viettel
TI

BÁO CÁO TÌNH HÌNH NGUY CƠ ATTT TẠI VIỆT NAM ẢNH HƯỞNG TỚI

LĨNH VỰC SẢN XUẤT, BÁN LẺ, GIÁO DỤC, TÀI CHÍNH-NGÂN HÀNG

• Năm 2023 •

MỤC LỤC

A. Tổng quan

B. Chi tiết từng lĩnh vực

A. Tổng quan

1. Nhận định chung:

Trong năm 2023, VCS-Threat Intelligence đã ghi nhận nhiều nguy cơ mới xuất hiện tại Việt Nam có ảnh hưởng tới các tổ chức, doanh nghiệp thuộc lĩnh vực sản xuất, bán lẻ, giáo dục, tài chính ngân hàng. Một số nguy cơ nổi bật như sau:

ĐỘC QUYỀN VCS – THREAT INTELLIGENCE

Số lượng tài khoản bị xâm nhập và đánh cắp

10,552	26,654	11,642	30,412
(bán lẻ)	(sản xuất)	(giáo dục)	(tài chính-ngân hàng)

200% (so với 2022)

Có nguy cơ gây thiệt hại lên tới **16.5 tỷ đồng**

Tên miền lừa đảo, giả mạo thương hiệu các doanh nghiệp, tổ chức được sử dụng trong các chiến dịch lừa đảo người dùng cá nhân.

~5,800
(Tên miền)
Thuộc lĩnh vực bán lẻ, tài chính ngân hàng

126 ↑ 58% (so với 2022)

Chiến dịch tấn công

mục đích xâm nhập, tống tiền, theo dõi đánh cắp thông tin.

- 793 dấu hiệu nhận biết chưa từng được ghi nhận.
- 7 chiến dịch lừa đảo lớn lợi dụng thương hiệu của doanh nghiệp, tổ chức
- 3 chiến dịch tấn công sử dụng các tài liệu, ứng dụng giả mạo cơ quan chức năng

ĐỘC QUYỀN TẠI VIỆT NAM

23 **Vụ lộ lọt dữ liệu do bị tấn công và rao bán thông tin**

Bùng nổ của việc rao bán thông tin người dùng cùng với dữ liệu hệ thống cùng nhiều dữ liệu nhạy cảm của các doanh nghiệp trong lĩnh vực sản xuất và bán lẻ, giáo dục tài chính-ngân hàng tại Việt Nam

vi phạm Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân

5 vụ tấn công ransomware

Ghi nhận 5 vụ tấn công ransomware trong lĩnh vực bán lẻ, sản xuất với hơn 200 GB bị mã hóa với số tiền chuộc lên đến gần 4 tỷ đồng

16 Lỗ hổng

Được sử dụng khai thác tấn công vào tổ chức, doanh nghiệp trong năm 2023

698 Cuộc tấn công DDoS >5Gps

→ Có thể gây gián đoạn dịch vụ 3000 phút

2. Khuyến nghị:

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

- 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.
- Cảnh báo sớm cho khách hàng cá nhân về các tài khoản ngân hàng bị lộ lọt, các chiến dịch lừa đảo người dùng.
- 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.
- Rà soát, nâng cấp phiên bản các phần mềm, ứng dụng có chứa các lỗ hổng bảo mật nghiêm trọng.

B. Chi tiết từng lĩnh vực

1. Rao bán, lộ lọt dữ liệu

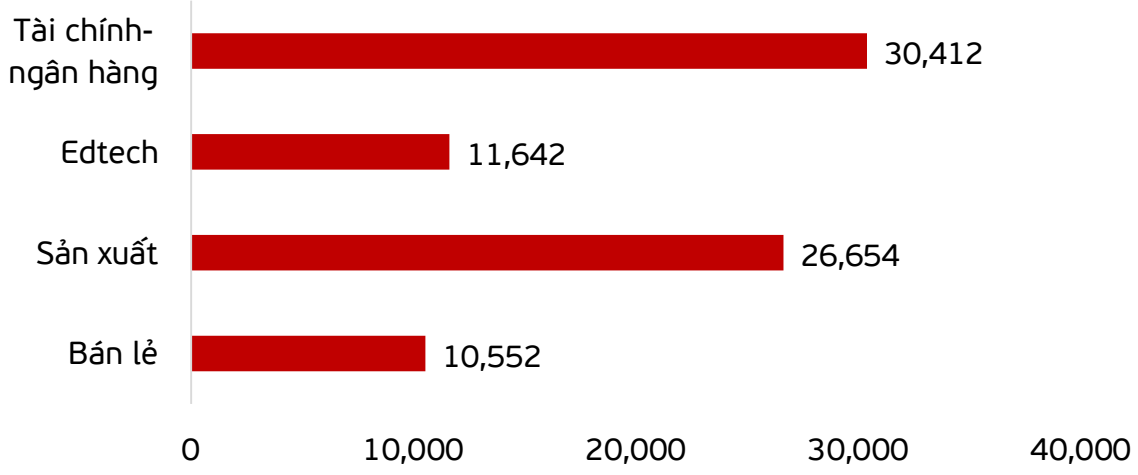
Lộ lọt do mã độc đánh cắp thông tin

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.

Dạng lộ lọt này cũng là một đòn đẩy giúp kẻ tấn công truy cập trái phép, trích xuất dữ liệu từ đó mang đi rao bán. Xu hướng mới này được mô tả chi tiết như sau: khi kẻ tấn công sử dụng các tài khoản bị đánh cắp để thực hiện xâm nhập trái phép và 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 hacker tin rằng có đủ khả năng chi trả để xử lý các nguy cơ khủng hoảng truyền thông.

Số lượng tài khoản lộ lọt liên quan đến nhóm ngành



(Danh sách chi tiết các tài khoản bị lộ lọt xem tại https://platform.cyberintel.io hoặc thư điện tử cảnh báo của VCS-Threat Intelligence)

❖ VCS-Threat Intelligence nhận định:

- Số lượng tài khoản lộ lọt của khách hàng cá nhân các ngân hàng tại Việt Nam vẫn đang ở mức đáng báo động, cho thấy sự phát triển không ngừng của các loại mã độc đánh cắp thông tin.

- Các hacker sử dụng các loại mã độc này đang trở nên ngày càng tinh vi với các chiêu trò phát tán mới như giả mạo các tập tin độc hại, qua mặt các phần mềm diệt virus, ...

❖ Khuyến nghị:

- Không/hạn chế tải về các phần mềm crack, các phần mềm không rõ nguồn gốc tiềm ẩn nguy cơ xuất hiện tràn lan trên không gian mạng.

- Hạn chế sử dụng tính năng lưu mật khẩu trên trình duyệt để giảm thiểu rủi ro bị lộ lọt thông tin. Đổi mật khẩu thường xuyên để ngăn ngừa rủi ro xảy ra. Bật tính năng xác thực đa yếu tố cho tài khoản đăng nhập.

- Doanh nghiệp, tổ chức có thể cân nhắc không cho phép truy cập hệ thống từ trên trình duyệt. Theo ghi nhận của VCS-Threat Intelligence, một số ngân hàng đã thay đổi thói quen người dùng chỉ cho phép đăng nhập trên các ứng dụng di động, từ đó đã giảm thiểu được 90% tài khoản bị lộ lọt.

Lộ lọt do bị tấn công và rao bán thông tin

Năm 2023 kiến sự bùng nổ của việc rao bán thông tin người dùng trong lĩnh vực sản xuất và bán lẻ, dữ liệu hệ thống cùng nhiều dữ liệu nhạy cảm của các doanh nghiệp lớn tại Việt Nam với 21 trường hợp lộ lọt liên quan tới lĩnh vực Bán lẻ (18) và Sản xuất (3).

STT	Thời gian rao bán	Nguồn rao bán	Dữ liệu bị rao bán	Số tiền chuộc	Nguồn gốc lộ lọt
1	05-Thg1-23	Diễn đàn Breachforums	2.583.320 thông tin đặt hàng của khách hàng	Chia sẻ miễn phí	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
2	13-Thg6-23	Diễn đàn Breachforums	1M+ thông tin của khách hàng	800$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
3	13-Thg6-23	Diễn đàn Breachforums	700k+ thông tin của khách hàng và thông tin các đơn hàng	350$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
4	17-Thg6-23	Diễn đàn Breachforums	Hơn 800K+ thông tin của khách hàng	2000$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
5	17-Thg6-23	Diễn đàn Breachforums	Hơn 800K+ thông tin của khách hàng	500$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
6	10-Thg7-23	Diễn đàn Breachforums	369,422 bản ghi thông tin của khách hàng	500$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
7	10-Thg7-23	Diễn đàn Breachforums	225463 thông tin của khách hàng	1000$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.

Lộ lọt do bị tấn công và rao bán thông tin

STT	Thời gian rao bán	Nguồn rao bán	Dữ liệu bị rao bán	Số tiền chuộc	Nguồn gốc lộ lọt
8	10-Thg7-23	Diễn đàn Breachforums	255770 thông tin của khách hàng	500$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
9	13-Thg7-23	Diễn đàn Breachforums	3380000 thông tin của khách hàng	Chia sẻ miễn phí	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
10	19-Thg7-23	Diễn đàn Breachforums	160k thông tin của khách hàng	8 credit	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
11	10-Thg8-23	Diễn đàn Breachforums	404577 thông tin của khách hàng	300$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
12	16-Thg8-23	Diễn đàn Breachforums	10000 thông tin của khách hàng	Chia sẻ miễn phí	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
13	19-Thg8-23	Diễn đàn Breachforums	400k+ thông tin của khách hàng	300$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
14	19-Thg8-23	Diễn đàn Breachforums	1M+ thông tin của khách hàng	2000$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
15	10-Thg9-23	Diễn đàn Breachforums	1796769 thông tin của khách hàng	2000$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.

Lộ lọt do bị tấn công và rao bán thông tin

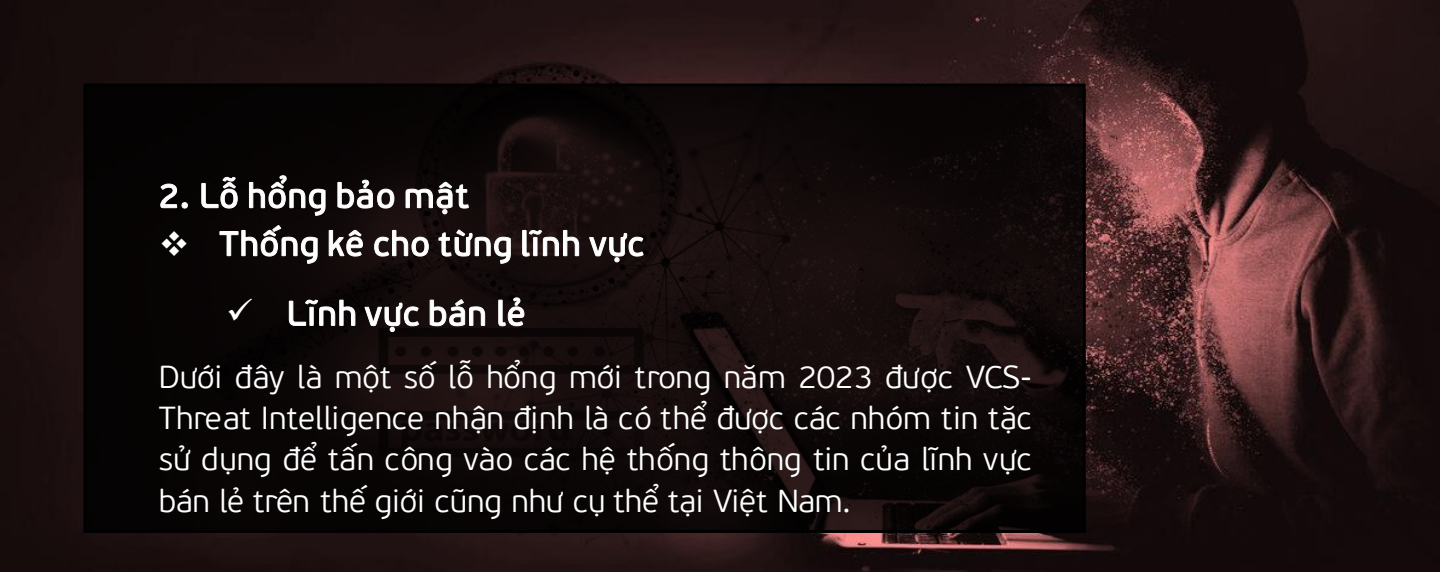
STT	Thời gian rao bán	Nguồn rao bán	Dữ liệu bị rao bán	Số tiền chuộc	Nguồn gốc lộ lọt
16	10-Thg9-23	Diễn đàn Breachforums	2192 thông tin của khách hàng	8 credit	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
17	23-Thg9-23	Diễn đàn Breachforums	Hơn 28534592 thông tin của khách hàng	2000$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
18	29-Thg9-23	Diễn đàn Breachforums	903,891 thông tin của khách hàng	1200$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
19	02-Thg10-23	Diễn đàn Breachforums	Tài khoản đăng nhập vào PhpMyAdmin	8 credit	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
20	02-Thg10-23	Diễn đàn Breachforums	145321 thông tin của khách hàng	500$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
21	02-Thg10-23	Diễn đàn Breachforums	134,971 thông tin của khách hàng & 2,245,558 thông tin đơn hàng	1500$	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.
22	05-Thg10-23	Diễn đàn Breachforums	600000 thông tin của khách hàng	Chia sẻ miễn phí	Do hacker sử dụng các tài khoản nội bộ bị đánh cắp để trực hiện trích xuất dữ liệu và rao bán.

❖ **VCS-Threat Intelligence nhận định:** Nguyên nhân các vụ rao bán, lộ lọt dữ liệu trên đều do tài khoản quản trị của các hệ thống lưu trữ dữ liệu bị ăn cắp (do quản trị viên đăng nhập hệ thống trên các máy tính nhiễm mã độc ăn cắp thông tin), sau đó các tin tặc mua bán tài khoản quản trị này và sử dụng truy cập trực tiếp vào hệ thống trích xuất dữ liệu.

❖ **Khuyến nghị:**

- Rà soát, đổi mật khẩu mạnh cho các tài khoản nội bộ ngân hàng bị lộ lọt, rao bán (có trong các cảnh báo của VCS-Threat Intelligence).

- Rà soát nhật ký truy cập các hệ thống có tài khoản bị lộ lọt, xác định các dấu hiệu truy cập bất thường, điều tra và phản ứng nếu xác định có sự cố xâm nhập trái phép.



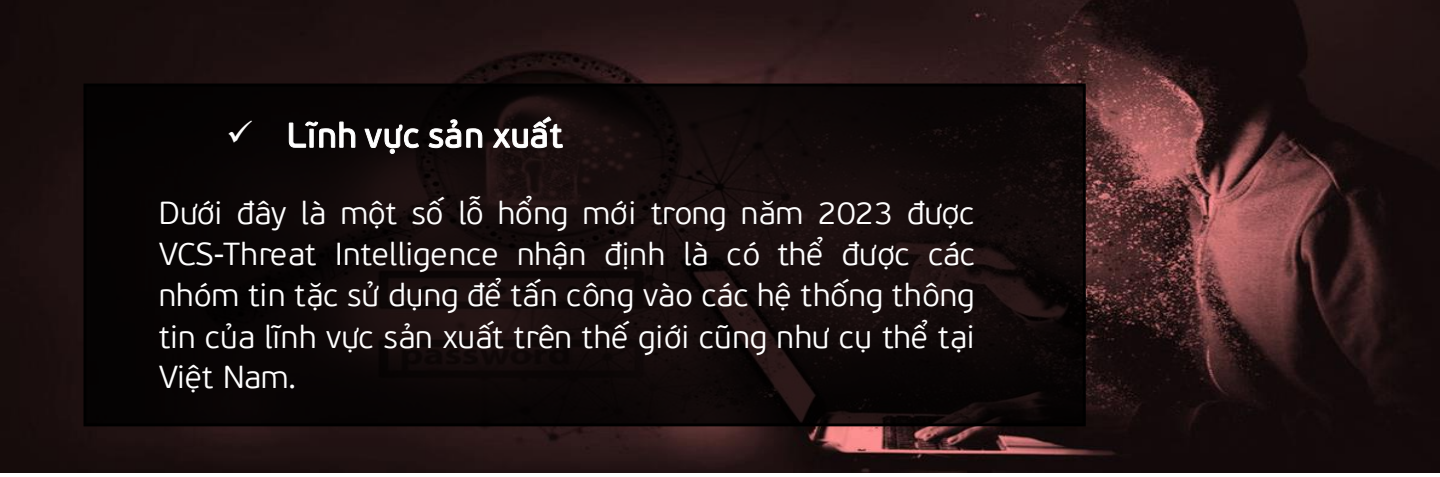
2. Lỗ hổng bảo mật

❖ Thống kê cho từng lĩnh vực

✓ Lĩnh vực bán lẻ

Dưới đây là một số lỗ hổng mới trong năm 2023 được VCS-Threat Intelligence nhận định là có thể được các nhóm tin tặc sử dụng để tấn công vào các hệ thống thông tin của lĩnh vực bán lẻ trên thế giới cũng như cụ thể tại Việt Nam.

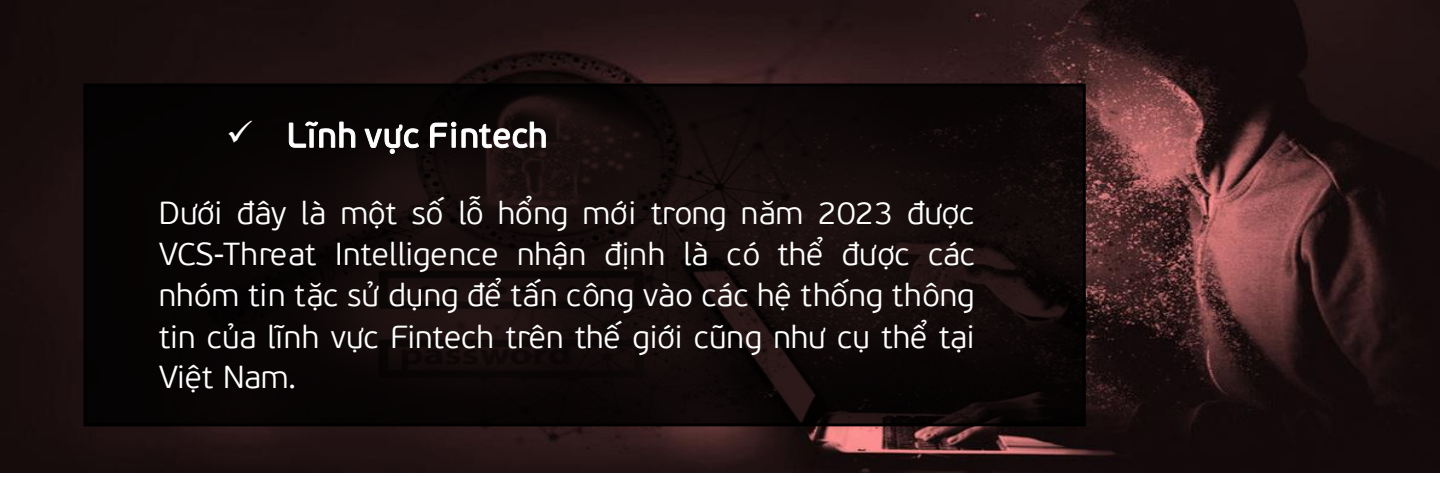
Tên lỗ hổng	Thông tin chung	Mức độ theo nhận định của Viettel Threat Intelligence
Magecart	Đây là một phương thức tấn công bằng cách khai thác các lỗ hổng trên các nền tảng Ecommerce như WooCommerce, Shopify, Magento, WordPress của các trang web bán lẻ, từ đó chèn các mã javascript độc hại để lấy cắp thông tin thanh toán của người dùng.	Nghiêm Trọng
CVE-2023-32243	Nguy cơ khai thác lỗ hổng leo thang đặc quyền trên Plugin Essential Addons for Elementor của WordPress, một plugin được sử dụng phổ biến trên thế giới. Tin tặc không cần xác thực có thể leo thang đặc quyền lên bất cứ người dùng nào của trang web WordPress kể cả người dùng quản trị bằng chức năng đặt lại mật khẩu.	Cao
CVE-2023-23397	Nguy cơ khai thác lỗ hổng Information Disclosure trên ứng dụng Microsoft Outlook, phần mềm quản lý thông tin như email, lịch, tệp phổ biến. Khai thác lỗ hổng thành công, tin tặc có thể lấy được thông tin nhạy cảm của người dùng.	Cao
CVE-2023-27997	Nguy cơ khai thác lỗ hổng CVE-2023-27997 trên Fortinet FortiOS và FortiProxy SSL-VPN, các giải pháp an ninh mạng phổ biến của Fostinet. Khai thác lỗ hổng thành công, tin tặc có thể thực thi mã tùy ý trên máy chủ mà không cần xác thực.	Cao
CVE-2023-29357	Nguy cơ khai thác lỗ hổng bỏ qua xác thực trên SharePoint Server. Tin tặc không cần xác thực có thể giả mạo bất cứ người dùng nào trên SharePoint, kể cả tài khoản quản trị viên thông qua việc giả mạo JSON Web Tokens (JWTs) trong quá trình xác thực Oauth, từ đó cho phép truy cập API. Tin tặc có thể kết hợp với việc khai thác lỗ hổng khác để thực thi mã từ xa.	Nghiêm Trọng
CVE-2023-38831 | CVE-2023-40477	Nguy cơ khai thác lỗ hổng bảo mật trong phần mềm WinRAR - phần mềm hỗ trợ người dùng trong việc nén và giải nén các tệp tin. Khai thác thành công, tin tặc có thể thực thi mã tùy ý và cài đặt mã độc vào máy nạn nhân. Các lỗ hổng đã được sử dụng trong các chiến dịch tấn công trong thực tế.	Cao



✓ Lĩnh vực sản xuất

Dưới đây là một số lỗ hổng mới trong năm 2023 được VCS-Threat Intelligence nhận định là có thể được các nhóm tin tặc sử dụng để tấn công vào các hệ thống thông tin của lĩnh vực sản xuất trên thế giới cũng như cụ thể tại Việt Nam.

Tên lỗ hổng	Thông tin chung	Mức độ theo nhận định của Viettel Threat Intelligence
CVE-2023-27524	Nguy cơ thực thi mã từ xa trên Apache Superset, công cụ mã nguồn mở được sử dụng phổ biến để trực quan hóa dữ liệu. Nguy cơ xảy ra do Apache Superset sử dụng cấu hình mặc định không an toàn. Tin tặc không cần xác thực có thể khai thác lỗ hổng để đăng nhập hệ thống với đặc quyền quản trị viên, từ đó lấy cắp thông tin nhạy cảm và thực thi mã từ xa trên hệ thống.	Cao
CVE-2023-34362	Nguy cơ khai thác lỗ hổng SQL Injection trên MOVEit Transfer cho phép tin tặc nâng cao đặc quyền, xem và tải xuống dữ liệu từ máy chủ cơ sở dữ liệu, ngoài ra còn cho phép tin tặc lấy được thông tin tài khoản và các thông tin nhạy cảm về Azure Blob Storage bao gồm AzureBlobStorageAccount, AzureBlobKey, và AzureBlobContainer. Lỗ hổng đã được sử dụng trong các chiến dịch tấn công thực tế.	Nghiêm Trọng
CVE-2023-23397	Nguy cơ khai thác lỗ hổng Information Disclosure trên ứng dụng Microsoft Outlook, phần mềm quản lý thông tin như email, lịch, tệp phổ biến. Khai thác lỗ hổng thành công, tin tặc có thể lấy được thông tin nhạy cảm của người dùng.	Cao
CVE-2023-27997	Nguy cơ khai thác lỗ hổng CVE-2023-27997 trên Fortinet FortiOS và FortiProxy SSL-VPN, các giải pháp an ninh mạng phổ biến của Fostinet. Khai thác lỗ hổng thành công, tin tặc có thể thực thi mã tùy ý trên máy chủ mà không cần xác thực.	Cao
CVE-2023-29357	Nguy cơ khai thác lỗ hổng bỏ qua xác thực trên SharePoint Server. Tin tặc không cần xác thực có thể giả mạo bất cứ người dùng nào trên SharePoint, kể cả tài khoản quản trị viên thông qua việc giả mạo JSON Web Tokens (JWTs) trong quá trình xác thực Oauth, từ đó cho phép truy cập API. Tin tặc có thể kết hợp với việc khai thác lỗ hổng khác để thực thi mã từ xa.	Nghiêm Trọng
CVE-2023-38831 | CVE-2023-40477	Nguy cơ khai thác lỗ hổng bảo mật trong phần mềm WinRAR - phần mềm hỗ trợ người dùng trong việc nén và giải nén các tệp tin. Khai thác thành công, tin tặc có thể thực thi mã tùy ý và cài đặt mã độc vào máy nạn nhân. Các lỗ hổng đã được sử dụng trong các chiến dịch tấn công trong thực tế.	Cao



✓ Lĩnh vực Fintech

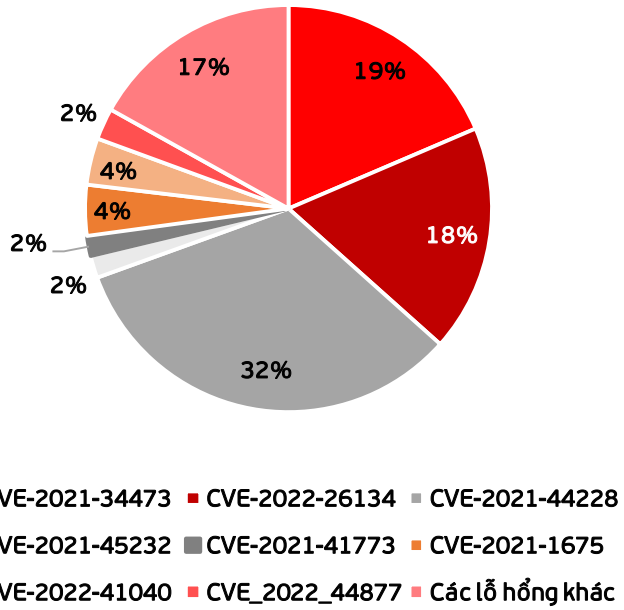
Dưới đây là một số lỗ hổng mới trong năm 2023 được VCS-Threat Intelligence nhận định là có thể được các nhóm tin tặc sử dụng để tấn công vào các hệ thống thông tin của lĩnh vực Fintech trên thế giới cũng như cụ thể tại Việt Nam.

Tên lỗ hổng	Thông tin chung	Mức độ theo nhận định của Viettel Threat Intelligence
CVE-2022-21587	Nguy cơ thực thi mã từ xa trên Oracle Web Applications Desktop Integrator thuộc Oracle E-Business Suite, giải pháp ERP (Enterprise Resource Planning) được sử dụng tương đối phổ biến. Lỗ hổng xảy ra tại component Upload, tin tặc chưa xác thực có thể khai thác lỗ hổng để tải lên webshell từ đó thực thi mã từ xa trên hệ thống.	Nghiêm Trọng
CVE-2023-3519	Nguy cơ khai thác lỗ hổng thực thi mã từ xa trên NetScaler ADC và NetScaler Gateway của Citrix, một giải pháp bảo mật của hãng Citrix. Tin tặc không cần xác thực có thể khai thác lỗ hổng để thực thi mã từ xa, từ đó thực hiện các hành vi độc hại trên hệ thống.	Nghiêm Trọng
CVE-2023-23397	Nguy cơ khai thác lỗ hổng Information Disclosure trên ứng dụng Microsoft Outlook, phần mềm quản lý thông tin như email, lịch, tệp phổ biến. Khai thác lỗ hổng thành công, tin tặc có thể lấy được thông tin nhạy cảm của người dùng.	Cao
CVE-2023-27997	Nguy cơ khai thác lỗ hổng CVE-2023-27997 trên Fortinet FortiOS và FortiProxy SSL-VPN, các giải pháp an ninh mạng phổ biến của Fostinet. Khai thác lỗ hổng thành công, tin tặc có thể thực thi mã tùy ý trên máy chủ mà không cần xác thực.	Cao
CVE-2023-29357	Nguy cơ khai thác lỗ hổng bỏ qua xác thực trên SharePoint Server. Tin tặc không cần xác thực có thể giả mạo bất cứ người dùng nào trên SharePoint, kể cả tài khoản quản trị viên thông qua việc giả mạo JSON Web Tokens (JWTs) trong quá trình xác thực Oauth, từ đó cho phép truy cập API. Tin tặc có thể kết hợp với việc khai thác lỗ hổng khác để thực thi mã từ xa.	Nghiêm Trọng
CVE-2023-38831 | CVE-2023-40477	Nguy cơ khai thác lỗ hổng bảo mật trong phần mềm WinRAR - phần mềm hỗ trợ người dùng trong việc nén và giải nén các tệp tin. Khai thác thành công, tin tặc có thể thực thi mã tùy ý và cài đặt mã độc vào máy nạn nhân. Các lỗ hổng đã được sử dụng trong các chiến dịch tấn công trong thực tế.	Cao

❖ Trend khai thác chung

Dưới đây là tỉ lệ của các lỗ hổng được sử dụng trong chiến dịch tấn công thực tế trong quý 3 năm 2023:

Tỉ lệ các lỗ hổng được rà quét, khai thác nhiều trong quý 3 năm 2023



Danh sách chi tiết một số lỗ hổng được sử dụng nhiều trong các chiến dịch thực tế tại Việt Nam:

Mã CVE	Thông tin chung	Mức độ theo nhận định của Viettel Threat Intelligence
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-2022-41040	Lỗ hổng Server-Side Request Forgery (SSRF) trên Microsoft Exchange Server. Kết hợp với CVE-2023-41082 với tên gọi ProxynotShell cho phép tin tặc đã xác thực có thể thực thi mã từ xa trên hệ thống mục tiêu. Lỗ hổng này được sử dụng nhiều trong các chiến dịch tấn công thực tế trước khi thông tin chi tiết về các lỗ hổng chưa được công bố.	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
CVE-2021-41773	Nguy cơ chiếm quyền điều khiển trên Apache Server 2.4.49. Nguy cơ xảy ra do việc Apache HTTP Server không chuẩn hóa dữ liệu đầu vào khiến tin tặc có thể thực hiện tấn công Path traversal để truy cập các đường dẫn, thông tin nhạy cảm trên máy chủ. Thậm chí, tin tặc có thể chiếm quyền điều khiển hệ thống thông qua tính năng mod-cgi.	Cao

(Danh sách chi tiết các lỗ hổng bảo mật mới được công bố xem tại https://platform.cyberintel.io hoặc thư điện tử cảnh báo của VCS-Threat Intelligence)

❖ VCS-Threat Intelligence nhận định:

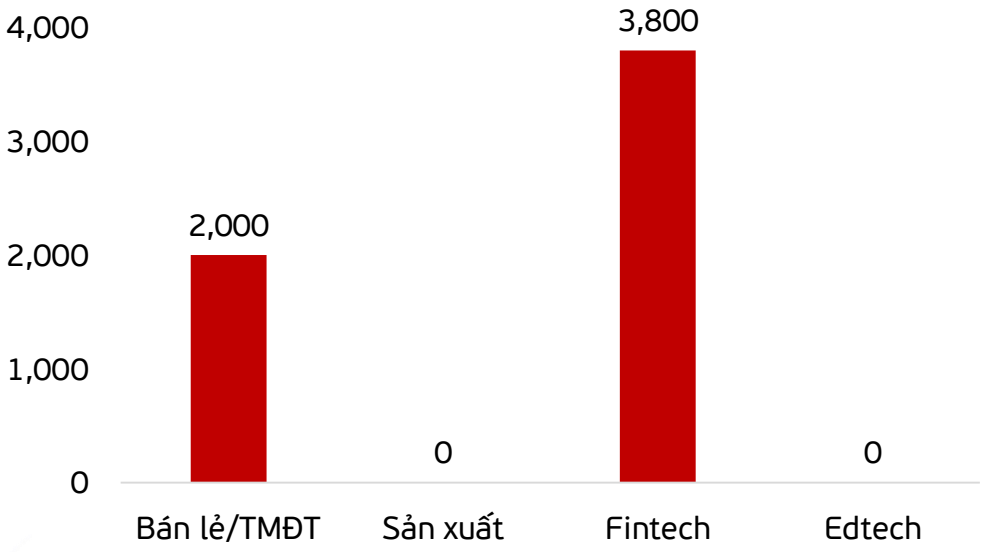
- Các nhóm tấn công đã sử dụng các lỗ hổng này trong các chiến dịch thực tế trước cả khi thông tin của các lỗ hổng được công bố.

❖ Khuyến nghị:

- Thực hiện các phương án cập nhật bản vá, khắc phục tạm thời (có trong các cảnh báo của VCS-Threat Intelligence).
- Người dùng không truy cập các đường dẫn lạ, không rõ nguồn gốc. Không mở các tệp tin từ các nguồn không tin tưởng.

3. Lừa đảo, giả mạo

Thống kê số liệu lừa đảo liên quan đến nhóm ngành



(Danh sách chi tiết các tên miền lừa đảo, giả mạo xem tại https://platform.cyberintel.io hoặc thư điện tử cảnh báo của VCS-Threat Intelligence)

❖ Hình thức lừa đảo

Lĩnh vực	Hình thức lừa đảo
Bán lẻ/Thương mại điện tử	- Giả mạo nhân viên chăm sóc khách hàng của doanh nghiệp, yêu cầu nạn nhân truy cập các trang web lừa đảo, cung cấp thông tin, tải ứng dụng giả mạo, ... - Lừa đảo tuyển cộng tác viên online, tuyển nhân viên bán thời gian trên các sàn thương mại điện tử - Lừa đảo các chương trình khuyến mãi, chương trình huy động vốn của doanh nghiệp
Sản xuất	- Lừa đảo thông qua hình thức vay tiền trực tuyến - Lừa đảo chuyển tiền quốc tế - Lừa đảo, giả mạo các dịch vụ liên quan đến thẻ tín dụng - Lừa đảo giả mạo ví điện tử

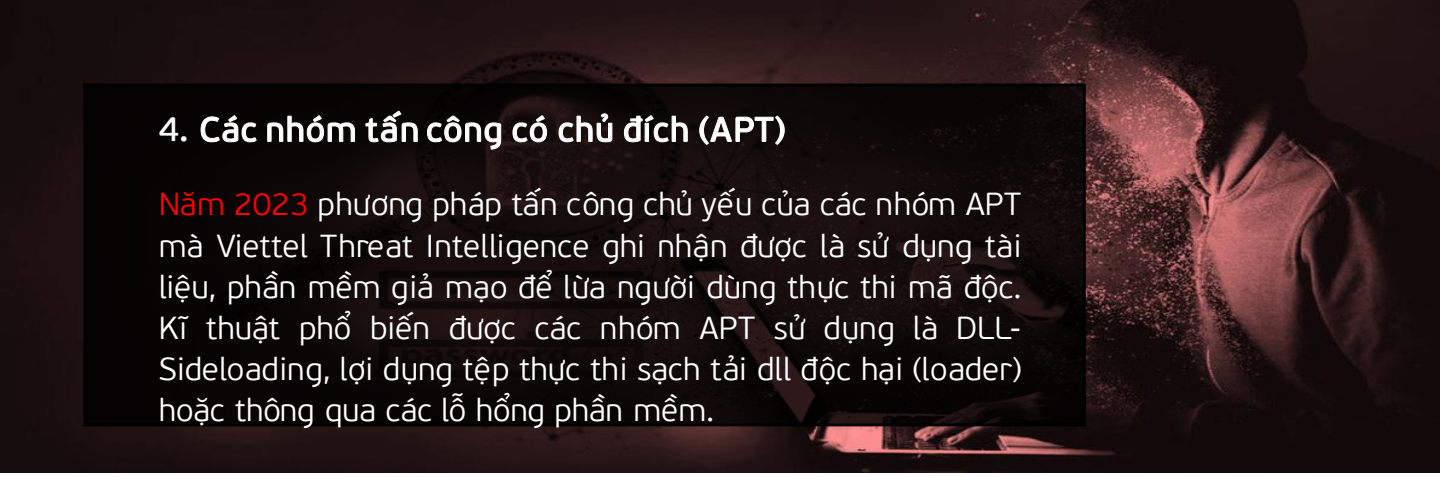
❖ VCS-Threat Intelligence nhận định:

Các chiến dịch lừa đảo giả mạo dịch vụ nâng cấp tín dụng vẫn diễn ra mạnh mẽ và có sự tăng trưởng qua các tháng, chưa có dấu hiệu suy giảm.

Có sự tăng trưởng trở lại của các tên miền lừa đảo giả mạo giao diện chính thức các dịch vụ của ngân hàng.

❖ Khuyến nghị:

- Cảnh báo tới khách hàng về các hình thức lừa đảo, chiến dịch lừa đảo mới.
- Trong tương lai, chiến dịch này có thể phát triển mạnh và tiếp tục nhằm vào các tổ chức tài chính, ngân hàng. tổ chức cần theo dõi và giám sát các chiến dịch lừa đảo, lợi dụng thương hiệu của tổ chức trên không gian mạng.



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

Năm 2023 phương pháp tấn công chủ yếu của các nhóm APT mà Viettel Threat Intelligence ghi nhận được là sử dụng tài liệu, phần 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 phần mềm.

Trong năm 2023, 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:

- Ngoài các kỹ thuật đã được đề cập trong báo cáo năm 2022, các nhóm tấn công có chủ đích đã nâng cấp, sử dụng một số kỹ thuật mới có thể kể đến như:

- 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.

- 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 để vượt qua giải pháp bảo mật hiệu quả.

- 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.

- Process Injection: Các nhóm tấn công thường sử dụng kỹ thuật này để vượt qua các kỹ thuật phòng thủ của hệ thống do được chạy trên một tiến trình hợp pháp.

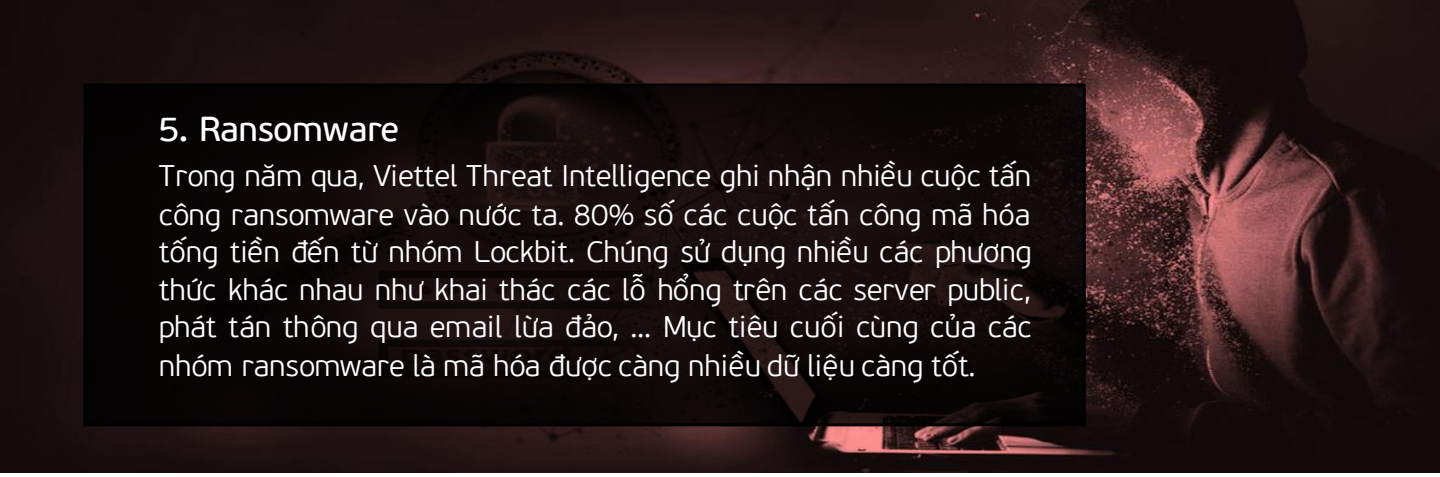
- DLL-SideLoading: Là kỹ thuật phổ biến nhất được các nhóm tấn công sử dụng. Các nhóm tấn công thường sử dụng kỹ thuật này để bỏ qua lớp phòng thủ của hệ thống do payload được thực thi thông qua một tiến trình hợp pháp.

Danh sách các nhóm tấn công có chủ đích hoạt động mạnh tại Việt Nam trong 6 tháng đầu năm 2023 mà Viettel Threat Intelligence phát hiện được:

STT	Tên nhóm	Mô tả	Các kỹ thuật, công cụ thường xuyên sử dụng
1	Mustang Panda	Nhóm tin tặc chuyên nhắm mục tiêu vào các tổ chức thuộc lĩnh vực chính phủ, quốc phòng và năng lượng. Trong năm 2023, Viettel Threat Intelligence phát hiện nhiều mẫu mã độc giả dạng nội dung của nhóm Mustang Panda.	Spearphishing Attachment, DLL Side Loading, Template Injection
2	APT32	Được phát hiện lần đầu vào năm 2004, mục tiêu chính của nhóm là lĩnh vực chính phủ - dịch vụ công ở nhiều quốc gia.	Spearphishing Attachment, DLL Side Loading, ActiveMime, Cobalt Strike
3	APT37	APT37 là nhóm APT hoạt động ít nhất từ năm 2012. APT37 thường nhắm mục tiêu vào lĩnh vực chính phủ - dịch vụ công ở nhiều quốc gia.	Khai thác CVE, Spearphishing Attachment
4	SharpPanda	SharpPanda là nhóm APT được phát hiện lần đầu vào năm 2018. SharpPanda thường sử dụng kĩ thuật email lừa đảo kết hợp các lỗ hổng trong Microsoft Office. Mục tiêu chính của nhóm là lĩnh vực chính phủ.	Spearphishing Attachment, DLL Side Loading, Khai thác CVE

STT	Tên nhóm	Mô tả	Các kỹ thuật, công cụ thường xuyên sử dụng
5	APT41	APT41 thường nhắm vào lĩnh vực chính phủ - dịch vụ công ở nhiều quốc gia. APT41 đã từng tấn công vào nhiều doanh nghiệp và tổ chức tại Việt Nam.	Khai thác CVE, LNK, Webshell
6	Lazarus	Lazarus là nhóm APT nhắm vào mục tiêu lĩnh vực quốc phòng, ngân hàng tài chính. Nhóm này từng có nhiều chiến dịch tấn công vào các tổ chức doanh nghiệp tại Việt Nam.	Spearphishing Attachment, DLL Side Loading, Template Injection, LNK
7	APT27	Còn được gọi là Goblin Panda. Thường nhắm mục tiêu vào lĩnh vực chính phủ. Nhóm đã từng tấn công vào nhiều doanh nghiệp và tổ chức tại Việt Nam.	Spearphishing Attachment, DLL Side Loading

(Thông tin chi tiết các chiến dịch tấn công có chủ đích xem tại https://platform.cyberintel.io hoặc thư điện tử cảnh báo của VCS-Threat Intelligence)



5. Ransomware

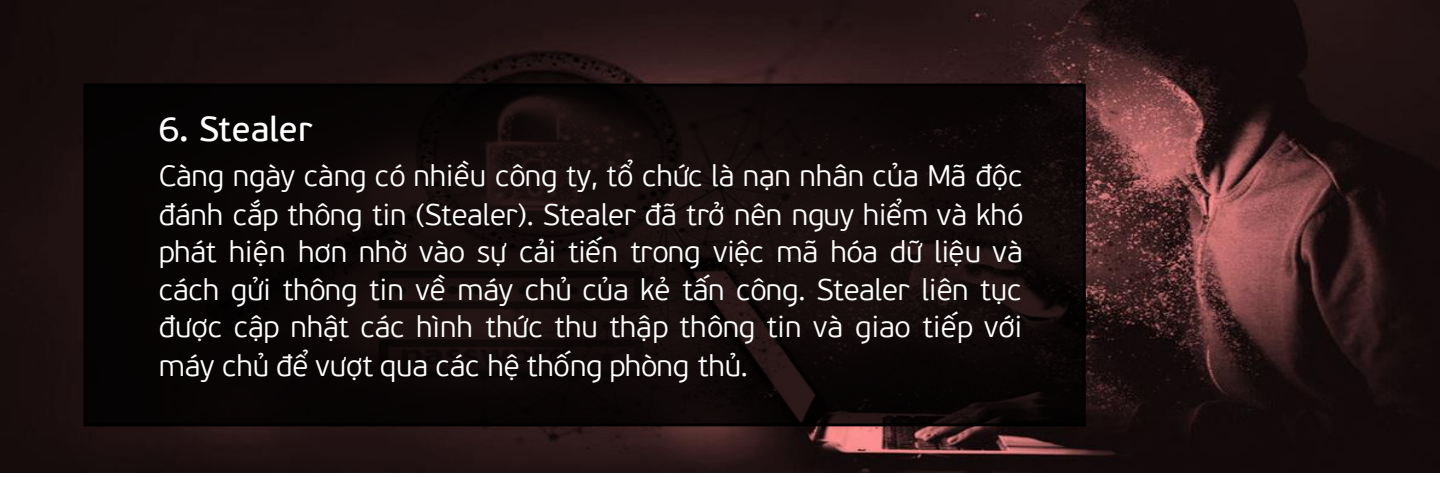
Trong năm qua, Viettel Threat Intelligence ghi nhận nhiều cuộc tấn công ransomware vào nước ta. 80% số các cuộc tấn công mã hóa tống tiền đến từ nhóm Lockbit. Chúng sử dụng nhiều các phương thức khác nhau như khai thác các lỗ hổng trên các server public, phát tán thông qua email lừa đảo, ... Mục tiêu cuối cùng của các nhóm ransomware là mã hóa được càng nhiều dữ liệu càng tốt.

Danh sách các cuộc tấn công ransomware:

STT	Tên	Thời gian	Dung lượng	Nhóm
1	Công ty cổ phần về ô tô	10/9/2023	>100GB	Lockbit3
2	Công ty lĩnh vực thực phẩm	17/2/2023	30GB	Lockbit3
3	Công ty lĩnh vực bán lẻ	13/2/2023	23.7GB	Lockbit3
4	Công ty lĩnh vực sản xuất	9/16/2023	7.24GB	Lockbit3
5	Công ty cổ phần về năng lượng	7/9/2023		Stormous

Thông tin về các nhóm ransomware:

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 vào các doanh nghiệp và tổ chức
2	Stormous	Được ghi nhận kể từ năm 2021, liên lạc với những người nạn nhân của mình thông qua các kênh Telegram, sau đó bổ sung thêm thông qua trang web dựa trên Tor.	Chủ yếu vào các doanh nghiệp và tổ chức



6. Stealer

Càng ngày càng có nhiều công ty, tổ chức là nạn nhân của Mã độc đánh cắp thông tin (Stealer). Stealer đã trở nên nguy hiểm và khó phát hiện hơn nhờ vào sự cải tiến trong việc mã hóa dữ liệu và cách gửi thông tin về máy chủ của kẻ tấn công. Stealer liên tục được cập nhật các hình thức thu thập thông tin và giao tiếp với máy chủ để vượt qua các hệ thống phòng thủ.

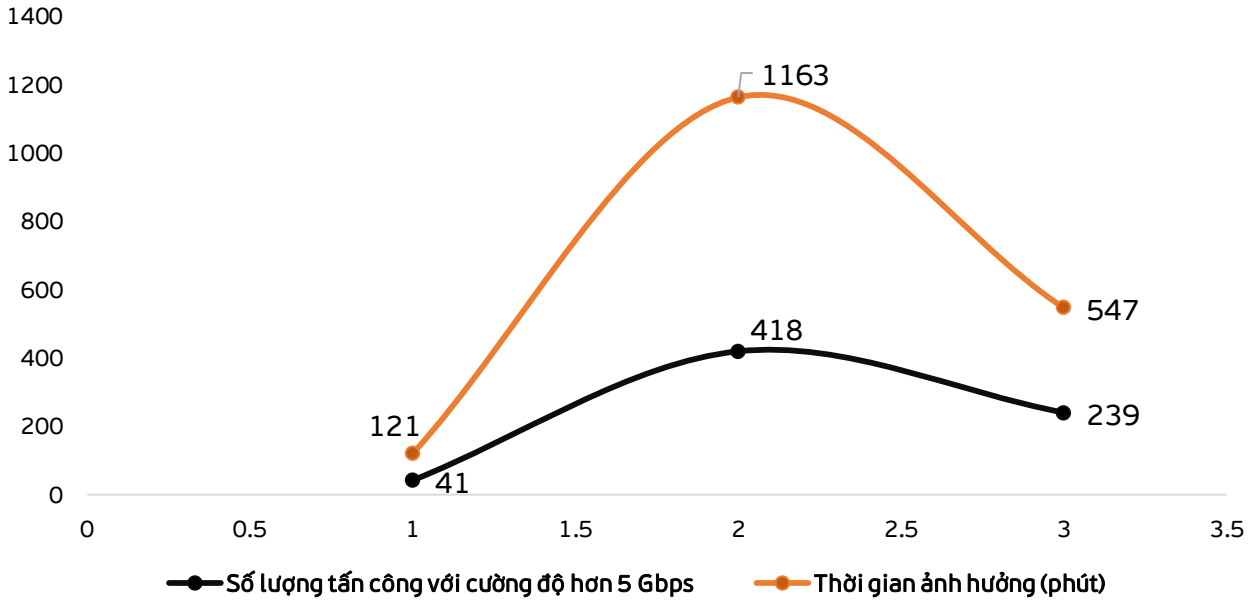
Danh sách các nhóm Stealer:

STT	Tên mã độc	Mô tả
1	Redline Stealer	Mã độc có số lượng xuất hiện hàng đầu kể từ đầu năm 2023. RedLine Stealer chủ yếu nhắm vào người dùng đơn lẻ nhằm đánh cắp thông tin ví tiền điện tử, cấu hình FTP/VPN, thông tin đăng nhập các ứng dụng như Discord, Steam, Telegram, …
2	Meta Stealer	MetaStealer, một phần mềm độc hại đánh cắp thông tin mới nổi đang nổi lên trong bối cảnh các mối đe dọa mạng, đã sinh sôi nảy nở thông qua chiến dịch malspam. Có vẻ như là một phiên bản tương tự hoặc cải tiến của RedLine.
3	Vidar Stealer	Việc lây nhiễm phần mềm độc hại bắt đầu bằng email lừa đảo hoặc Drive-by download. Những người dùng đang cố tải xuống phần mềm miễn phí cho Windows hầu hết đều bị nhiễm phần mềm đánh cắp Vidar Infosec. Các máy bị nhiễm sẽ bắt đầu liên lạc với Youtube.com và Sites.google.com bằng cách chuyển hướng trang web.

7. Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ phân tán vẫn luôn là hình thúc tấn công mạng phổ biến gây ảnh hưởng mạnh tới dịch vụ khách hàng. Lợi dụng giao thức như TCP, tin tặc có thể khiến các thiết bị như tường lửa, router , ... trở nên cao tải. Hoặc với các giao thức như UDP, DNS, ... tin tặc có thể sinh ra tấn công với băng thông lên tới hàng trăm Gbps, ảnh hưởng tới hạ tầng doanh nghiệp. Hệ quả là gây nên mất dịch vụ, ảnh hưởng tới trải nghiệm của khách hàng. Từ đó khiến uy tín doanh nghiệp giảm sút cũng như thiệt hại nặng về tài chính.

Tỷ lệ ảnh hưởng bởi tấn công DDoS trong 3 quý đầu năm



❖ Nhận định:

- Trong 3 quý đầu năm, Viettel AntiDDoS ghi nhận hơn 700 cuộc tấn công DDoS với cường độ lớn hơn 5Gbps, đây là cường độ mà đa số các DDoS appliance của các doanh nghiệp ở VN không chống được (do license của doanh nghiệp thường mua < 5 Gbps)
- Hệ thống ghi nhận trung bình mỗi cuộc tấn công diễn ra trong khoảng thời gian trung bình 5 phút. Đặc biệt trong quý 2, tổng thời gian mà các doanh nghiệp sẽ phải chịu ảnh hưởng là hơn 1000 phút.

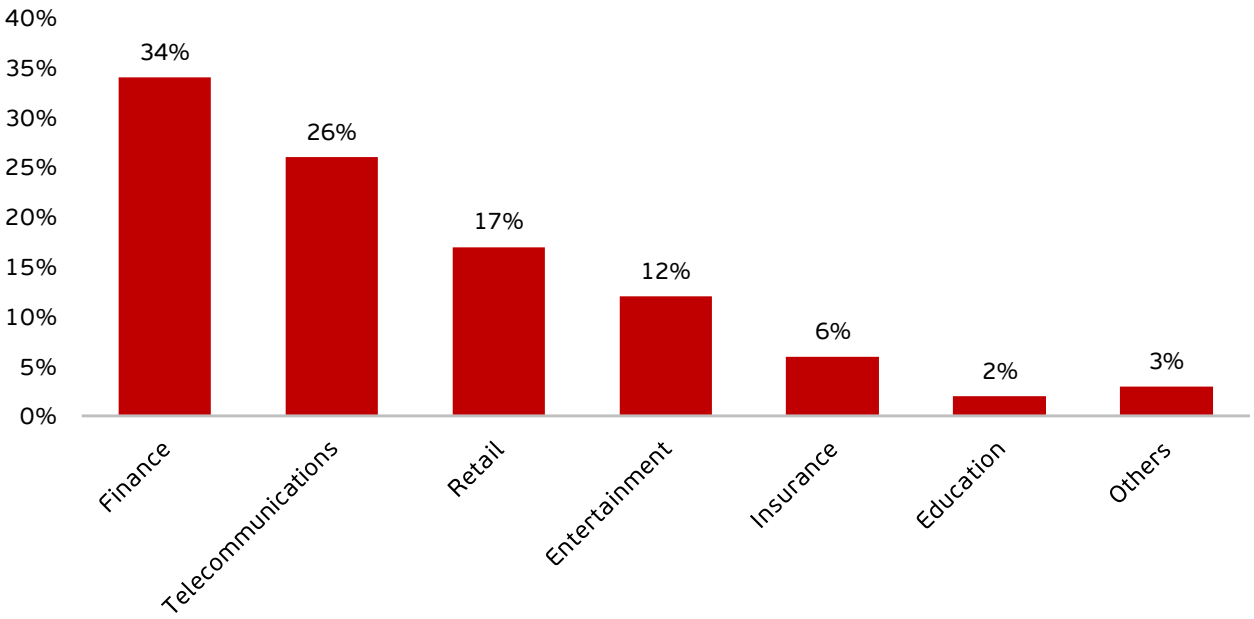
❖ Khuyến nghị

- Để có thể chống đỡ trước các cuộc tấn công DDoS với quy mô lớn, việc sử dụng các giải pháp mức mạng lưới của các nhà mạng là cấp thiết

7. Tấn công từ chối dịch vụ

Tấn công từ chối dịch vụ phân tán vẫn luôn là hình thức tấn công mạng phổ biến gây ảnh hưởng mạnh tới dịch vụ khách hàng. Lợi dụng giao thức như TCP, tin tặc có thể khiến các thiết bị như tường lửa, router , ... trở nên cao tải. Hoặc với các giao thức như UDP, DNS, ... tin tặc có thể sinh ra tấn công với băng thông lên tới hàng trăm Gbps, ảnh hưởng tới hạ tầng doanh nghiệp. Hệ quả là gây nên mất dịch vụ, ảnh hưởng tới trải nghiệm của khách hàng. Từ đó khiến uy tín doanh nghiệp giảm sút cũng như thiệt hại nặng về tài chính.

Các lĩnh vực bị tấn công DDoS nhiều nhất



Nguồn: https://www.infosecurity-magazine.com/blogs/2022-ddos-yearinreview/

❖ Nhận định:

- Lĩnh vực bị tấn công nhiều nhất là mảng tài chính (BFSI) 34%
- Sau đó là mảng truyền thông, giải trí đa phương tiện, bán lẻ, giáo dục, ...

41st Floor, Keangnam Landmark 72, Pham Hung Rd., Nam Tu Liem Dist., Hanoi, Vietnam.

https://cyberintel.io

cyberthreat@viettel.com.vn

(+84) 971 360 360