2021-41379 trên hệ điều hành Microsoft Windows: Khai thác lỗ hổng thành công, tin tặc có thể thực thi mã tùy ý với quyền SYSTEM trên máy nạn nhân.	Cao
5	CVE-2023-21931 và CVE-2023-21839	Nguy cơ khai thác lỗ hổng CVE-2023-21931 và CVE-2023-21839 trên Oracle WebLogic Server, máy chủ ứng dụng hàng đầu trên nền tảng Java: Nguyên nhân của lỗ hổng là do máy chủ không xử lý an toàn khi deserialize dữ liệu truyền từ người dùng qua các giao thức T3, IIOP. Khai thác thành công, tin tặc có thể thực thi mã tùy ý trên hệ thống.	Cao
6	CVE-2022-39952	Nguy cơ khai thác CVE-2022-39952 trên các máy chủ Fortinet FortiNAC: Khai thác lỗ hổng thành công cho phép tin tặc tải lên tập tin tuỳ ý, từ đó thực thi mã trên máy chủ.	Nghiêm Trọng
7	CVE-2023-22515	Nguy cơ khai thác lỗ hổng CVE-2023-22515 trên Confluence Data Center and Server: Khai thác lỗ hổng thành công, tin tặc có thể tạo tài khoản quản trị viên và truy cập vào hệ thống để thực hiện các hành vi độc hại.	Cao
8	CVE-2020-10148	Nguy cơ khai thác lỗ hổng trên SolarWinds Orion Platform - hệ thống giám sát và quản lý hạ tầng công nghệ thông tin: Tin tặc chưa được xác thực có thể truy cập trực tiếp các API và thực thi mã tùy ý. Khai thác thành công cho phép tin tặc chiếm quyền điều khiển hệ thống.	Cao

**Nguồn: Viettel Threat Intelligence*

3. Tình hình lỗ hổng bảo mật

Dưới đây là tỉ lệ các lỗ hổng được sử dụng trong các chiến dịch tấn công thực tế:

Hình 6: Thống kê tỉ lệ các lỗ hổng được sử dụng để rà quét, khai thác trong thực tế tại Việt Nam 6 tháng đầu năm 2025



Nguồn: Viettel Threat Intelligence

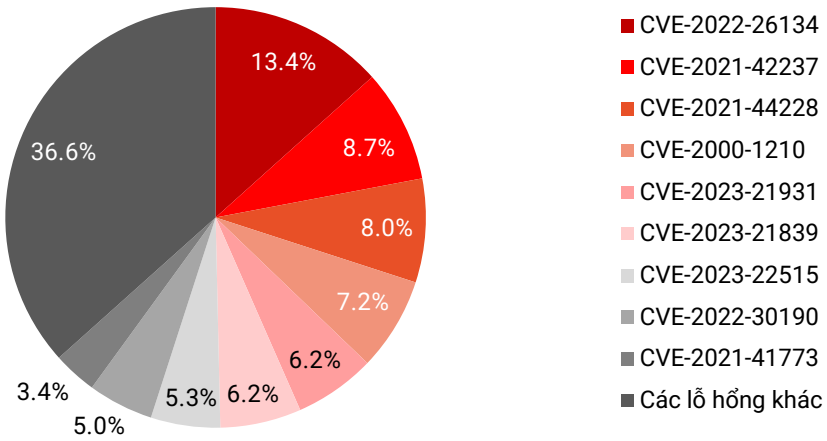
Các lỗ hổng được các nhóm tấn công sử dụng trong thực tế để rà quét và khai thác trên các hệ thống của các tổ chức trong 6 tháng đầu năm 2025 có thể kể đến là: **CVE-2023-21931 và CVE-2023-21839** (Lỗ hổng thực thi mã tùy ý trên Oracle WebLogic Server), **CVE-2022-39952** (Lỗ hổng thực thi mã từ xa trên FortiNAC), **CVE-2021-44228** (lỗ hổng thực thi mã từ xa trên Apache Log4j), **CVE-2021-41379** (Lỗ hổng leo thang đặc quyền trên Microsoft Windows), **CVE-2023-22515** (Lỗ hổng truy cập trái phép trên Confluence Data Center and Server), **CVE-2020-10148** (Lỗ hổng thực thi mã tùy ý trên SolarWinds Orion Platform),... Đây đều là các lỗ hổng trên các sản phẩm phổ biến được sử dụng trong môi trường doanh nghiệp và là các lỗ hổng cho phép tin tặc có thể thực thi mã từ xa sau khi khai thác mà không cần xác thực, kịch bản khai thác đơn giản. Các nhóm tấn công lợi dụng các lỗ hổng này nhằm mục đích làm bàn đạp ban đầu để truy cập hệ thống từ đó thực thi các hành vi độc hại tiếp theo.

3. Tình hình lỗ hổng bảo mật

Tỉ lệ lỗ hổng bị khai thác theo lĩnh vực

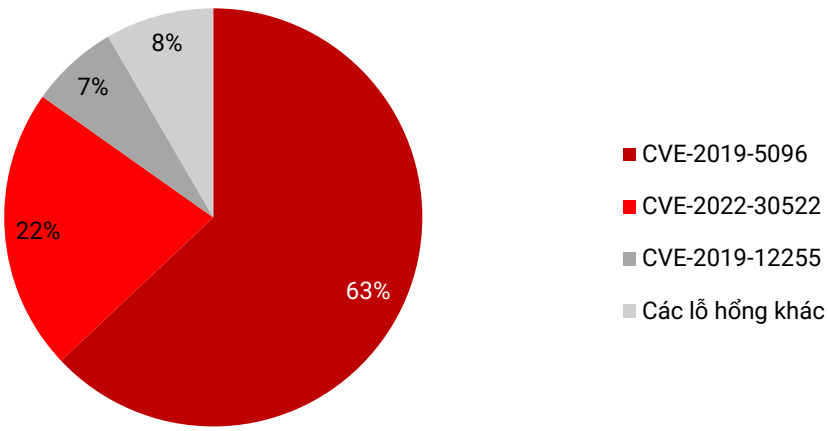
Dưới đây là tỉ lệ lỗ hổng bị khai thác theo lĩnh vực trong 6 tháng đầu năm 2025:

Hình 7: Thống kê tỉ lệ các lỗ hổng được sử dụng để rà quét, khai thác trong thực tế theo lĩnh vực Tài chính - Ngân hàng tại Việt Nam trong 6 tháng đầu năm 2025



Nguồn: Viettel Threat Intelligence

Hình 8: Thống kê tỉ lệ các lỗ hổng được sử dụng để rà quét, khai thác trong thực tế theo lĩnh vực Năng lượng tại Việt Nam trong 6 tháng đầu năm 2025



Nguồn: Viettel Threat Intelligence

4. Tấn công từ chối dịch vụ phân tán (DDoS)

*Các số liệu, biểu đồ trong mục **Tấn công từ chối dịch vụ phân tán (DDoS)** được tổng hợp từ dữ liệu độc quyền của hệ thống Viettel Anti-DDoS.*

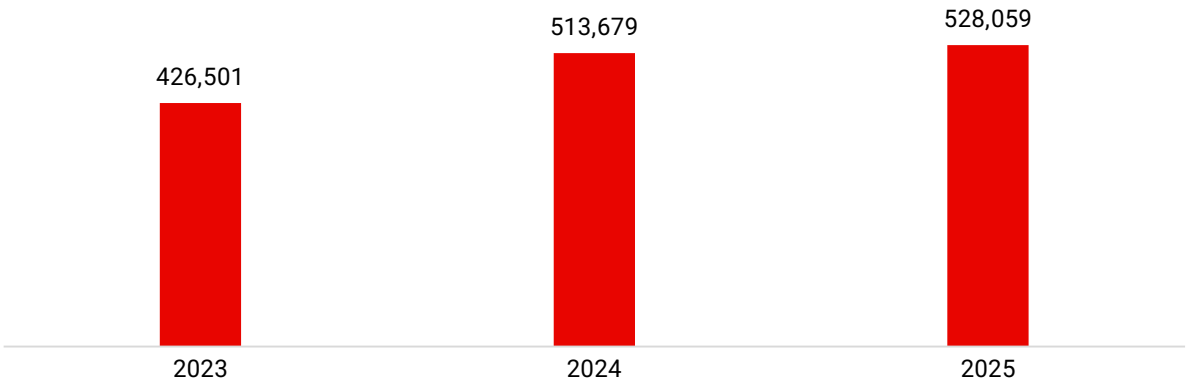
Trong 6 tháng đầu năm 2025, hệ thống Viettel Anti-DDoS đã ghi nhận **hơn 528 nghìn cuộc tấn công từ chối dịch vụ phân tán (DDoS)**. Các cuộc tấn công DDoS ghi nhận có sự dàn trải không quá chênh lệch xuyên suốt các tháng, không có tháng tăng đột biến về số lượng tấn công như trong 6 tháng cùng kỳ năm 2024. Trong đó, tháng 1 năm nay ghi nhận số lượng tấn công DDoS cao nhất, do sự xuất hiện các cuộc tấn công dạng **Hit-and-Run** - với đặc điểm tấn công ngắt quãng, cường độ cao - **gia tăng mạnh**, chủ yếu nhắm vào các tổ chức thuộc lĩnh vực **Tài chính – Ngân hàng**. Bên cạnh đó, trong tháng 6, hình thức tấn công DDoS kiểu **Carpet Bomb** – trong đó toàn bộ các địa chỉ IP thuộc cùng một dải IP của mục tiêu đều bị tấn công với cường độ trung bình nhưng tạo ra tổng băng thông rất lớn (lên tới hàng chục Gbps) – đã xuất hiện trở lại và nhắm vào các doanh nghiệp trong lĩnh vực **Công nghệ**.

Các cuộc tấn công DDoS với cường độ băng thông cao tiếp tục là mối lo ngại lớn. Trong 6 tháng đầu năm 2025, hệ thống đã ghi nhận cuộc tấn công DDoS **đạt đỉnh lên tới gần 800Gbps**, đặc biệt nhắm vào các doanh nghiệp thuộc **lĩnh vực Công nghệ**. Ngoài ra, các tổ chức trong lĩnh vực **Dịch vụ giải trí số**, **Giáo dục - Edtech và Dịch vụ công** vẫn thường xuyên bị nhắm tới, thể hiện sự phân bổ rộng rãi và không phân biệt lĩnh vực trong chiến lược của các nhóm tấn công.

Các cuộc tấn công có số lượng không chêch lệch quá lớn giữa các tháng, trong đó các tháng đều cao hơn so với năm 2024 cho thấy tần suất tấn công tăng đều của tin tặc. Nguyên nhân có thể do sự lan rộng các thiết bị IoT với bảo mật yếu đã phần nào hình thành nên các mạng **botnet**, cũng như sự xuất hiện các dịch vụ tấn công DDoS mà không yêu cầu hiểu biết quá nhiều về kỹ thuật. Đặc biệt chất lượng các cuộc tấn công này ngày càng tăng và thiệt hại ngày càng lớn, tin tặc đang dần kết hợp tấn công số lượng lớn với nhắm mục tiêu cụ thể với cường độ cao hơn, kỹ thuật phức tạp hơn, tận dụng yếu tố thời điểm và lĩnh vực có cơ chế bảo mật yếu nhằm tối đa hóa tác động.

Số lượng tấn công DDoS tăng nhẹ

Hình 9: Số lượng các cuộc tấn công DDoS theo cùng kỳ 6 tháng đầu năm 2023, 2024 và 2025



Trong 6 tháng đầu năm 2025, số lượng các cuộc tấn công DDoS đã **tăng hơn 14 nghìn cuộc**, tương đương **mức tăng gần 3%** so với cùng kỳ năm 2024.

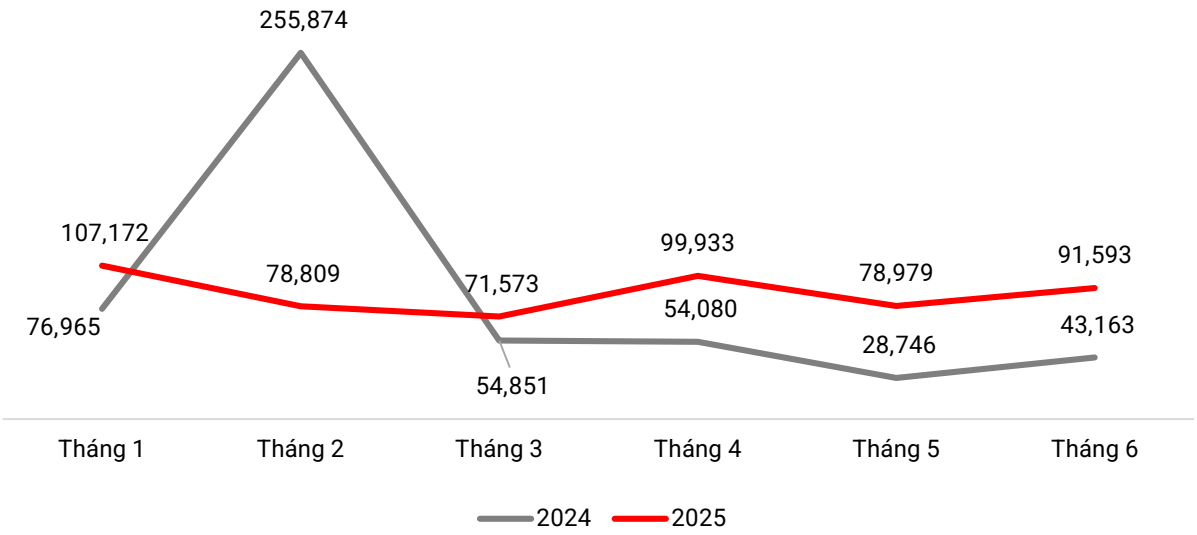
4. Tấn công từ chối dịch vụ phân tán (DDoS)

Nguyên nhân dẫn tới sự gia tăng về số lượng tấn công là do chỉ trong 2 quý đầu 2025, tin tặc không những gia tăng tần suất tấn công mà còn kết hợp đa dạng các kiểu tấn công DDoS. Nếu ở mỗi giai đoạn trước kia, tin tặc chỉ chú ý tới một yếu tố chủ yếu – số lượng tấn công DDoS cao và mạnh hoặc là số lượng tấn công ít nhưng chất lượng, gây nên hậu quả cao thì tới thời điểm này, cả 2 yếu tố trên đều đã được tin tặc áp dụng. Điều này cho thấy các cuộc tấn công đang có xu hướng được **điều chỉnh linh hoạt về thời gian và tần suất**, nhằm né tránh các cơ chế phòng thủ theo ngưỡng, cho thấy sự chuyển hướng từ **"tấn công số lượng"** sang **kết hợp** với **"tấn công chất lượng"**.

Cụ thể, trong quý 1 năm 2025, tin tặc đã sử dụng dạng tấn công **Hit-and-Run**. Với dạng tấn công này, các cuộc tấn công DDoS nhỏ lẻ được **thực hiện trong một khoảng thời gian ngắn rồi tạm ngưng một khoảng thời gian**, với mục đích gây gián đoạn dịch vụ của mục tiêu trong **khoảng thời gian cần thiết để hệ thống bảo vệ có thể phát hiện và chặn lọc tấn công**.

Tiếp đó tới cuối quý 2, tấn công **Carpet Bomb** đã xuất hiện trở lại, với **mục tiêu là nguyên một dải IP dịch vụ**. Cường độ tấn công vào mỗi IP có thể bé, nhưng tổng dung lượng tấn công vào nguyên dải IP mục tiêu sẽ lên tới hàng chục, thậm chí hàng trăm Gbps.

So sánh số lượng các cuộc tấn công DDoS qua các tháng trong cùng kỳ 6 tháng đầu năm



Nhìn theo cùng kỳ 6 tháng đầu năm 2025, có thể thấy các cuộc tấn công tập trung dồn dập vào tháng 2 năm 2024 với sự ghi nhận tăng đột biến của **2 dạng tấn công Hit-and-Run và Carpet Bomb**, thì tới năm nay các đợt tấn công diễn ra dàn trải hơn với **tần suất dày hơn**, có chủ đích và tính toán thời điểm kỹ lưỡng hơn. Đặc biệt, trong tháng 6 năm 2025, hệ thống Viettel Anti-DDoS cũng đã ghi nhận nhiều cuộc tấn công vào một doanh nghiệp thuộc lĩnh vực Logistics, đây là hệ quả do hệ thống của doanh nghiệp này đã từng bị tấn công DDoS Layer 7 (L7). Sự tăng cao về request mỗi giây (rps – đơn vị trong tấn công DDoS L7) cũng kéo theo sự tăng đột biến về băng thông so với lưu lượng trung bình ghi nhận của doanh nghiệp này.

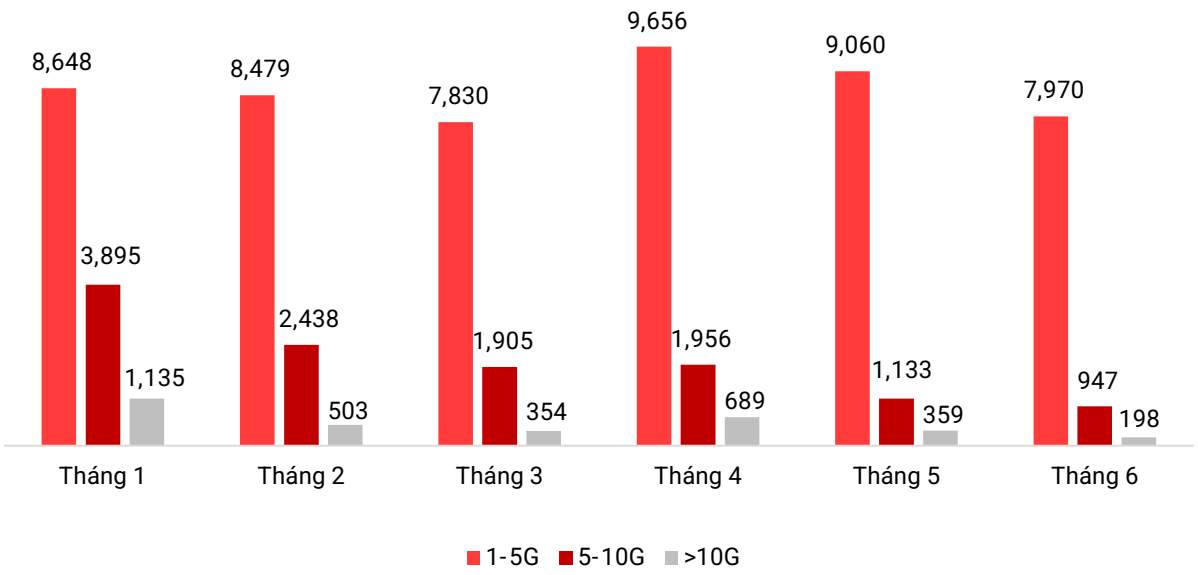
4. Tấn công từ chối dịch vụ phân tán (DDoS)

Cường độ tấn công DDoS

Hình 11: Số lượng các cuộc tấn công có cường độ <1Gbps trong 6 tháng đầu năm 2024 và 2025

Đối với các cuộc tấn công **<1Gbps**, trong 6 tháng đầu năm 2025 đã có sự giảm nhẹ về số lượng so với cùng kỳ năm 2024. Nguyên nhân đến từ kết hợp đa dạng với các kiểu tấn công Hit-and-Run hay Carpet Bomb như đã phân tích ở trên.

Hình 12: Số lượng các cuộc tấn công DDoS theo cường độ qua từng tháng trong 6 tháng đầu năm 2025



Các cuộc tấn công DDoS từ 1 – 5Gbps vẫn chiếm số lượng chủ đạo khi **chiếm tới 77% tổng số các cuộc tấn công có cường độ >1Gbps**, do đây là cường độ tấn công dễ dàng tạo ra khi tin tặc có lượng tài nguyên ít và là cường độ thường thấy được giới thiệu ở các dịch vụ tấn công DDoS underground (DDoS-as-a-Service).

4. Tấn công từ chối dịch vụ phân tán (DDoS)

Trong 2 quý đầu năm 2025, nhiều cuộc tấn công DDoS cường độ cực lớn đã được Viettel Anti-DDoS ghi nhận, cuối tháng 1 đã **xuất hiện cuộc tấn công DDoS dẫn đầu về cường độ băng thông (gần 800Gbps)**, cuộc tấn công lớn thứ 2 cũng đạt **cường độ gần 700Gbps**. Các cuộc tấn công này đều có điểm chung là lợi dụng **giao thức UDP** để tạo ra cuộc tấn công DDoS quy mô lớn, một vài cuộc tấn công đã cho thấy lượng băng thông cực lớn được sinh ra khi lợi dụng tính khuếch đại trong cơ chế của giao thức DNS. Mục tiêu bị nhắm tới là các doanh nghiệp, tổ chức thuộc **lĩnh vực Công nghệ**.

First attacks	IP	Protocol	Duration	Attacktype details	Peak BPS	Peak PPS
2025-01-28 12:25:06	[redacted]	udp	84	UDP_FLOOD	798.29Gb	184.79Mpps
2025-01-07 09:14:04	[redacted]	udp	96	Teardrop, UDP_FLOOD, DNS_REFLECTION	696.40Gb	62.27Mpps
2025-02-01 12:18:50	[redacted]	udp	90	UDP_FLOOD	567.06Gb	96.67Mpps
2025-02-18 15:21:41	[redacted]	udp	144	UDP_FLOOD	456.04Gb	40.28Mpps
2025-05-15 01:49:27	[redacted]	udp	78	UDP_FLOOD, Teardrop	405.72Gb	37.07Mpps
2025-05-15 01:49:45	[redacted]	udp	6	UDP_FLOOD, Teardrop	405.72Gb	37.07Mpps
2025-02-06 21:48:01	[redacted]	udp	144	UDP_FLOOD	364.19Gb	84.30Mpps
2025-03-02 16:41:13	[redacted]	udp	144	UDP_FLOOD	275.78Gb	24.23Mpps
2025-02-15 01:56:06	[redacted]	udp	240	Teardrop, DNS_REFLECTION, UDP_FLOOD	234.81Gb	21.39Mpps
2025-05-16 21:31:45	[redacted]	udp	48	DNS_FLOOD	226.60Gb	283.25Mpps

Hình 13: Hình ảnh thực tế một số cuộc tấn công DDoS có cường độ lớn trong quý 1 năm 2025

Có thể thấy số lượng tấn công DDoS trong 2 quý đầu năm 2025 đã có sự gia tăng rõ rệt so với năm 2024, kết hợp giữa số lượng tấn công cao và **chất lượng các cuộc tấn công ngày càng tăng, thiệt hại ngày càng lớn**. Lợi dụng bộ giao thức TCP, các cuộc tấn công DDoS có thể dễ dàng làm cao tải tài nguyên và gây treo các thiết bị quan trọng như tường lửa, thiết bị phân tải, từ đó làm ảnh hưởng tới trải nghiệm người dùng.

Tiếp đó là các kiểu tấn công **DDoS lợi dụng DNS** khai thác tài nguyên máy chủ DNS public trên mạng làm bàn đạp để khuếch đại tấn công vẫn luôn hiện diện và là một trong những kiểu tấn công phổ biến, gây ảnh hưởng tới hạ tầng của mục tiêu. Thêm đó là các cuộc tấn công **DDoS DNS Recursive** gây ảnh hưởng tới máy chủ DNS, làm gián đoạn dịch vụ mục tiêu.

Đặc biệt, đối với kiểu tấn công **DDoS làm tràn băng thông**, hiện tại và trong tương lai vẫn sẽ là kiểu tấn công phổ biến và dễ sử dụng nhất. Kết hợp các máy chủ DNS, NTP hay các thiết bị IoT bảo mật yếu, tấn công **DDoS khuếch đại** (DDoS Amplification) **băng thông** sẽ trở thành công cụ được sử dụng nhiều bởi các tin tặc, khi lượng băng thông sinh ra từ kiểu tấn công này có thể lên tới vài trăm Gbps, dễ dàng gây nghẽn đường truyền của doanh nghiệp, ảnh hưởng trực tiếp tới dịch vụ khách hàng.

Kết hợp đa dạng các hình thức tấn công khác nhau như **Carpet Bomb**, tấn công cường độ thấp tới toàn bộ dải IP của mục tiêu, hay **Hit-and-Run** là tấn công làm cao tải thiết bị của mục tiêu trong 1 khoảng thời gian ngắn rồi dừng, sau đó lặp lại liên tục trong nhiều ngày là một phương án xuất hiện nhiều gần đây. Cách thức này hoàn toàn có thể sinh ra lượng băng thông cực lớn, làm cạn kiệt tài nguyên thiết bị mạng, gây ảnh hưởng nghiêm trọng tới hạ tầng song song đó là dịch vụ khách hàng.

Với các hình thức tấn công DDoS ngày càng tinh vi và phức tạp, các doanh nghiệp không thể chỉ dựa vào các giải pháp phòng thủ truyền thống mà cần đầu tư vào các giải pháp chống tấn công DDoS chuyên dụng với hiệu quả cao. Giải pháp Viettel Anti-DDoS cung cấp khả năng phát hiện tấn công sớm và ngăn chặn tấn công hiệu quả, đảm bảo tính sẵn sàng cho dịch vụ của các doanh nghiệp.

5. Các nhóm tấn công có chủ đích (APT)

Trong 6 tháng đầu năm 2025, phương pháp tấn công chủ yếu của các nhóm APT vẫn là sử dụng tài liệu, phần mềm giả mạo để đánh lừa người dùng thực thi mã độc. Theo ghi nhận của Viettel Threat Intelligence, xu hướng tấn công trong 6 tháng đầu năm nay phần lớn nhắm vào các tổ chức, doanh nghiệp thuộc lĩnh vực **Năng lượng, Sản xuất - Công nghiệp, Dịch vụ công.**

Trong 6 tháng đầu năm 2025, các nhóm tấn công có chủ đích đã nâng cấp thêm công cụ, mã độc sử dụng trong các chiến dịch tấn công. Một trong các kỹ thuật được các nhóm tấn công sử dụng nhiều nhất có thể kể đến như:

- **DLL-Sideloading**: Là kỹ thuật phổ biến nhất được các nhóm tấn công sử dụng. Kỹ thuật này có chức năng bỏ qua lớp phòng thủ của hệ thống do payload được thực thi thông qua một tiến trình hợp pháp.
- **Mã hoá payload dựa trên thông tin máy tính của nạn nhân**: Payload được mã hoá dựa trên các thông tin đặc trưng của máy tính mục tiêu (ví dụ: địa chỉ MAC hoặc tên máy), đảm bảo chỉ hoạt động trên hệ thống đã xác định, từ đó giảm nguy cơ bị phân tích trên các môi trường khác.
- **Domain Fronting**: Là kỹ thuật che giấu lưu lượng mạng bằng cách lợi dụng giao thức HTTPS và CDN để ngụy trang kết nối đến tên miền hợp pháp, trong khi thực tế lưu lượng mạng đó được kết nối đến máy chủ điều khiển (C2), giúp vượt qua các hệ thống giám sát và tường lửa (firewall).

Bảng 8. Danh sách nhóm APT được Viettel Threat Intelligence thu thập và đánh giá có ảnh hưởng lớn đến doanh nghiệp, tổ chức tại Việt Nam trong 6 tháng đầu năm 2025

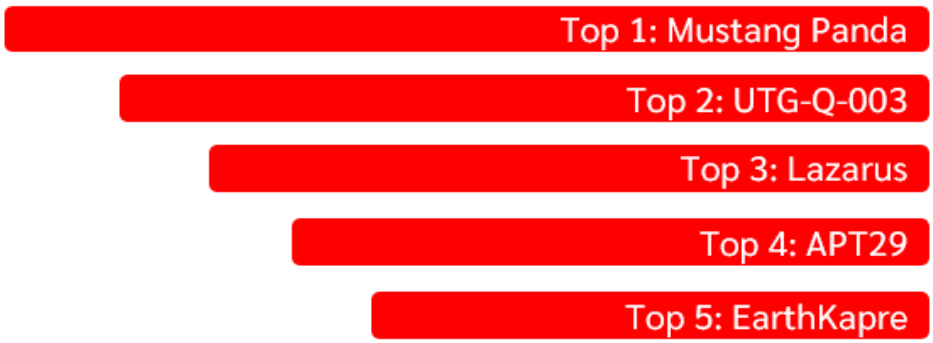
STT	Tên nhóm	Mô tả	Các kỹ thuật, công cụ thường xuyên sử dụng
1	Mustang Panda	Nhóm tin tặc chuyên nhắm mục tiêu vào các tổ chức thuộc lĩnh vực Dịch vụ công và Năng lượng. Trong 6 tháng đầu năm 2025, Viettel Threat Intelligence phát hiện nhiều mẫu mã độc của nhóm Mustang Panda được phát tán với nội dung liên quan đến các doanh nghiệp, tổ chức.	Spearphishing Attachment, DLL Side Loading, Template Injection
2	Lotus Blossom	Còn được biết đến với tên DRAGONFISH, Spring Dragon, Lotus Panda. Nhóm đã hoạt động từ năm 2012, tập trung tấn công các cơ quan chức năng và doanh nghiệp lớn, với các phương thức tấn công ngày càng tinh vi.	Spearphishing Attachment, DLL Side Loading, Domain Fronting, ShadowShell
3	APT37	Còn được gọi là Reaper, ScarCruft. Nhóm này đã hoạt động ít nhất từ 2012, tập trung vào thực hiện các chiến dịch gián điệp mạng.	Spearphishing Attachment, DLL Side Loading

**Nguồn: Viettel Threat Intelligence*

*Thông tin về **Chiến dịch tấn công mới của nhóm APT Lotus Blossom** đã được phân tích chi tiết trong báo cáo độc quyền của Viettel Threat Intelligence tại blog Viettel Cyber Security: [Chiến dịch tấn công mới của nhóm APT Lotus Blossom]*

5. Các nhóm tấn công có chủ đích (APT)

Dưới đây là mức độ hoạt động mạnh của các nhóm APT tại Việt Nam trong 6 tháng đầu năm 2025:



Hình 14: Mức độ hoạt động mạnh của các nhóm APT tại Việt Nam trong 6 tháng đầu năm 2025

**Nguồn: Viettel Threat Intelligence*

Dưới đây là danh sách chiến dịch nổi bật được Viettel Threat Intelligence phát hiện và đánh giá có ảnh hưởng trong 6 tháng đầu năm 2025:

Bảng 9. Danh sách các chiến dịch tấn công có chủ đích nổi bật được Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2025

Thời gian	Chiến dịch	Mô tả	Lĩnh vực
Tháng 1/2025	Cảnh báo nhóm APT Earth Estries tấn công vào các tổ chức thuộc lĩnh vực Công nghệ tại Đông Nam Á	Viettel Threat Intelligence cảnh báo nhóm APT Earth Estries triển khai mã độc thông qua khai thác các lỗ hổng n-day nhắm mục tiêu vào nhiều công ty thuộc lĩnh vực Công nghệ tại Đông Nam Á.	Công nghệ
	Cảnh báo nhóm RedDelta tấn công các tổ chức thuộc lĩnh vực Dịch vụ công tại Việt Nam	Viettel Threat Intelligence cảnh báo nhóm APT RedDelta thực hiện tấn công mạng nhắm vào tổ chức thuộc lĩnh vực Dịch vụ công tại Việt Nam.	Dịch vụ công
Tháng 2/2025	Cảnh báo về chiến dịch tấn công của nhóm Earth Preta (Mustang Panda APT) nhắm vào các tổ chức khu vực Châu Á - Thái Bình Dương	Viettel Threat Intelligence cảnh báo về các chiến dịch tấn công của nhóm Earth Preta (hay còn gọi là Mustang Panda APT) nhắm mục tiêu vào các tổ chức trong khu vực Châu Á - Thái Bình Dương.	Dịch vụ công
	Cảnh báo nhóm APT Mustang Panda nhắm vào các tổ chức, doanh nghiệp khu vực ASEAN	Viettel Threat Intelligence cảnh báo nhóm APT Mustang Panda sử dụng biến thể của mã độc Bookworm; nhắm mục tiêu vào các tổ chức, doanh nghiệp tại các quốc gia ASEAN.	Doanh nghiệp, tổ chức

5. Các nhóm tấn công có chủ đích (APT)

Bảng 9 (tiếp). Danh sách các chiến dịch tấn công có chủ đích nổi bật được Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2025

Thời gian	Chiến dịch	Mô tả	Lĩnh vực
Tháng 2/2025	Cảnh báo nhóm APT41 tiếp tục sử dụng ShadowPad kết hợp ransomware trong các chiến dịch tấn công	Viettel Threat Intelligence cảnh báo nhóm APT41 sử dụng mã độc Shadowpad kết hợp với ransomware tự tạo để tấn công mã hóa và đòi tiền chuộc. Nhóm nhắm vào các tổ chức, doanh nghiệp tại các quốc gia khu vực Đông Nam Á và Châu Âu.	Doanh nghiệp, tổ chức
	Cảnh báo chiến dịch APT SalmonSlalom nhắm vào lĩnh vực công nghiệp tại khu vực APAC	Viettel Threat Intelligence cảnh báo chiến dịch APT SalmonSlalom nhắm vào các doanh nghiệp thuộc lĩnh vực công nghiệp tại khu vực Châu Á - Thái Bình Dương (APAC).	Công nghiệp
Tháng 3/2025	Cảnh báo nhóm APT Lotus Blossom nhắm vào nhiều lĩnh vực trong khu vực Đông Á và Đông Nam Á	Viettel Threat Intelligence cảnh báo nhóm APT Lotus Blossom nhắm vào các tổ chức, doanh nghiệp thuộc nhiều lĩnh vực tại khu vực Đông Á và Đông Nam Á như Philippines, Việt Nam, Hồng Kông, Đài Loan.	Nhiều lĩnh vực
	Cảnh báo về chiến dịch tấn công diện rộng của nhóm APT SideWinder	Viettel Threat Intelligence cảnh báo về chiến dịch tấn công diện rộng của nhóm SideWinder APT với mục tiêu chính là các cơ quan chức năng, các công ty logistics và cơ sở hạ tầng hàng hải tại Nam Á và Đông Nam Á, Trung Đông và Châu Phi.	Nhiều lĩnh vực
	Cảnh báo về nhóm APT37 phát tán mã độc RokRat	Viettel Threat Intelligence cảnh báo về nhóm APT37 phát tán mã độc RokRat thông qua email lừa đảo có chứa tệp ZIP độc hại.	Công nghiệp
Tháng 4/2025	Cảnh báo về mẫu mã độc mới của nhóm Mustang Panda	Viettel Threat Intelligence cảnh báo về mẫu mã độc Mustang Panda APT. Nhóm tấn công nhắm mục tiêu vào các doanh nghiệp, tổ chức tại khu vực châu Á - Thái Bình Dương.	Doanh nghiệp, tổ chức
	Cảnh báo mã độc nghi ngờ thuộc nhóm APT Lotus Blossom	Viettel Threat Inteligence cảnh báo trong quá trình giám sát không gian mạng đã phát hiện mẫu mã độc nghi ngờ thuộc nhóm APT Lotus Blossom.	Doanh nghiệp, tổ chức
	Cảnh báo về chiến dịch tấn công nhóm Earth Kurma APT	Viettel Threat Intelligence cảnh báo về chiến dịch tấn công nhóm Earth Kurma APT nhắm mục tiêu là các tổ chức thuộc lĩnh vực Công nghệ và Dịch vụ công tại khu vực Đông Nam Á, bao gồm Philippines, Việt Nam, Thái Lan, và Malaysia. Nhóm tấn công sử dụng các mã độc tùy chỉnh như TESDAT, SIMPOBOXSPY, KRNRAT, MORIYA và rootkit để đánh cắp dữ liệu, duy trì truy cập lâu dài và ẩn mình trong hệ thống của nạn nhân. Đồng thời nhóm lợi dụng các dịch vụ đám mây công cộng để truyền dữ liệu.	Công nghệ, Dịch vụ công

5. Các nhóm tấn công có chủ đích (APT)

Bảng 9 (tiếp). Danh sách các chiến dịch tấn công có chủ đích nổi bật được Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2025

Thời gian	Chiến dịch	Mô tả	Lĩnh vực
Tháng 5/2025	Cảnh báo nhóm APT TheWizards tiến hành các cuộc tấn công Adversary-in-the-Middle nhằm mục tiêu vào các tổ chức, doanh nghiệp khu vực châu Á	Viettel Threat Intelligence cảnh báo về nhóm APT TheWizards: Nhóm này sử dụng công cụ Spellbinder để thực hiện các cuộc tấn công Adversary-in-the-Middle (AitM) thông qua kỹ thuật giả mạo IPv6 SLAAC (Stateless Address Autoconfiguration) nhằm chiếm quyền điều khiển cơ chế cập nhật của phần mềm hợp pháp để triển khai backdoor WizardNet.	Doanh nghiệp, tổ chức
	Cảnh báo về chiến dịch tấn công APT nhắm vào các công ty, tổ chức ngành Năng lượng	Viettel Threat Intelligence cảnh báo trong quá trình giám sát không gian mạng đã ghi nhận chiến dịch tấn công có chủ đích nhắm vào các công ty, tổ chức ngành Năng lượng. Dựa trên hành vi và hạ tầng của nhóm tấn công, Viettel Threat Intelligence nghi ngờ chiến dịch được thực hiện bởi nhóm Lotus Blossom.	Năng lượng
	Cảnh báo mã độc Reshell từ nhóm APT EarthKrahang	Viettel Threat Intelligence cảnh báo trong quá trình giám sát không gian mạng đã ghi nhận mã độc Reshell từ nhóm APT EarthKrahang nhắm vào các công ty, tổ chức tại Việt Nam.	Doanh nghiệp, tổ chức
	Cảnh báo nhóm APT Earth Lamia khai thác lỗ hổng để xâm nhập vào hệ thống	Viettel Threat Intelligence cảnh báo nhóm APT Earth Lamia nhắm mục tiêu vào các công ty, tổ chức tại Brazil, Ấn Độ và các quốc gia Đông Nam Á. Nhóm này chủ yếu khai thác lỗ hổng trong các ứng dụng web để xâm nhập vào tổ chức mục tiêu, sau đó phát triển và tùy biến các công cụ tấn công nhằm né tránh phát hiện và tăng hiệu quả đánh cắp dữ liệu.	Doanh nghiệp, tổ chức
Tháng 6/2025	Cảnh báo chiến dịch APT mới sử dụng Microsoft OneDrive làm C&C nhằm mục tiêu vào các tổ chức, doanh nghiệp thuộc lĩnh vực Năng lượng tại Việt Nam	Viettel Threat Intelligence cảnh báo mã độc APT mới từ một nhóm tin tặc chưa xác định, nhằm mục tiêu vào các tổ chức thuộc lĩnh vực Năng lượng tại Việt Nam. Mẫu APT mới này hoạt động cực kì tinh vi bằng cách sử dụng Microsoft OneDrive làm C&C giúp ẩn giấu hành vi.	Năng lượng
	Cảnh báo mã độc RAT Spectralviper nghi ngờ thuộc APT Ocean Lotus tấn công vào công ty, tổ chức tại Việt Nam	Trong quá trình giám sát không gian mạng, Viettel Threat Intelligence đã phát hiện mẫu mã độc RAT Spectralviper nghi ngờ thuộc nhóm APT Ocean Lotus tấn công vào các công ty, tổ chức tại Việt Nam. Ocean Lotus là nhóm tấn công APT từng có tiền sử tấn công vào các tổ chức Việt Nam với mục đích đánh cắp các dữ liệu nhạy cảm.	Doanh nghiệp, tổ chức

**Nguồn: Viettel Threat Intelligence*

*Thông tin phân tích chi tiết về các nguy cơ tấn công có chủ đích (APT) được chia sẻ **độc quyền** trong các báo cáo chuyên sâu của Viettel Threat Intelligence tại https://platform.cyberintel.io/#/.*

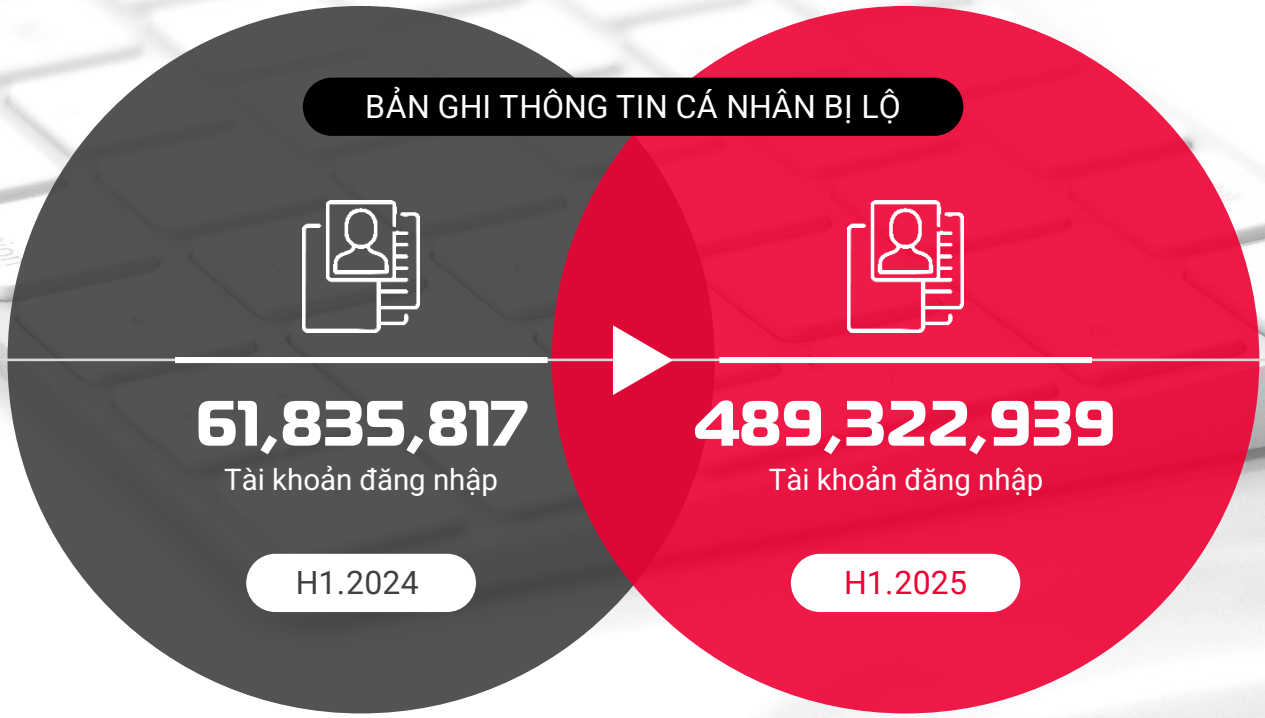
6. Lộ lọt, rò rỉ dữ liệu

Trong 6 tháng đầu năm 2025, Viettel Threat Intelligence ghi nhận số lượng hơn **489 triệu** thông tin tài khoản bị lộ lọt trên thế giới, **tăng gấp gần 7 lần** so với cùng kỳ năm 2024. Tại Việt Nam, trong 6 tháng đầu năm 2025 ghi nhận số tài khoản lộ lọt lên tới **gần 8.5 triệu tài khoản**, chiếm 1.7% số lượng toàn cầu. Sự phát triển của các nhóm tấn công sử dụng mã độc đánh cắp dữ liệu, cũng như mô hình Stealer-as-a-Service đã dẫn tới sự gia tăng mạnh mẽ số lượng tài khoản lộ lọt.

Thông tin cá nhân bị đánh cắp

Lộ lọt dữ liệu là một trong những mối đe dọa nghiêm trọng đối với mọi tổ chức, đặc biệt là khi các thông tin nhạy cảm và quan trọng bị tiết lộ hoặc truy cập trái phép. Những sự cố này có thể xảy ra dưới nhiều hình thức, từ việc rò rỉ thông tin cá nhân, tài khoản đăng nhập, đến các dữ liệu doanh nghiệp quan trọng. Rất nhiều trường hợp lộ lọt thông tin tài khoản đăng nhập vào các hệ thống quan trọng và nhạy cảm như hệ thống Email, hệ thống quản lý tập trung SSO hoặc hệ thống VPN dùng để truy cập nội bộ. Khi các dữ liệu này rơi vào tay kẻ xấu, hậu quả có thể rất nặng nề, ảnh hưởng trực tiếp đến hoạt động kinh doanh và uy tín của tổ chức.

So sánh số lượng bản ghi thông tin tài khoản cá nhân bị đánh cắp trên thế giới trong 6 tháng đầu năm 2024 và 6 tháng đầu năm 2025:

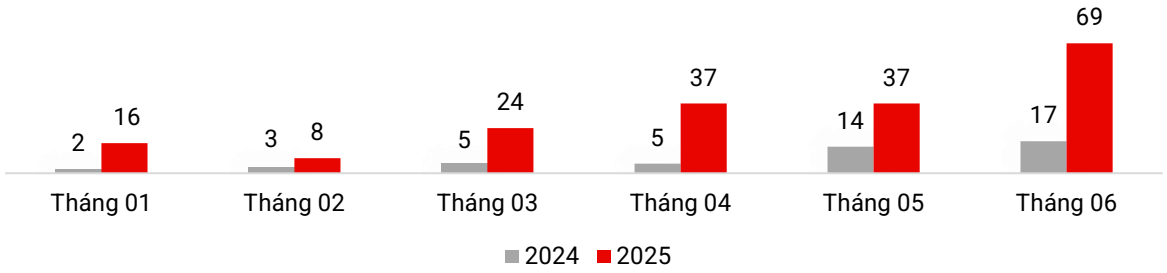


Hình 15: Số lượng bản ghi thông tin tài khoản cá nhân lộ lọt 6 tháng đầu năm 2024 và 6 tháng đầu năm 2025

**Nguồn: Viettel Threat Intelligence*

6. Lộ lọt, rò rỉ dữ liệu

Dữ liệu nhạy cảm của các tổ chức, doanh nghiệp bị lộ lọt, rao bán



Nguồn: Viettel Threat Intelligence

Trong 6 tháng đầu năm 2025 chứng kiến sự bùng nổ của việc rao bán thông tin người dùng, dữ liệu hệ thống cùng nhiều dữ liệu nhạy cảm của các doanh nghiệp lớn tại Việt Nam: ghi nhận **191 vụ lộ lọt dữ liệu**, tăng 3 lần so với cùng kỳ năm trước, với gần **3 tỷ bản ghi** và **482.1 GB dữ liệu**.

Có thể thấy, ngoại trừ tháng 02/2025 thì số lượng các vụ rao bán, chia sẻ dữ liệu nhạy cảm theo từng tháng trong 6 tháng đầu năm nay đều tăng đáng kể so với cùng kỳ năm 2024. Dưới đây là danh sách các vụ lộ lọt, rao bán dữ liệu nổi bật theo ngành trong 6 tháng đầu năm 2025:

Bảng 10. Danh sách các vụ lộ lọt dữ liệu nổi bật tại Việt Nam trong 6 tháng đầu năm 2025

STT	Thông tin	Lĩnh vực	Số vụ	Chi tiết
1	Mã nguồn, thông tin cấu trúc hệ thống, dữ liệu khách hàng.	Công nghệ - Viễn thông	17	1,323,624 bản ghi ~ 0.34 GB dữ liệu
2	Dữ liệu, thông tin cá nhân, tài liệu của nhiều trường đại học, tổ chức giáo dục tại Việt Nam.	Giáo dục - Edtech	16	5,614,604 bản ghi ~ 10 MB dữ liệu
3	Thông tin khách hàng, thông tin mua bán.	Bán lẻ - Thương mại điện tử	50	13,668,912 bản ghi
4	Dữ liệu thông tin khách hàng, dữ liệu trích xuất từ hệ thống nội bộ.	Tài chính - Ngân hàng	20	16,740,083 bản ghi
5	Dữ liệu thông tin khách hàng, dữ liệu trích xuất từ hệ thống nội bộ.	Bảo hiểm	5	~ 51 triệu bản ghi 3.10 GB dữ liệu
6	Thông tin khách hàng, dữ liệu trích xuất từ hệ thống nội bộ.	Năng lượng – Hạ tầng thiết yếu	8	74,700,089 bản ghi 4.5 GB dữ liệu
7	Thông tin cá nhân, thông tin eKYC.	Khác	23	64,872,872 bản ghi 41.03 GB dữ liệu
8	Thông tin của khách hàng, thông tin sử dụng dịch vụ.	Dịch vụ tiêu dùng – Cá nhân	31	2,689,875,272 bản ghi 356 GB dữ liệu
9	Thông tin người dùng, thông tin trích xuất từ hệ thống nội bộ.	Dịch vụ công	6	10,674,949 bản ghi 77.10 GB dữ liệu
10	Dữ liệu thông tin đơn hàng vận tải, dữ liệu trích xuất từ hệ thống nội bộ.	Giao thông vận tải	2	81,759 bản ghi
11	Thông tin của khách hàng, thông tin mua bán, đầu tư.	Chứng khoán – Đầu tư	9	3,620,333 bản ghi
12	Thông tin khách hàng, thông tin trích xuất từ hệ thống nội bộ.	Sản xuất - Công nghiệp	2	40,001 bản ghi
13	Thông tin khách hàng, thông tin trích xuất từ hệ thống nội bộ.	Y tế	2	474,453 bản ghi

Nguồn: Viettel Threat Intelligence

6. Lộ lọt, rò rỉ dữ liệu

Lộ lọt dữ liệu do vô tình tải lên các nền tảng công khai

Các nhà phát triển phần mềm (Developer) chia sẻ mã nguồn của các dự án lên các nền tảng như **Github**, **DockerHub** hoặc **Postman** để dễ dàng quản lý và kiểm thử. Tuy nhiên, trong mã nguồn của dự án khi đẩy lên công khai có chứa các trường thông tin nhạy cảm được hardcoded như địa chỉ IP nội bộ, thông tin đăng nhập hoặc các mã bí mật. Các thông tin này thường vô tình bị đăng tải công khai lên không gian mạng. Điều này dẫn tới việc tin tặc có thể đọc hiểu mã nguồn nội bộ, từ đó thực hiện khai thác và tấn công khi phát hiện lỗ hổng (nếu có) hoặc lấy mã nguồn và xây dựng trang web lừa đảo.

Ngoài ra, việc tài liệu của tổ chức được tải lên các trang chia sẻ như **Scribd,** nếu không có sự kiểm soát quyền truy cập có thể dẫn đến nhiều nguy cơ rủi ro liên quan đến việc lộ lọt thông tin và dữ liệu nhạy cảm. Các tài liệu này có thể bị chỉnh sửa hoặc sao chép bởi bên thứ ba mà không có sự đồng ý của chủ sử hữu, dẫn đến việc thông tin bị hiểu sai hoặc giả mạo, gây mất uy tín cho doanh nghiệp, tổ chức. Nếu các tài liệu này chứa thông tin mật khẩu, dữ liệu cá nhân của nhân viên hoặc thông tin về các hệ thống nội bộ của tổ chức thì tin tặc có thể dễ dàng lợi dụng để khai thác và xâm nhập hệ thống của tổ chức.

Trong 6 tháng đầu năm 2025, Viettel Threat Intelligence đã phát hiện nhiều trường hợp lộ lọt dữ liệu, trong đó có **33 trường hợp (Nghiêm Trọng: 1, Cao: 13)** liên quan tới các lĩnh vực **Tài chính - Ngân hàng, Giao thông vận tải, Công nghệ - Viễn thông, Hàng không, Dịch vụ công, Năng lượng - Hạ tầng thiết yếu**.

Dưới đây là danh sách các trường hợp lộ lọt do vô tình chia sẻ mã nguồn theo ngành trong 6 tháng đầu năm 2025:

Bảng 11. Các trường hợp lộ lọt dữ liệu do vô tình chia sẻ mã nguồn nổi bật trong 6 tháng đầu năm 2025

STT	Lĩnh vực	Số vụ	Chi tiết
1	Tài chính - Ngân hàng	20	Lộ lọt thông tin mã nguồn, bộ cài đặt có chứa thông tin tài khoản đăng nhập, khóa API nhạy cảm, tài liệu.
2	Công nghệ - Viễn thông	6	Lộ lọt thông tin mã nguồn có chứa thông tin tài khoản đăng nhập các hệ thống nội bộ.
3	Năng lượng - Hạ tầng thiết yếu	1	Lộ lọt thông tin mã nguồn chứa thông tin nhạy cảm liên quan đến các hệ thống nội bộ.
4	Giao thông vận tải	2	Lộ lọt thông tin API chứa thông tin tài khoản đăng nhập các hệ thống dịch vụ, tài liệu.
5	Hàng không	3	Lộ lọt thông tin mã nguồn có chứa API nhạy cảm và các thông tin dịch vụ.
6	Dịch vụ công	1	Lộ lọt thông tin mã nguồn chứa thông tin nhạy cảm liên quan đến các hệ thống nội bộ.

**Nguồn: Viettel Threat Intelligence*

VIETTEL THREAT INTELLIGENCE

Giải pháp cập nhật tri thức An ninh mạng số 1 Việt Nam

viettel security

TRỤ SỞ CHÍNH TẠI HÀ NỘI

Tầng 41-43, tòa nhà Keangnam Landmark 72,
đường Phạm Hùng, phường Từ Liêm, TP. Hà Nội

VĂN PHÒNG MIỀN NAM

Tầng 28A2, tòa nhà Viettel, 285 Cách Mạng
Tháng Tám, phường Hoà Hưng, TP. Hồ Chí Minh

LIÊN HỆ

(+84) 971 360 360

vcs.sales@viettel.com.vn

www.viettelcybersecurity.com