viettel
security

BÁO CÁO TÌNH HÌNH NGUY CƠ ATTT VIỆT NAM QUÝ 1 NĂM 2025

VIETTEL THREAT INTELLIGENCE

MỤC LỤC

Phần I.
TỔNG QUAN

1. Xu hướng

Trong quý 1 năm 2025, Viettel Threat Intelligence đã ghi nhận nhiều nguy cơ mất 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:

~4.5 triệu

Tài khoản bị đánh cắp tại Việt Nam

Số lượng tài khoản lộ lọt tại Việt Nam chiếm **12.6%** trong tổng số tài khoản bị đánh cắp trên thế giới (gần 36 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.

48

Vụ rao bán dữ liệu tại Việt Nam với:

- >155 triệu bản ghi
- 24.65GB dữ liệu

▲ Tăng 380% so với Q1.2024 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 doanh nghiệp.

>1.3 TB

Dữ liệu bị mã hóa

Tấn công bằng mã độc vẫn là nguy cơ lớn và ngày càng tinh vi, đặc biệt là các loại như Ransomware, RAT.

Các loại mã độc mới tiếp tục có sự gia tăng đáng kể về cả số lượng, cách thức phát tán và cách thức hoạt động với các dạng mã độc **Stealer As a Service**, **Ransomware As a Service**. Các cuộc tấn công không chỉ mã hóa mà còn đánh cắp dữ liệu, gây áp lực chi trả tiền chuộc.

36 lỗ hổng

Có khả năng ảnh hưởng tới hệ thống của các doanh nghiệp, tổ chức tại Việt Nam được Viettel Threat Intelligence phân tích chi tiết.

Tốc độ phát triển nhanh của công nghệ cũng như việc mở rộng chuyển đổi số trong doanh nghiệp đã & đang dẫn tới lỗ hổng bảo mật mới ngày càng xuất hiện nhiều.

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

911

Tên miền lừa đảo

746

Trang giả mạo

Hình thức lừa đảo phổ biến:

- Lừa đảo, giả mạo 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.

>257.000

Cuộc tấn công DDoS

▼ Giảm 30% so với Q1.2024

Nhóm lĩnh vực mục tiêu: Tài chính, Công nghệ, Giáo dục, Giải trí điện tử.

Tuy số lượng các cuộc tấn công DDoS có sự suy giảm so với cùng kỳ năm ngoái, nhưng hiện vẫn **duy trì ở mức cao** với các phương thức tấn công không ngừng cải tiến và biến đổi. Các chiến thuật tấn công như Hit-and-Run ngày càng tinh vi với các đợt **tấn công cao điểm lên tới 800Gbps**.

2. 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:

Bảo vệ tài khoản và dữ liệu nhạy cảm

- Triển khai giám sát rò rỉ dữ liệu (Data Leak Monitoring) cho email, VPN, SSO và các tài khoản truy cập nội bộ.
- Áp dụng mô hình Zero Trust và các công cụ quản lý truy cập đặc quyền (PAM/PIM) để giới hạn truy cập theo nguyên tắc quyền tối thiểu.
- Giám sát hoạt động truy cập bất thường vào hệ thống và dữ liệu nhạy cảm theo thời gian thực (real-time).

Giám sát liên tục và phản ứng sớm

- Thiết lập trung tâm giám sát ATTT 24/7 (SOC) hoặc sử dụng dịch vụ thuê ngoài.
- Kết hợp với dịch vụ Threat Intelligence để phát hiện các chiến dịch tấn công, các dấu hiệu, nguy cơ ATTT đang diễn ra trên toàn cầu và xung quanh doanh nghiệp.
- Chủ động thực hiện Threat Hunting định kỳ nhằm phát hiện tấn công ẩn sâu.
- Hợp tác với đơn vị chuyên trách ATTT để tiếp cận cảnh báo sớm và hỗ trợ xử lý sự cố kịp thời.

Quản trị rủi ro từ chuỗi cung ứng và bên thứ ba

- Triển khai chương trình đánh giá Third Party Risk Management (TPRM).
- Đưa yêu cầu bảo mật thành điều khoản bắt buộc trong hợp đồng với đối tác.

Phòng chống mã độc và tấn công tống tiền

- Định kỳ rà soát các điểm trọng yếu dễ bị tấn công mã hóa tống tiền (ransom-points) như máy chủ, máy trạm, file server,...
- Cập nhật bản vá cho phần mềm, hệ điều hành kịp thời.
- Sao lưu định kỳ mã nguồn, dữ liệu khách hàng, dịch vụ quan trọng, có chiến lược phục hồi khi xảy ra sự cố.

Xây dựng văn hóa an toàn thông tin nội bộ

- Tổ chức đào tạo nhận thức ATTT định kỳ, đặc biệt với bộ phận xử lý dữ liệu và quản trị hệ thống.
- Áp dụng chính sách kiểm soát truy cập phân quyền, tránh chia sẻ thông tin nội bộ không kiểm soát.
- Xây dựng lộ trình năng lực ATTT gắn với chiến lược chuyển đổi số bền vững của doanh nghiệp.

Phần II.

THỐNG KÊ & PHÂN TÍCH CHI TIẾT

1. Các dòng mã độc

Trong quý 1 năm 2025, Viettel Threat Intelligence ghi nhận sự gia tăng rõ rệt các dòng mã độc nhắm vào doanh nghiệp Việt Nam, đặc biệt là Ransomware và RAT.

Mã độc mã hóa tống tiền (Ransomware)

Trong quý 1 năm 2025, số lượng dữ liệu bị tấn công mã hóa **lên tới hơn 1 Terabyte**. Có thể thấy mức độ ảnh hưởng của các cuộc tấn công Ransomware ngày càng nghiêm trọng, không chỉ mã hóa dữ liệu mà còn kết hợp đánh cắp thông tin, gia tăng áp lực buộc nạn nhân phải trả tiền chuộc. Các tổ chức lớn thường đối mặt với rủi ro cao hơn do quy mô hệ thống phức tạp. Các ngành như **Tài chính, Công nghệ, Dịch vụ công và Chăm sóc sức khỏe** là mục tiêu bị nhắm đến hàng đầu.

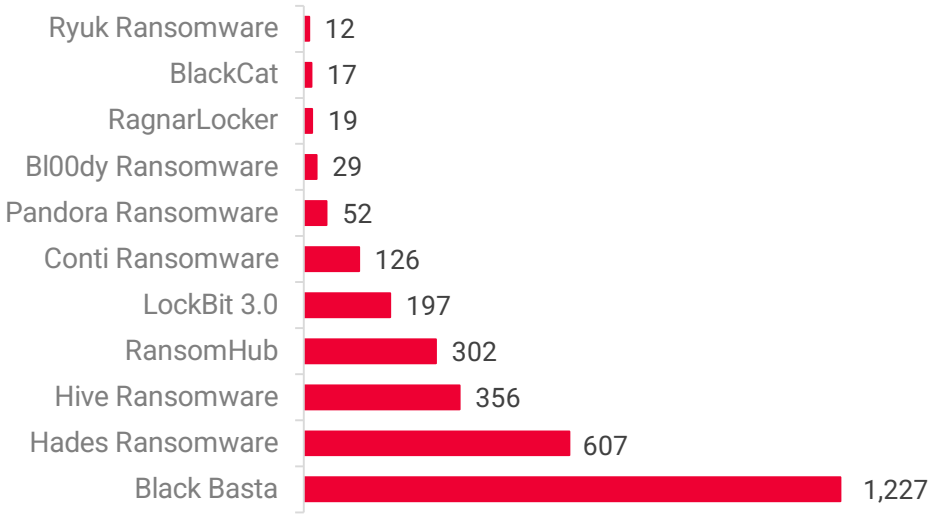
Bảng 1. Các vụ tấn công Ransomware nổi bật trong quý 1 năm 2025 được ghi nhận bởi Viettel Threat Intelligence

STT	Lĩnh vực	Nhóm tấn công	Số vụ	Thời gian tấn công
1	Y tế, Bán lẻ	Funksec	2	Tháng 01/2025
2	Năng lượng	Hunters	1	Tháng 01/2025
3	Sản xuất	RansomHub	1	Tháng 02/2025
4	Công nghệ	Fog ransomware	1	Tháng 03/2025

Nguồn: Viettel Threat Intelligence

Dưới đây là danh sách các Ransomware có nhiều kết nối tới trong quý 1 năm 2025:

Hình 1: Các Ransomware có số lượng IP kết nối đến nhiều nhất trong quý 1 năm 2025



Nguồn: Viettel Threat Intelligence

1. Các dòng mã độc

Theo ghi nhận của Viettel Threat Intelligence, gần đây tại Việt Nam, các nhóm APT có xu hướng sử dụng Ransomware trong các vụ tấn công để tối ưu hóa lợi nhuận. Việc sử dụng Ransomware vào giai đoạn cuối của các cuộc tấn công không chỉ làm gia tăng thiệt hại đối với nạn nhân mà còn giúp các nhóm tin tặc thu được số tiền lớn. Bên cạnh đó, chúng còn có thể bán dữ liệu của nạn nhân cho các bên thứ ba để thu lợi thêm.

Dưới đây là danh sách các nhóm Ransomware hoạt động mạnh trong quý 1 năm 2025 theo Viettel Threat Intelligence ghi nhận:

Bảng 2. Nhóm Ransomware hoạt động mạnh trong quý 1 năm 2025 theo Viettel Threat Intelligence

STT	Tên nhóm	Mô tả	Đối tượng ảnh hưởng
1	Lockbit	Hoạt động theo mô hình Ransomware-as-a Service (RaaS). Theo thông tin ghi nhận, nhóm đã phát hành phiên bản mới nhất Lockbit 3.0.	Doanh nghiệp & Tổ chức
2	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.	Các tổ chức trong lĩnh vực giáo dục
3	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.	Công nghiệp
4	Medusa	Hoạt động theo mô hình Ransomware-as-a Service (RaaS). Theo ghi nhận đã có hơn 40 nạn nhân trong 3 tháng đầu năm 2025.	Người dùng Windows
5	RansomHub	Hoạt động theo mô hình Ransomware-as-a Service (RaaS). Thường nhắm vào tổ chức lớn có khả năng trả tiền chuộc cao.	Doanh nghiệp & Tổ chức

**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

Mã độc RAT (Remote Access Trojan)

Trong 3 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 quý 1 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.

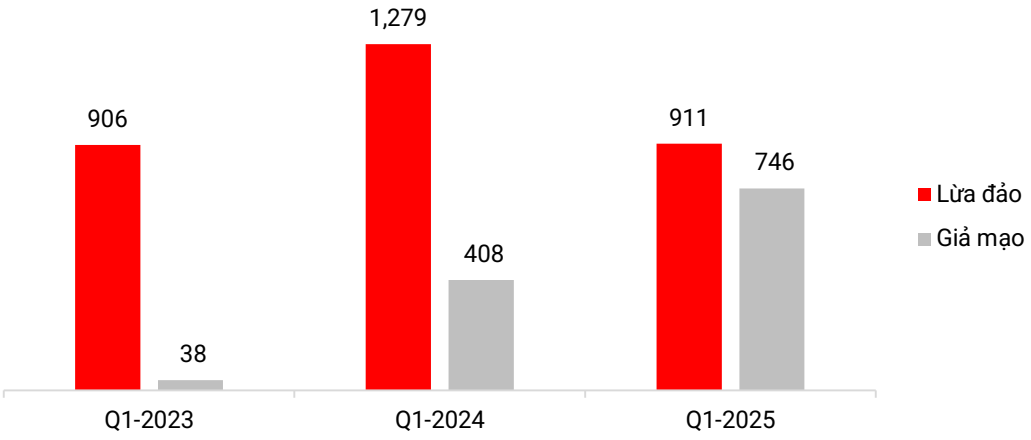
**Nguồn: Viettel Threat Intelligence*

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 quý 1 năm 2025 đã ghi nhận **911** tên miền lừa đảo nhắm vào người dùng, khách hàng của các tổ chức lớn tại Việt Nam. Số lượng tên miền lừa đảo **giảm 28.8%** so với quý 1 năm 2024, tuy nhiên, số lượng trang giả mạo **tăng 82.8%**, cho thấy xu hướng chung của tấn công lạm dụng thương hiệu vẫn có dấu hiệu gia tăng.

Viettel Threat Intelligence ghi nhận sự dịch chuyển mục tiêu của các nhóm lừa đảo, 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 **Năng lượng** và **Vận tải** cho thấy rằng các hình thức lừa đảo đang ngày càng phức tạp và tinh vi, không bó hẹp phạm vi nạn nhân.

Ngoài ra, Viettel Threat Intelligence cũng đã phát hiện và cảnh báo **746** trang giả mạo, sử dụng trái phép thương hiệu của các tổ chức, doanh nghiệp tại Việt Nam, **tăng gần 83%** so với quý 1 năm 2024. Điều này đặt ra những vấn đề cấp bách và thiết yếu liên quan đến công tác bảo vệ thương hiệu đối với các tổ chức, doanh nghiệp tại Việt Nam. Các doanh nghiệp cần chú trọng hơn trong việc xây dựng và duy trì hình ảnh thương hiệu, đồng thời triển khai các biện pháp bảo vệ hiệu quả để tránh các tổn thất về uy tín và giá trị thương hiệu.

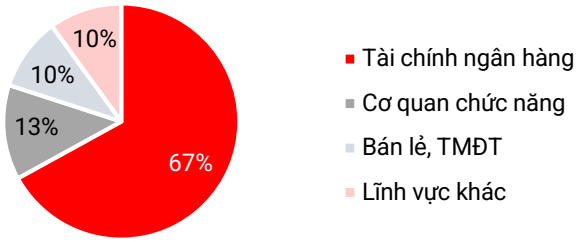
Về mặt hình thức, trong quý 1 năm 2025, Viettel Threat Intelligence không ghi nhận các hình thức lừa đảo mới xuất hiện. Thay vào đó, việc các nhóm tội phạm sử dụng những dữ liệu lộ lọt được rao bán, trao đổi trên diễn đàn DarkWeb, cùng với việc áp dụng công nghệ AI (như AI tạo kịch bản lừa đảo, sử dụng DeepFake/DeepVoice,...) trong các chiến dịch lừa đảo cho thấy một sự chuyển biến mạnh mẽ trong phương thức hoạt động của tội phạm. 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.

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 67% tổng số các cuộc tấn công.

Bảng 4. Một số chiến dịch tấn công lừa đảo, giả mạo tiêu biểu được Viettel Threat Intelligence ghi nhận trong quý 1 năm 2025

Chiến dịch	Mô tả	Ảnh hưởng
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 ngân hàng
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, ngân hàng
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 lừa đảo, 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 nhằm chiếm đoạt tài sản của nạn nhân.	Người dùng ngân hàng
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, thực chất là lừa đảo chiếm đoạt tài sản.	Người dùng các ứng dụng nộp tiền điện
Giả mạo cơ quan chức năng để lừa người dùng cài đặt ứng dụng Android độc hại	Kẻ tấn công 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 dịch vụ công
Mạo danh công chức thuế	Kẻ tấn công 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
Mời chào khuyến mãi Tết	Lợi dụng thời điểm nhu cầu mua sắm và đi lại tăng cao. Kẻ tấn công 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.	Người dân
Lừa đảo thông qua hình thức báo lỗi tài khoản	Kẻ tấn công thu thập thông tin cá nhân và tài khoản ngân hàng của người dùng thông qua chợ đen giao dịch dữ liệu hoặc những thông tin bị lộ trên mạng xã hội. Kẻ tấn công sẽ cố tình làm vô hiệu hoá tài khoản bằng cách nhập sai mật khẩu nhiều lần, sau đó kẻ tấn công sẽ giả mạo nhân viên ngân hàng để hướng dẫn người dùng cài đặt ứng dụng độc hại hoặc quét QR chứa đường dẫn độc hại.	Người dùng ngân hàng

Nguồn: Viettel Threat Intelligence

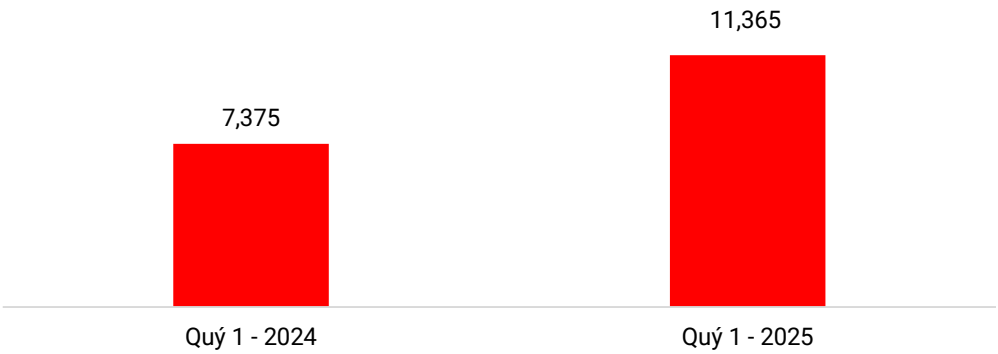
3. Tình hình lỗ hổng bảo mật

Viettel Threat Intelligence đã **cảnh báo chi tiết về 36 lỗ hổng bảo mật** trong các sản phẩm, phần mềm phổ biến được công bố trong quý 1 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: **Oracle WebLogic Server** (CVE-2023-21931 và CVE-2023-21839), **FortiNAC** (CVE-2022-39952), **Apache Log4j** (CVE-2021-44228),... 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 quý 1 năm 2025

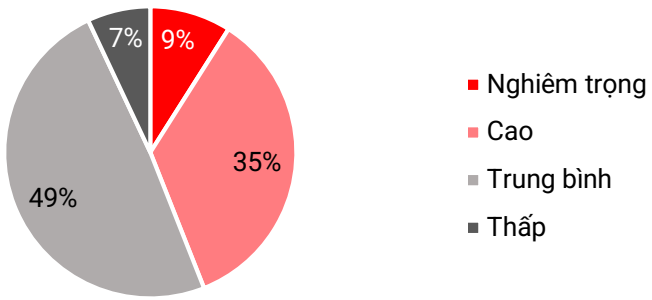
Hình 4: Số lượng lỗ hổng mới xuất hiện trong quý 1 năm 2024 và quý 1 năm 2025



Nguồn: Viettel Threat Intelligence

Trong quý 1 năm 2025, số lượng lỗ hổng ghi nhận trên thế giới đã **tăng 54.1%** so với cùng kỳ năm 2024. Số lượng lỗ hổng gia tăng theo từng năm cho thấy xu hướng phát triển nhanh chóng của công nghệ và sự mở rộng của bề mặt tấn công từ các sản phẩm trong môi trường doanh nghiệp.

Hình 5: Tỉ lệ lỗ hổng trong quý 1 năm 2025 theo mức độ



Nguồn: Viettel Threat Intelligence

Các lỗ hổng mức **Cao** và **Trung bình** (theo hệ thống chấm điểm phổ biến – CVSS 3.0) chiếm tỉ trọng lớn nhất với lần lượt là **35%** và **49%**. Trong khi đó, số lượng lỗ hổng mức **Nghiêm trọng** mặc dù chỉ chiếm **9%** nhưng các lỗ hổng này thường xuyên được các nhóm tin tặc sử dụng trong 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 đưa ra **36** phân tích chi tiết liên quan đến lỗ hổng bảo mật trong quý 1 năm 2025 có nguy cơ 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	2
Cao	10
Trung bình	23
Thấp	1

**Nguồn: Viettel Threat Intelligence*

Bảng 5. Danh sách 12 lỗ hổng nổi bật trong quý 1 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
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-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
4	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

3. Tình hình lỗ hổng bảo mật

Bảng 5 (tiếp). Danh sách 12 lỗ hổng nổi bật trong quý 1 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-2024-21182	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 lợi dụng lỗ hổng này để thực thi mã tùy ý trên máy chủ thông qua giao thức T3, IIOP.	Cao
6	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 thành công, tin tặc có thể tải tệp lên hệ thống và thực thi mã từ xa.	Cao
7	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
8	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
9	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
10	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 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
11	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
12	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

**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 quý 1 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 quý 1 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 quý 1 năm 2025

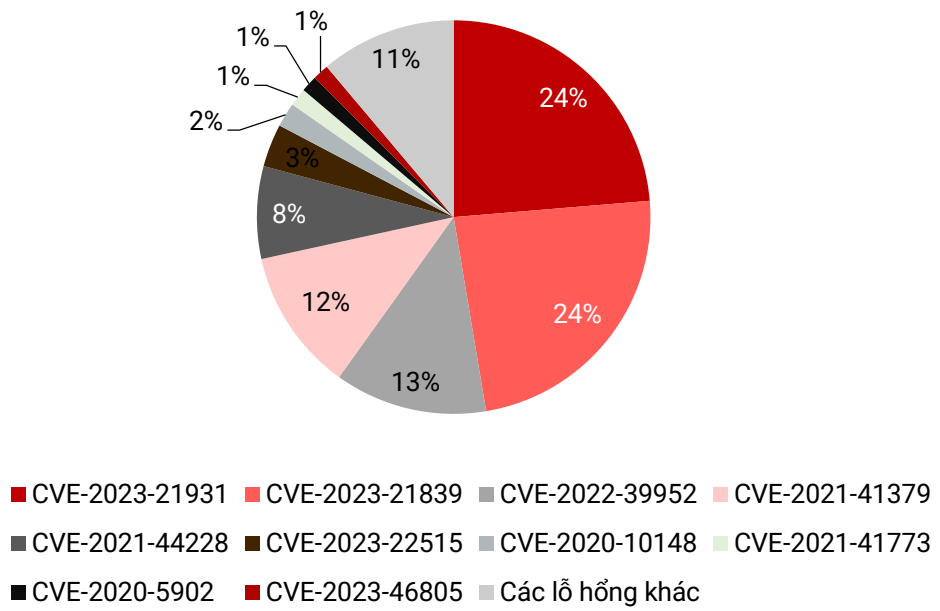
STT	Tên lỗ hổng	Thông tin chung	Mức độ đánh giá của Viettel Threat Intelligence
1	CVE-2023-21931 và CVE-2023-21839	Nguy cơ khai thác lỗ hổng CVE-2023-21931 và CVE-2023-21839 trên Oracle WebLogic Server, máy chủ ứng dụng hàng đầu trên nền tảng Java: Nguyên nhân của lỗ hổng là do máy chủ không xử lý an toàn khi deserialize dự 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-2021-41379	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
4	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

**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 trong quý 1 năm 2025



Nguồn: Viettel Threat Intelligence

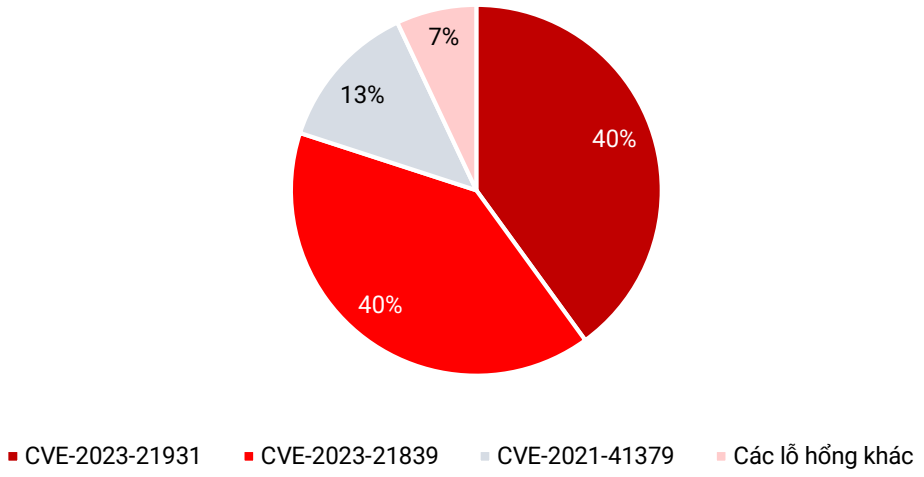
Nhìn vào các biểu đồ trên có thể thấy các lỗ hổng được các nhóm tấn công sử dụng trong thực tế để rà quét và khai thác trên các hệ thống của các tổ chức trong quý 1 năm 2025 có thể kể đến là: **CVE-2023-21931 và CVE-2023-21839** (Lỗ hổng thực thi mã tùy ý trên Oracle WebLogic Server), **CVE-2022-39952** (Lỗ hổng thực thi mã từ xa trên FortiNAC), **CVE-2021-41379** (Lỗ hổng leo thang đặc quyền trên Microsoft Windows), **CVE-2021-44228** (lỗ hổng thực thi mã từ xa trên Apache Log4j),... 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 kẻ tấn công 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

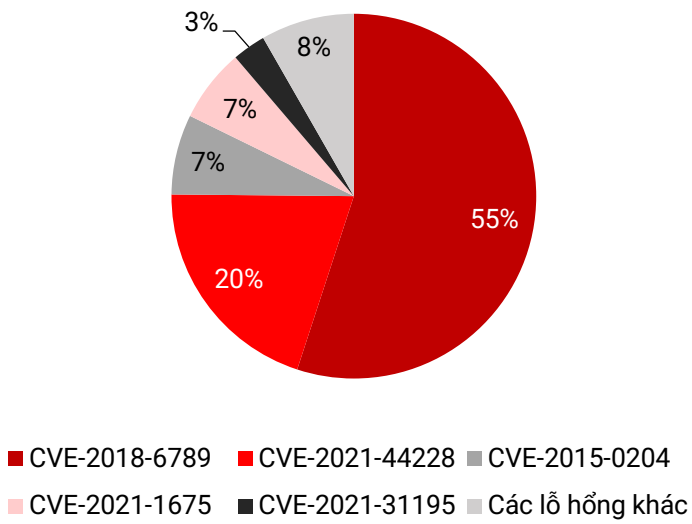
Dưới đây là tỉ lệ lỗ hổng bị khai thác theo lĩnh vực trong quý 1 năm 2025:

Hình 7: Thống kê tỉ lệ các lỗ hổng được sử dụng để rà quét, khai thác trong thực tế tại Việt Nam theo lĩnh vực Tài chính - Ngân hàng trong quý 1 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 tại Việt Nam theo lĩnh vực Năng lượng trong quý 1 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 quý 1 năm 2025, hệ thống Viettel Anti-DDoS đã ghi nhận **hơn 257,000** cuộc tấn công từ chối dịch vụ phân tán (DDoS). Đáng chú ý, **hơn 41%** số cuộc tấn công tập trung vào tháng 1. Cũng trong khoảng cuối tháng 1 - đầu tháng 2, các cuộc tấn công DDoS dạng Hit-and-Run đã có sự gia tăng, chủ yếu nhắm vào các doanh nghiệp thuộc khối **Tài chính**. Các cuộc tấn công DDoS với cường độ băng thông cao vẫn luôn là mối lo ngại lớn, và trong 3 tháng đầu năm 2025, đã xuất hiện các cuộc tấn công DDoS với cường độ băng thông **đạt đỉnh lên tới gần 800Gbps** với mục tiêu là các doanh nghiệp thuộc lĩnh vực **Công nghệ thông tin**. Ngoài ra, các doanh nghiệp, tập đoàn thuộc các lĩnh vực như **Dịch vụ giải trí điện tử, Giáo dục, Cơ quan chức năng** vẫn thường xuyên bị nhắm mục tiêu, thể hiện sự phân bổ rộng rãi và không phân biệt lĩnh vực trong chiến lược của các nhóm tấn công.

Số lượng tấn công DDoS có xu hướng giảm dần

Hình 9: Số lượng các cuộc tấn công DDoS theo cùng kỳ năm 2024 và năm 2025

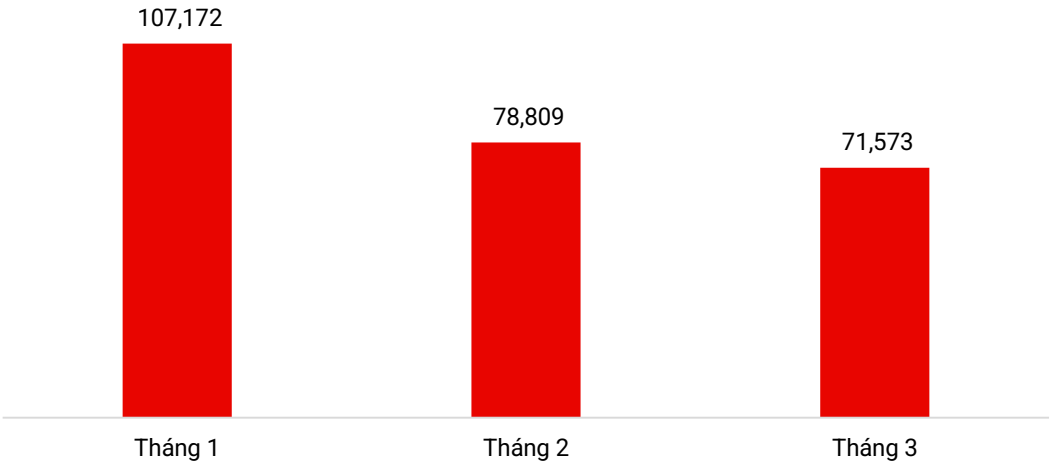
Ở quý 1 năm 2025, số lượng các cuộc tấn công DDoS có sự **sụt giảm** so với cùng kỳ năm 2024 khi số cuộc tấn công đã giảm đi hơn 100 nghìn cuộc, tương đương 30%.

Nguyên nhân dẫn tới sự suy giảm về số lượng tấn công là do **sự thay đổi về cách thức tấn công và độ phức tạp của cuộc tấn công**. Trong quý 1 năm 2024, tin tặc liên tục sử dụng đa dạng các kiểu tấn công DDoS và thay đổi luân phiên các tấn công dạng Hit-and-Run và CarpetBomb nhằm cố gắng bypass các cơ chế bảo vệ. Đặc trưng của các kiểu tấn công trên là tạo nên số lượng lớn các cuộc tấn công với cường độ tối thiểu nhằm vượt qua các cơ chế bảo vệ tấn công dựa theo ngưỡng cứng. Với dạng tấn công Hit-and-Run, các cuộc tấn công nhỏ lẻ được thực hiện trong một khoảng thời gian ngắn rồi dừng lại 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. Còn với dạng CarpetBomb, các cuộc tấn công nhỏ lẻ cũng được sử dụng, tuy nhiên mục tiêu sẽ là toàn bộ một dải IP dịch vụ của hệ thống. Cường độ tấn công vào mỗi IP có thể bé, nhưng tổng dung lượng tấn công vào toàn bộ dải IP sẽ lên tới hàng chục, thậm chí hàng trăm Gbps.

Còn đối với quý 1 năm 2025, dạng tấn công DDoS Carpet Bomb không được ghi nhận, thay vào đó, chỉ có sự xuất hiện của dạng tấn công **Hit-and-Run**. Đây cũng là một dạng tấn công sinh ra nhiều cuộc tấn công nhỏ lẻ. Mặc dù số lượng cuộc tấn công suy giảm, mức độ tinh vi và ảnh hưởng thực tế lại gia tăng. Đặc biệt, các chiến dịch tấn công dạng DNS Hit-and-Run 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 "tấn công chất lượng".

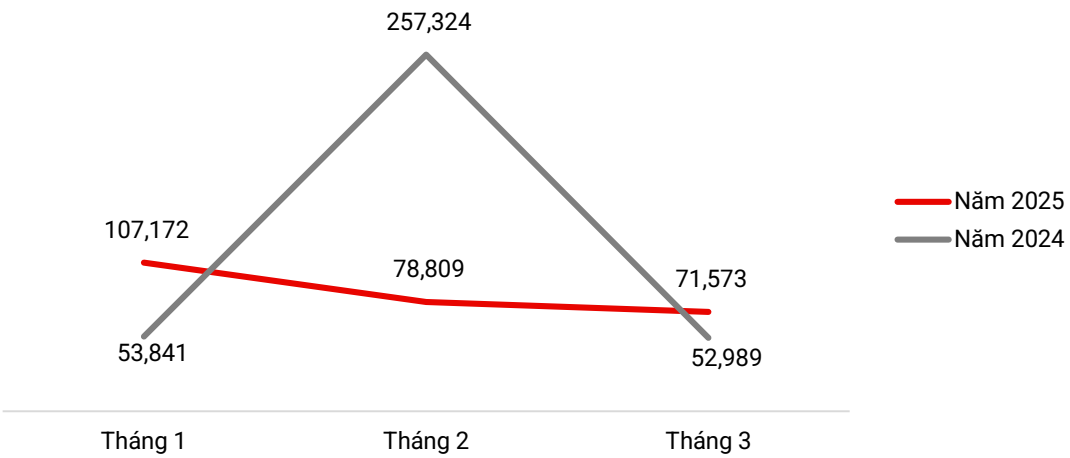
4. Tấn công từ chối dịch vụ phân tán (DDoS)

Hình 10: Số lượng các cuộc tấn công DDoS theo tháng trong quý 1 năm 2025



Cụ thể theo tháng, số lượng tấn công DDoS tập trung chủ yếu trong tháng 1, ngay trong và sau thời điểm dịp Tết Nguyên Đán, chiếm hơn 40% tổng số cuộc tấn công trong quý. Sau đó, số lượng các cuộc tấn công DDoS giảm dần về cuối quý.

Hình 11: So sánh số lượng các cuộc tấn công DDoS qua các tháng trong quý 1 năm 2024 và quý 1 năm 2025

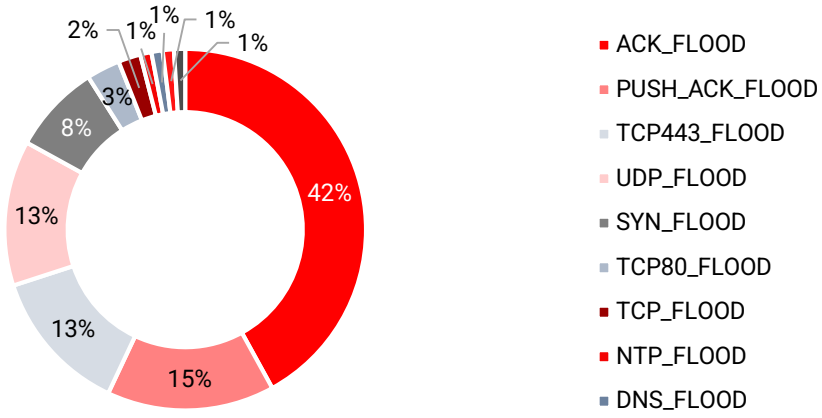


So sánh sâu thêm giữa các tháng cùng kỳ năm 2024 và năm 2025, có thể thấy các cuộc tấn công trong quý 1 năm 2025 có sự dàn trải đều hơn so với năm ngoái. Trong quý 1 năm ngoái, các cuộc tấn công tập trung nhiều nhất vào tháng 2 - là tháng đã ghi nhận sự gia tăng đột biến các cuộc tấn công DDoS của cả 2 dạng Hit-and-Run và Carpet Bomb.

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

Tỷ trọng xuất hiện các kiểu tấn công DDoS

Hình 12: Tỷ trọng các loại tấn công DDoS trong quý 1 năm 2025



Các kỹ thuật được sử dụng trong các chiến dịch DDoS ngày càng đa dạng, chủ yếu bao gồm:

- **UDP Flood/TCP SYN Flood:** Tấn công bão hòa băng thông làm quá tải máy chủ xử lý kết nối.
- **DNS Amplification:** Lợi dụng hệ thống máy chủ DNS mở để khuếch đại dữ liệu, tạo ra lưu lượng tấn công lớn.
- **Traffic Bursting/Hit-and-Run:** Tạo ra các đợt tấn công ngắn, mạnh và liên tục, khiến hệ thống phản ứng không kịp, làm gián đoạn tạm thời dịch vụ.
- **HTTP Flood thông minh:** Nhắm vào tầng ứng dụng với các yêu cầu có cấu trúc tương tự người dùng thực, gây khó khăn cho hệ thống lọc và phân biệt.

Đặc biệt, chiến thuật **Hit-and-Run** (như đã đề cập ở trên) ghi nhận xu hướng gia tăng, với nhiều đợt tấn công lặp đi lặp lại, kéo dài vài phút đến vài chục phút mỗi lần, nhưng gây gián đoạn dịch vụ tại các khung giờ cao điểm.

Số lượng cuộc tấn công DDoS **lợi dụng bộ giao thức TCP** vẫn luôn đứng đầu theo phương thức tấn công, chiếm tới hơn 80% tổng số cuộc tấn công trong quý. Đây là những cuộc tấn công lợi dụng các cờ trong bộ giao thức TCP/IP như ACK, SYN-ACK hay phổ biến nhất là cờ SYN. Các cuộc tấn công này dễ dàng làm treo hoặc sập các thiết bị như tường lửa, thiết bị phân tải,... đứng trung gian giữa tin tặc và mục tiêu bằng cách làm cao tải tài nguyên thiết bị như CPU, RAM hay gây tràn bảng session khiến tính sẵn sàng của dịch vụ bị ảnh hưởng.

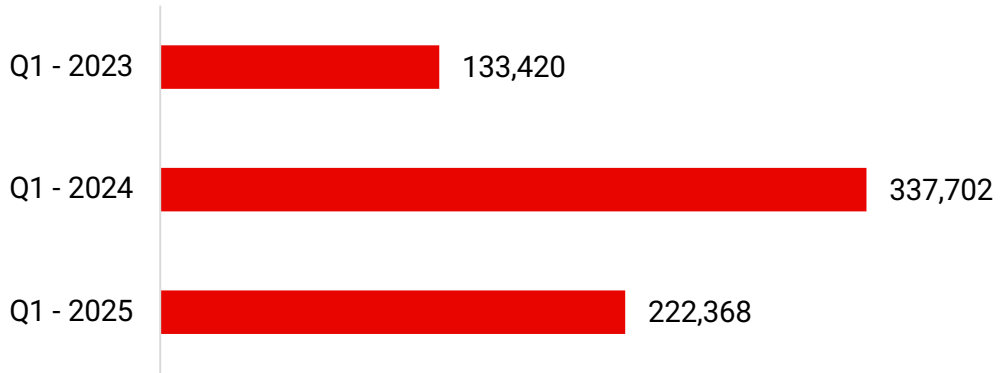
Bên cạnh giao thức TCP, các cuộc tấn công **lợi dụng giao thức UDP** cũng luôn là vector tấn công phổ biến và dễ thực thi. Điển hình là tấn công DDoS UDP Flood sẽ tạo ra một luồng băng thông tấn công cực lớn, dễ dàng gây nghẽn băng thông uplink của các doanh nghiệp, từ đó gây ảnh hưởng tới hạ tầng cũng như các dịch vụ của hệ thống mục tiêu. Đặc biệt, bằng cách khai thác các máy chủ trung gian như máy chủ DNS hay máy chủ NTP, tin tặc hoàn toàn có thể tạo nên các cuộc tấn công tràn băng thông với quy mô lên tới hàng trăm Gbps, mà vẫn có thể che giấu nguồn gốc tấn công.

Ngoài sự xuất hiện vốn có của các tấn công kiểu DNS Flood và DNS Amplification, hệ thống Viettel Anti-DDoS ghi nhận cả sự xuất hiện tấn công DDoS **DNS Recursive Attack**, kiểu tấn công này gây ảnh hưởng tới dịch vụ DNS của mục tiêu, gián tiếp gây cao tải các thành phần mạng trung gian như tường lửa hay thậm chí chính máy chủ DNS. Do lợi dụng các máy chủ DNS public internet làm bàn đạp, nên các nguồn của các truy vấn DNS đều là từ các IP thật, từ đó sẽ gây ra thách thức lớn trong quá trình bảo vệ hệ thống khỏi tấn công dạng này. Nhiều tổ chức thuộc lĩnh vực Tài chính đã ghi nhận bị tấn công bởi kiểu tấn công DDoS trên trong khoảng cuối tháng 1, đầu tháng 2 năm 2025.

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

Cường độ tấn công DDoS

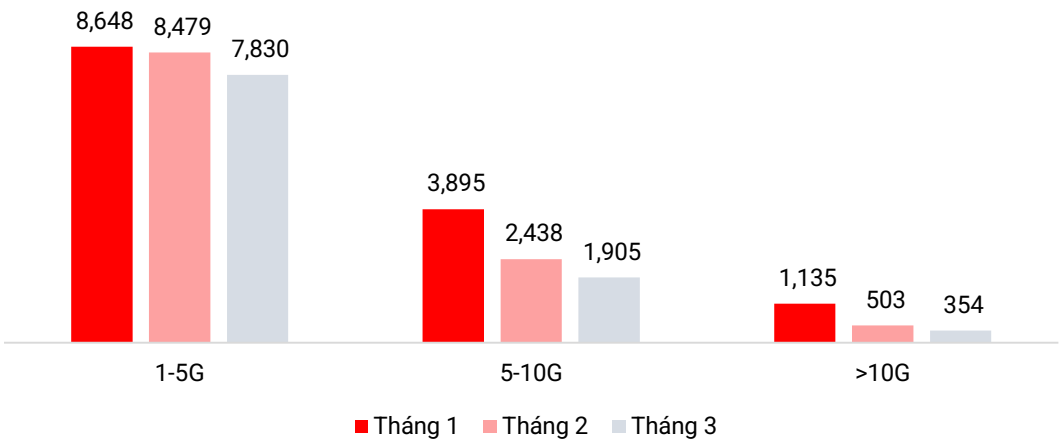
Hình 13: Số lượng các cuộc tấn công có cường độ <1Gbps theo cùng kỳ 3 năm gần đây



Đối với các cuộc tấn công dưới 1Gbps, trong quý 1 năm 2025 đã có sự suy giảm về số lượng tấn công. Nguyên nhân như đã trình bày ở mục trên, các cuộc tấn công DDoS dạng Hit-and-Run hay Carpet Bomb, thậm chí tấn công DDoS DNS Recursive đã ghi nhận xuất hiện nhiều và tăng cao trong quý 1 năm 2024. Tới quý 1 năm 2025, số lượng các cuộc tấn công dạng Hit-and-Run đã giảm và không ghi nhận thêm sự xuất hiện tấn công DDoS dạng Carpet Bomb, các cuộc tấn công DDoS DNS Recursive cũng xuất hiện với tấn suất thấp hơn.

Nhìn xa từ quý 1 năm 2023, có thể thấy do chưa có sự xuất hiện của các kiểu tấn công DDoS dạng nhỏ lẻ trên nên số lượng các cuộc tấn công DDoS dưới 1Gbps thấp hơn nhiều so với cùng kỳ 2 năm gần đây.

Hình 14: Số lượng các cuộc tấn công DDoS theo cường độ qua từng tháng trong quý 1 năm 2025



Các cuộc tấn công DDoS từ 1 – 5Gbps vẫn chiếm số lượng chủ đạo khi chiếm tới hơn 70% tổng số các cuộc tấn công có cường độ lớn hơn 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). Càng về cuối quý, số lượng các cuộc tấn công DDoS cường độ cao có dấu hiệu giảm dần.

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

Trong quý 1 năm 2025, nhiều cuộc tấn công DDoS cường độ cực lớn đã được hệ thống Viettel AntiDDoS ghi nhận, riêng trong tháng 1 đã xuất hiện 2 cuộc tấn công DDoS đứng đầu về cường độ băng thông (đạt gần 700Gbps và 800Gbps). Các cuộc tấn công này có điểm chung là đều lợi dụng giao thức UDP để tạo ra cuộc tấn công DDoS quy mô lớn. Một số 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
2025-02-06 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
2025-02-18 21:59:13	[redacted]	udp	270	UDP_FLOOD, WSD, Teardrop	222.16Gb	19.56Mpps
2025-02-18 22:01:49	[redacted]	udp	102	UDP_FLOOD	222.16Gb	19.56Mpps
2025-02-12 17:52:45	[redacted]	udp	126	UDP_FLOOD	187.23Gb	16.72Mpps

Hình 15. Hình ảnh thực tế một số cuộc tấn công DDoS có cường độ lớn trong quý 1 năm 2025 (nguồn: Viettel Anti-DDoS)

Có thể thấy số lượng tấn công DDoS trong quý 1 năm 2025 đã suy giảm nhẹ so với quý 1 năm 2024, tuy nhiên chất lượng các cuộc tấn công này ngày càng tăng và 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 gây ảnh hưởng tới trải nghiệm người dùng.

Tiếp theo là các kiểu tấn công DDoS lợi dụng DNS khai thác tài nguyên máy chủ DNS public trên Internet làm bàn đạp để khuếch đại tấn công, gây ảnh hưởng tới hạ tầng của mục tiêu. Bên cạnh đó, các cuộc tấn công DDoS DNS Recursive gây ảnh hưởng tới máy chủ DNS và 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. Với sự xuất hiện công nghệ IoT, tấn công DDoS khuếch đại (DDoS Amplification) băng thông sẽ trở thành công cụ mới cho 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.

Các kiểu tấn công trên thường được kết hợp với 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. Điều 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.

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

Trong quý 1 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 quý 1 năm 2025 phần lớn nhắm vào các tổ chức thuộc lĩnh vực **Tài chính, Công nghiệp, Dịch vụ công và Công nghệ**.

Trong quý 1 năm 2025, các nhóm tấn công có chủ đích đã nâng cấp thêm các 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. Các nhóm tấn công thường sử dụng kỹ thuật này để 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 quý 1 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 quý 1 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, trong đó có lĩnh vực Dịch vụ công tại Việt Nam.	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 đã hoạt động ít nhất từ 2012, tập trung vào thực hiện các chiến dịch gián điệp mạng.	Spearphishing Attachment, DLL Side Loading

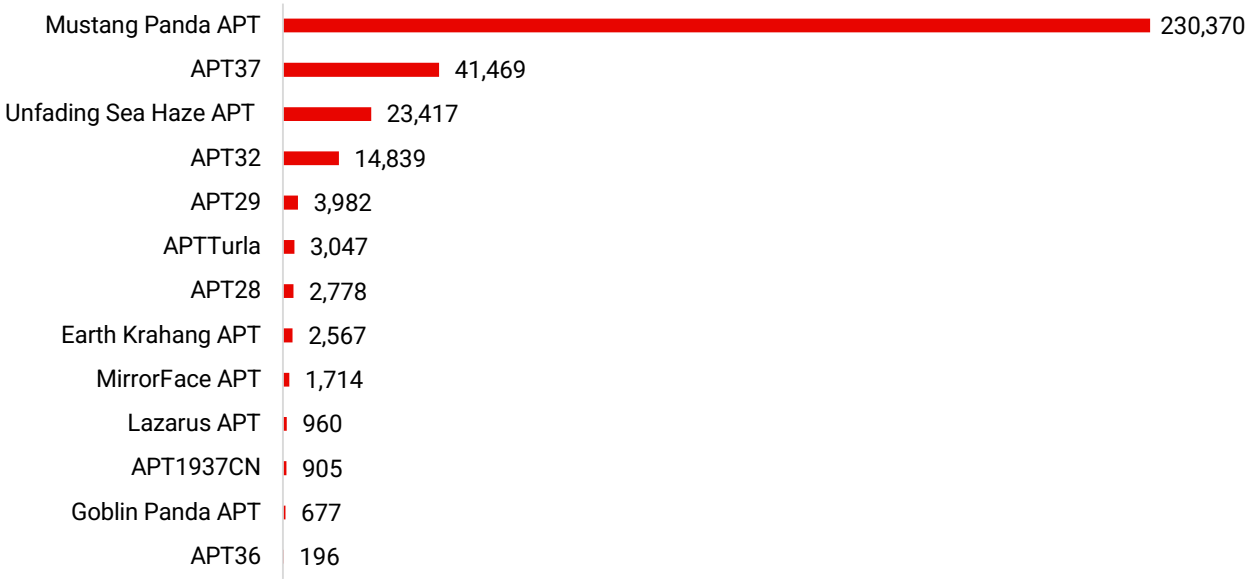
**Nguồn: Viettel Threat Intelligence*

*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: Phần 1, Phần 2, Phần 3.*

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

Dưới đây là danh sách các nhóm APT có số lượng IP tại Việt Nam được ghi nhận truy cập kết nối đến nhiều nhất trong quý 1 năm 2025 theo Viettel Threat Intelligence:

Hình 16: Số lượng IP kết nối tới các C&C APT



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 quý 1 năm 2025:

Bảng 9. Danh sách các chiến dịch tấn công có chủ đích nổi bật được Viettel Threat Intelligence ghi nhận trong quý 1 năm 2025

STT	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 nhằm mục tiêu vào nhiều công ty thuộc lĩnh vực công nghệ tại Đông Nam Á.	Công nghệ
Tháng 2/2025	Cảnh báo về chiến dịch tấn công của nhóm **Earth Preta (Mustang Panda APT)** nhằm 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) nhằm mục tiêu vào các tổ chức trong khu vực Châu Á - Thái Bình Dương.	Dịch vụ công
	Cảnh báo nhóm APT **Mustang Panda** nhằm 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; nhằm 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 quý 1 năm 2025

STT	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

**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/#/.*

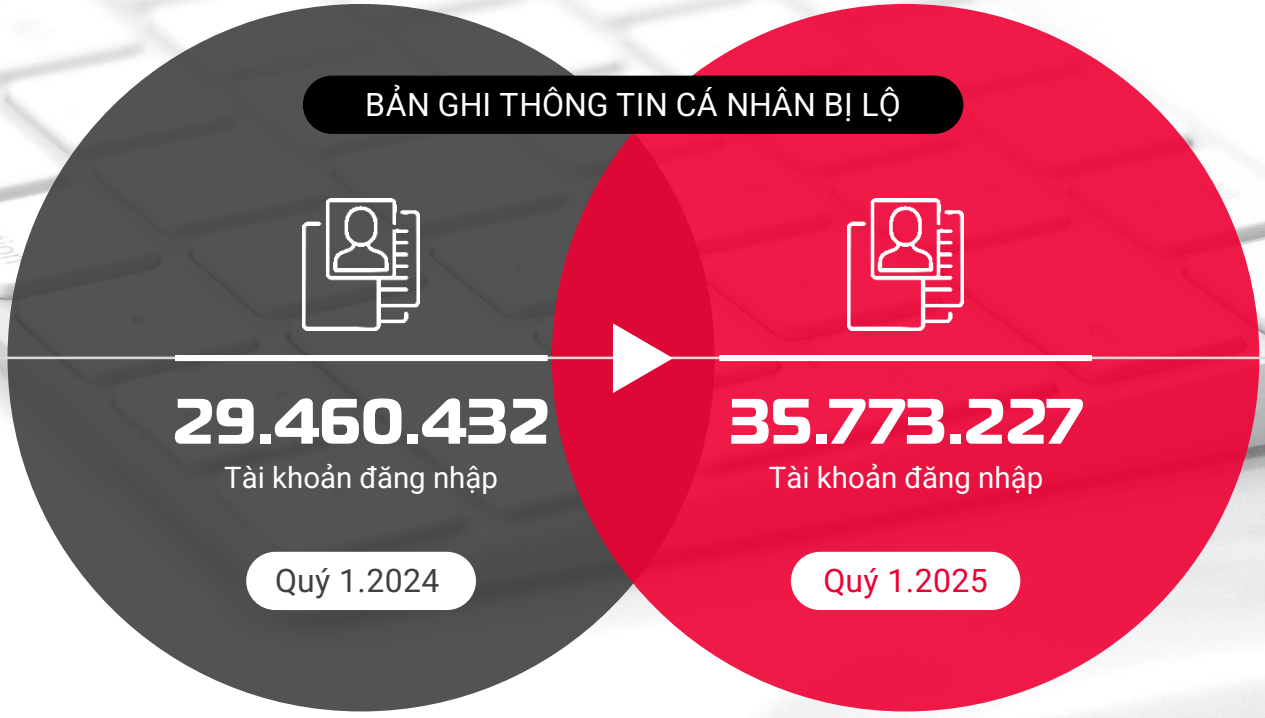
6. Lộ lọt, rò rỉ dữ liệu

Trong quý 1 năm 2025, Viettel Threat Intelligence ghi nhận số lượng **gần 36 triệu** thông tin tài khoản bị lộ lọt, **tăng khoảng 21.4%** so với quý 1 năm 2024. Trong đó, số lượng tài khoản lộ lọt tại Việt Nam là **hơn 4.5 triệu**, chiếm khoảng 12.6%. Sự phát triển của các nhóm tấn công đánh cắp mã độc, 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 quý 1 năm 2024 và quý 1 năm 2025:



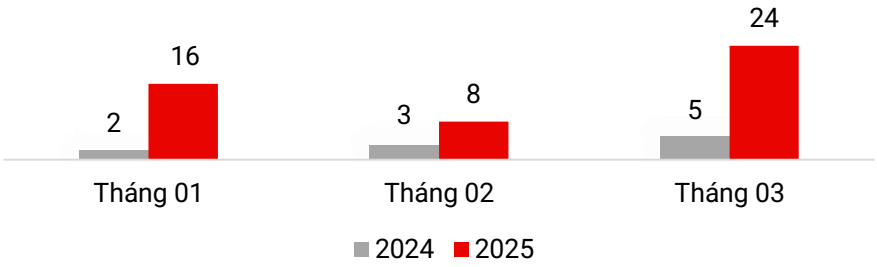
Nguồn: Viettel Threat Intelligence

Hình 17. Số lượng bản ghi thông tin tài khoản cá nhân lộ lọt quý 1 năm 2024 và quý 1 năm 2025

6. Lộ lọt, rò rỉ dữ liệu

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

Hình 18: Số lượng vụ lộ lọt dữ liệu tại Việt Nam theo tháng trong quý 1 năm 2024 và quý 1 năm 2025



Nguồn: Viettel Threat Intelligence

Trong quý 1 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 **48 vụ lộ lọt dữ liệu** với hơn **155 triệu bản ghi** và **24.65 GB dữ liệu**.

Có thể thấy, ngoại trừ tháng 02/2024 thì số lượng các vụ rao bán, chia sẻ dữ liệu nhạy cảm theo từng tháng trong quý 1 năm 2025 đều tăng đáng kể so với cùng kỳ năm 2024.

Dưới đây là danh sách các vụ lộ lọt, rao bán dữ liệu theo ngành trong quý 1 năm 2025:

Bảng 10. Danh sách các vụ lộ lọt dữ liệu nổi bật tại Việt Nam trong quý 1 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	8	1,860,322 bản ghi 246 MB 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	4	52,754 bản ghi 13.4 MB dữ liệu
3	Thông tin khách hàng, thông tin mua bán.	Bán lẻ	9	~ 520,000 bản ghi
4	Dữ liệu thông tin khách hàng, dữ liệu trích xuất từ hệ thống nội bộ.	Tài chính	1	~ 2,130,000 bản ghi
5	Dữ liệu thông tin khách hàng, dữ liệu trích xuất từ hệ thống nội bộ.	Bảo hiểm	1	~ 1,000,000 bản ghi
6	Thông tin khách hàng, dữ liệu trích xuất từ hệ thống nội bộ.	Năng lượng	2	~ 63,000,000 bản ghi 4.5 GB dữ liệu
7	Thông tin cá nhân, thông tin eKYC.	Khác	13	83,552,443 bản ghi 19.8 GB dữ liệu
8	Thông tin của khách hàng, thông tin sử dụng dịch vụ.	Dịch vụ	1	81,612 bản ghi 53.4 MB dữ liệu
9	Thông tin người dùng, thông tin trích xuất từ hệ thống nội bộ.	Dịch vụ công	1	44,083 bản ghi 44.7 MB dữ liệu
10	Thông tin về máy chủ hệ thống, thông tin của khách hàng.	Giải trí	2	~100,000 bản ghi
11	Thông tin của khách hàng, thông tin giao dịch.	Ngân hàng	3	~ 113,000 bản ghi
12	Thông tin khách hàng, thông tin trích xuất từ hệ thống nội bộ.	Tiện ích	1	~ 3,000,000 bản ghi
13	Thông tin khách hàng, thông tin trích xuất từ hệ thống nội bộ.	Y tế	1	4,453 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 quý 1 năm 2025, Viettel Threat Intelligence đã phát hiện nhiều trường hợp lộ lọt dữ liệu, trong đó có **11 trường hợp mức độ Cao** liên quan tới các lĩnh vực **Tài chính - Ngân hàng, Giao thông vận tải và Công nghệ**.

Dưới đây là danh sách các trường hợp lộ lọt do vô tình chia sẻ mã nguồn theo ngành trong quý 1 năm 2025:

Bảng 11. Các trường hợp lộ lọt dữ liệu do vô tình chia sẻ mã nguồn nổi bật trong quý 1 năm 2025

STT	Lĩnh vực	Số vụ	Chi tiết
1	Ngân hàng	6	Lộ lọt thông tin mã nguồn, bộ cài đặt có chứa thông tin tài khoản đăng nhập, khóa API nhạy cảm.
2	Công nghệ	2	Lộ lọt thông tin mã nguồn có chứa thông tin tài khoản đăng nhập các hệ thống nội bộ.
3	Tài chính - dịch vụ	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	1	Lộ lọt thông tin API chứa thông tin tài khoản đăng nhập các hệ thống dịch vụ.
5	Hàng không	1	Lộ lọt thông tin mã nguồn có chứa API nhạy cảm và các thông tin dịch vụ.

**Nguồn: Viettel Threat Intelligence*

Phần III.

PHỤ LỤC ĐÍNH KÈM

Chiến dịch tấn công mới của nhóm APT Lotus Blossom: Kỹ thuật Domain Fronting và lợi dụng hệ thống quản trị tập trung

Nhóm tấn công APT Lotus Blossom (còn được biết đến với tên DRAGONFISH, Spring Dragon, Lotus Panda) là một trong những nhóm tấn công có chủ đích (APT) nguy hiểm nhất đang hoạt động mạnh mẽ tại khu vực Đông Nam Á, đặc biệt là Việt Nam. 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.

Kể từ năm 2018 đến nay, tuy thông tin công khai về hoạt động của Lotus Blossom rất hạn chế, Viettel Threat Intelligence vẫn liên tục ghi nhận những hoạt động tích cực của Lotus Blossom tại Việt Nam.

Trong các chiến dịch gần đây, Lotus Blossom không chỉ dựa vào email phishing truyền thống, mà chuyển hướng sang khai thác tài khoản VPN bị rò rỉ, tận dụng các nền tảng OTT (Over-The-Top – các ứng dụng nhắn tin như Zalo, Telegram, Viber,...) để phát tán mã độc, và lợi dụng tính năng của các hệ thống quản trị CNTT như Active Directory, Endpoint Security Center để phát tán và duy trì sự hiện diện trong hệ thống của nạn nhân. Nhóm cũng sử dụng kỹ thuật Domain Fronting để che giấu hạ tầng điều khiển, giúp né tránh các giải pháp bảo mật truyền thống.

Các nguy cơ chính đối với tổ chức, doanh nghiệp:

- **Nguy cơ xâm nhập từ tài khoản VPN bị đánh cắp:** Nhiều tổ chức tại Việt Nam đã mở rộng quyền truy cập từ xa sau COVID-19 nhưng chưa kiểm soát chặt chẽ tài khoản VPN, tạo điều kiện cho tin tặc khai thác.
- **Lợi dụng hệ thống quản trị CNTT để phát tán mã độc:** Lotus Blossom có thể kiểm soát và sử dụng chính các công cụ bảo mật và quản trị nội bộ để phát tán mã độc, vượt qua các biện pháp phòng thủ thông thường.
- **Mã độc có khả năng ẩn mình trong hệ thống lâu dài:** Nhóm sử dụng các loại mã độc tinh vi như ShadowShell, SignLoader, Lotus Tunnel, có khả năng vô hiệu hóa phần mềm bảo mật và ẩn nấp trong các thư mục hệ thống hợp pháp.
- **Domain Fronting giúp che giấu hoạt động tấn công:** Nhóm lợi dụng các dịch vụ CDN (như Fastly) để ngụy trang lưu lượng độc hại, khiến các hệ thống giám sát an ninh mạng khó phát hiện.

Chiến dịch tấn công mới của nhóm APT Lotus Blossom: Kỹ thuật Domain Fronting và lợi dụng hệ thống quản trị tập trung

Các phát hiện chính

- **Phương thức xâm nhập:** Nhóm đã tận dụng các tài khoản VPN bị rò rỉ, thu thập thông qua các mã độc stealer hoặc các chiến dịch phishing trên các nền tảng OTT, thay vì sử dụng email phishing truyền thống. Phương thức này khai thác tối đa những điểm yếu từ việc gia tăng làm việc từ xa sau đại dịch COVID-19, khi nhiều tổ chức mở rộng truy cập VPN cho nhân viên.
- **Kỹ thuật phát tán và xâm nhập sâu:** Nhóm đã lợi dụng các công cụ quản trị tập trung như SMBExec và tính năng cài đặt từ xa của Endpoint Security Center để phát tán mã độc trong nội bộ mạng. Đồng thời, nhóm sử dụng kỹ thuật DLL sideloading, trong đó mã độc được che giấu dưới dạng file thực thi hợp pháp, để qua mặt các giải pháp bảo mật hiện có.
- **Các loại mã độc đặc trưng:**
    - **ShadowShell:** Mã độc này được triển khai ngay khi nhóm tấn công thâm nhập thành công vào hệ thống, với khả năng giải mã và thực thi shellcode.
    - **SignLoader:** Một mã độc tinh vi được thiết kế để tận dụng các lỗ hổng trong các giải pháp Endpoint Detection and Response (EDR), cho phép mã độc tồn tại trong thư mục và tiến trình hợp pháp mà không bị phát hiện.
    - **LotusTunnel:** Loại mã độc này được sử dụng để duy trì kết nối ẩn danh với máy chủ chỉ huy, sử dụng các kênh giao tiếp ngụy trang để đảm bảo duy trì quyền kiểm soát.
- **Kỹ thuật Domain Fronting:** Nhóm tấn công sử dụng kỹ thuật Domain Fronting để che giấu lưu lượng độc hại dưới dạng lưu lượng hợp pháp. Kỹ thuật này lợi dụng các nhà cung cấp dịch vụ CDN để làm cho các kết nối Command and Control (C&C) trông như đang tương tác với các tên miền uy tín, giúp nhóm tránh bị phát hiện bởi các giải pháp bảo mật truyền thống.

*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: Phần 1, Phần 2, Phần 3.*

viettel security

TRỤ SỞ CHÍNH TẠI HÀ NỘI
Tầng 41, Tòa Keangnam Landmark 72,
Đường Phạm Hùng, Quận Nam Từ Liêm, Hà Nội

VĂN PHÒNG MIỀN NAM
Tầng 28A2, Tòa nhà Viettel, 285 đường Cách Mạng Tháng Tám,
Phường 12, Quận 10, Hồ Chí Minh

CONTACT US
(+84) 971 360 360
vcs.sales@viettel.com.vn
www.viettelcybersecurity.com