viettel security

NGUY CƠ LỘ LỌT THÔNG TIN CÁ NHÂN NGHIÊM TRỌNG DO CÁC LOẠI MÃ ĐỘC ĐÁNH CẮP THÔNG TIN

viettel security

MỤC LỤC

TỔNG QUAN

Lộ lọt dữ liệu đang là một trong những chủ đề rất nóng tại Việt Nam trong những năm trở lại đây với số lượng thông tin cá nhân bị lộ lọt và rao bán trên không gian mạng ngày càng lớn.

viettel security

Lộ lọt dữ liệu

Dữ liệu lộ lọt được phân loại thành một số dạng phổ biến như sau:

- Personal Data: Dữ liệu cá nhân, các loại thông tin định danh cá nhân (PII).
- Credentials: Tài khoản cá nhân, tài khoản đăng nhập vào các hệ thống.
- Documents: Các tài liệu nội bộ, tài liệu mật của doanh nghiệp, tổ chức.
- Source Code: Mã nguồn của hệ thống, có thể bị lộ lọt do tấn công hoặc cấu hình sai.

Nguồn lộ lọt dữ liệu

Dữ liệu lộ lọt thường được phát hiện tại một số các nền tảng như:

- Clear Web
- Dark Web
- Social Media
- Instant Messenging

viettel security

Tác nhân gây lộ lọt dữ liệu

Một số nguyên nhân và các tác động khiến dữ liệu bị lộ lọt:

- Do kẻ tấn công xâm nhập và đánh cắp dữ liệu.
- Lộ lọt không có chủ ý như cấu hình sai hệ thống hoặc vô tình tải lên công khai các tập tin nhạy cảm.
- Do chính người dùng vô tình tiết lộ công khai.
- Do nội bộ chia sẻ ra ngoài phạm vi tổ chức, doanh nghiệp.
- Do bị lây nhiễm các loại mã độc đánh cắp thông tin.

Nguy cơ ảnh hưởng khi dữ liệu bị lộ lọt

Kẻ xấu sau khi chiếm đoạt được các thông tin cần thiết có thể thực hiện các hành vi như sau:

- Rao bán các dữ liệu nhạy cảm của người dùng.
- Xâm nhập trái phép vào hệ thống sử dụng các thông tin đã có với mục đích phá hoại hoặc tống tiền.
- Tấn công bằng phương pháp Social-Engineering.
- Giả mạo danh tính, sử dụng để làm giả giấy tờ nhằm chiếm đoạt tài sản.

viettel security

MÃ ĐỘC đánh cắp thông tin

- Mã độc đánh cắp thông tin (Infostealing Malware) là một trong những tác nhân cực kỳ nguy hiểm có mức độ ảnh hưởng tới dữ liệu, tài sản số của cá nhân và tổ chức, doanh nghiệp.

- Các loại mã độc có chức năng đánh cắp thông tin phổ biến hiện nay:
  - Trojans: Trojan Banking, Stealer
  - Botnets
  - Keyloggers
  - Droppers/Downloaders

- **Redline Stealer, Raccoon Stealer hay Azorult** - ba trong nhiều chủng mã độc đánh cắp thông tin (Stealer) hoạt động phổ biến nhất trong những năm trở lại đây - đã được phát tán và đánh cắp hàng tỷ tài khoản đăng nhập và các dữ liệu nhạy cảm khác của các cá nhân và doanh nghiệp trong và ngoài nước.

Bạn có biết?

Tính đến thời điểm tháng 8/2022, trên KGM đã xuất hiện gần 200 loại Stealer và hơn 30 loại vẫn đang hoạt động mạnh mẽ.

viettel security

STEALER

Giới thiệu về mối đe dọa

- Malware Stealer - chỉ một trong những loại mã độc đánh cắp thông tin hoạt động dưới dạng Malware As A Service.

  ◀ Mối đe dọa (Adversary)

- Bất kỳ ai cũng có thể là nạn nhân của các loại mã độc này nếu vô tình tải về các phần mềm không rõ nguồn gốc được cài cắm mã độc. *Điều này có thể là vô tình hoặc đang rơi vào tầm ngắm của một chiến dịch cụ thể.*

  ◀ Nạn nhân ảnh hưởng (Victims)

- Một khi bị lây nhiễm, nạn nhân sẽ bị đánh cắp các thông tin từ hệ thống, trình duyệt như tài khoản đăng nhập, cookies, ví điện tử và một số các thông tin có giá trị khác. *Ngoài ra, mã độc tiếp tục cài cắm thêm các công cụ độc hại đi kèm khác.*

  ◀ Khả năng ảnh hưởng (Capabilities)

- Hạ tầng và dấu vết của các loại mã độc này sử dụng HTTP-SOAP để trích xuất dữ liệu, tải về và thực thi mã từ xa. *Do tính chất của các loại mã độc MaaS thì mỗi người dùng sẽ đi với một C&C khác nhau.*

  ◀ Hạ tầng và dấu vết (Infrastructure)

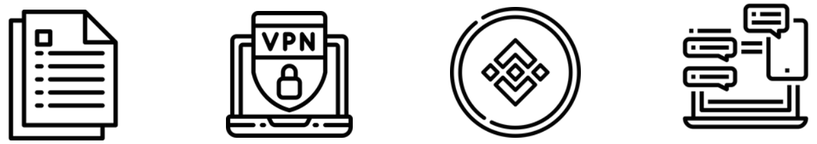
viettel security

STEALER

Khả năng ảnh hưởng của mối đe dọa

Threat Actor Capabilities

- Đánh cắp thông tin đăng nhập được lưu trên trình duyệt của nạn nhân
- Đánh cắp thông tin hệ thống
- Đánh cắp thông tin ví điện tử
- Ảnh chụp màn hình nạn nhân
- Các tập tin trong máy của nạn nhân



- Đánh cắp thông tin các ứng dụng Instant Messenging như Discord và Telegram
- Đánh cắp thông tin ứng dụng VPN
- Đánh cắp thông tin FTP
- Đánh cắp thông tin người chơi Steam
- Đánh cắp thông tin 2FA từ các ứng dụng như Authentication

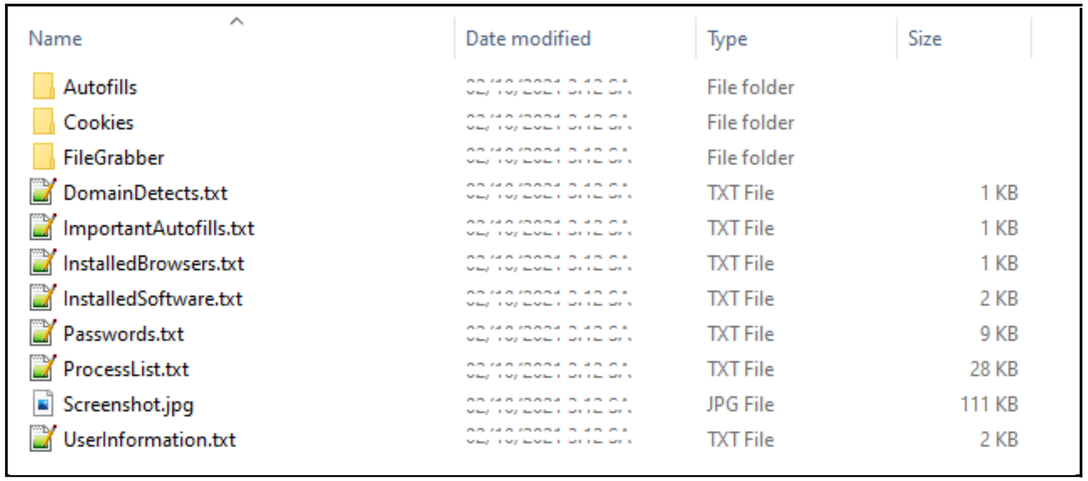
viettel security

STEALER

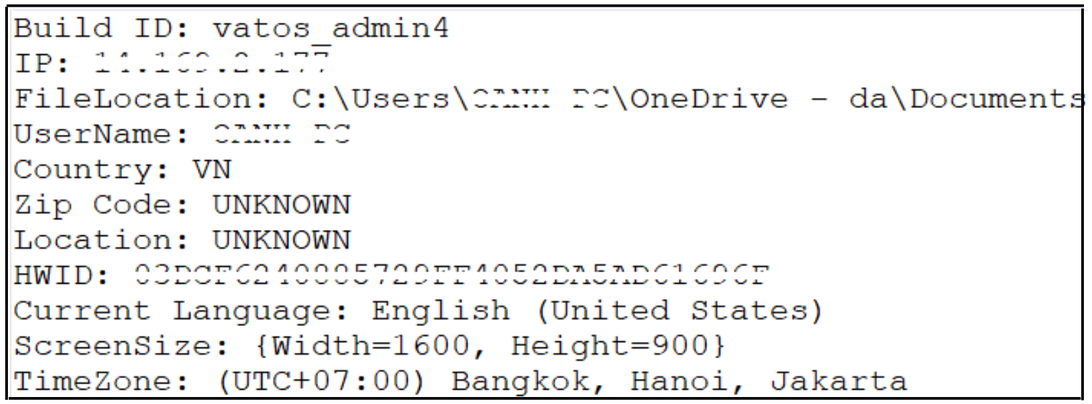
Khả năng ảnh hưởng của mối đe dọa

Threat Actor Capabilities

- Sau khi bị lây nhiễm, dữ liệu của nạn nhân sẽ được trích xuất vào một tập tin nén và được đẩy lên máy chủ của kẻ tấn công. Những tập dữ liệu này được gọi là **LOGS.**
- Kẻ tấn công có toàn quyền sử dụng các dữ liệu này, lọc ra các dữ liệu cần thiết hoặc mang lên các hội nhóm để rao bán.
- Do mã độc hoạt động theo dạng MaaS, số lượng kẻ tấn công phân tán logs trên không gian mạng là cực kỳ lớn. Mỗi tuần, dung lượng các khu vực mua bán và chia sẻ logs ước tính xấp xỉ **100GB** dữ liệu.



Name	Date modified	Type	Size
Autofills	[redacted]	File folder	
Cookies	[redacted]	File folder	
FileGrabber	[redacted]	File folder	
DomainDetects.txt	[redacted]	TXT File	1 KB
ImportantAutofills.txt	[redacted]	TXT File	1 KB
InstalledBrowsers.txt	[redacted]	TXT File	1 KB
InstalledSoftware.txt	[redacted]	TXT File	2 KB
Passwords.txt	[redacted]	TXT File	9 KB
ProcessList.txt	[redacted]	TXT File	28 KB
Screenshot.jpg	[redacted]	JPG File	111 KB
UserInformation.txt	[redacted]	TXT File	2 KB



```
Build ID: vatos_admin4
IP: [redacted]
FileLocation: C:\Users\[redacted]\OneDrive - da\Documents
UserName: [redacted]
Country: VN
Zip Code: UNKNOWN
Location: UNKNOWN
HWID: [redacted]
Current Language: English (United States)
ScreenSize: {Width=1600, Height=900}
TimeZone: (UTC+07:00) Bangkok, Hanoi, Jakarta
```

Bạn có biết?

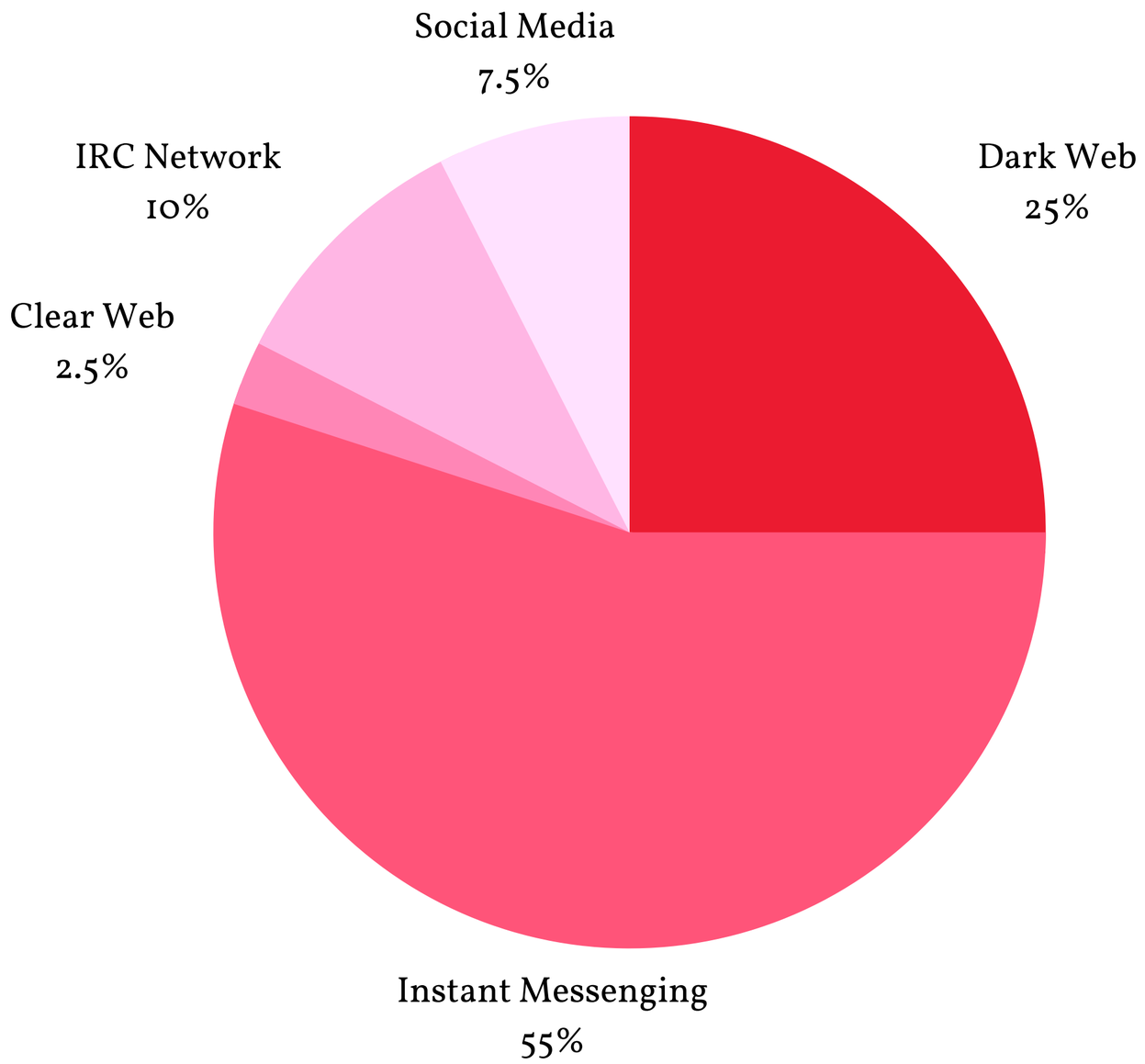
--

Instant Messenging là khu vực chia sẻ dữ liệu lộ lọt dạng logs nhiều nhất hiện nay

viettel security

STEALER

Khả năng ảnh hưởng của mối đe dọa



Threat Actor Capabilities

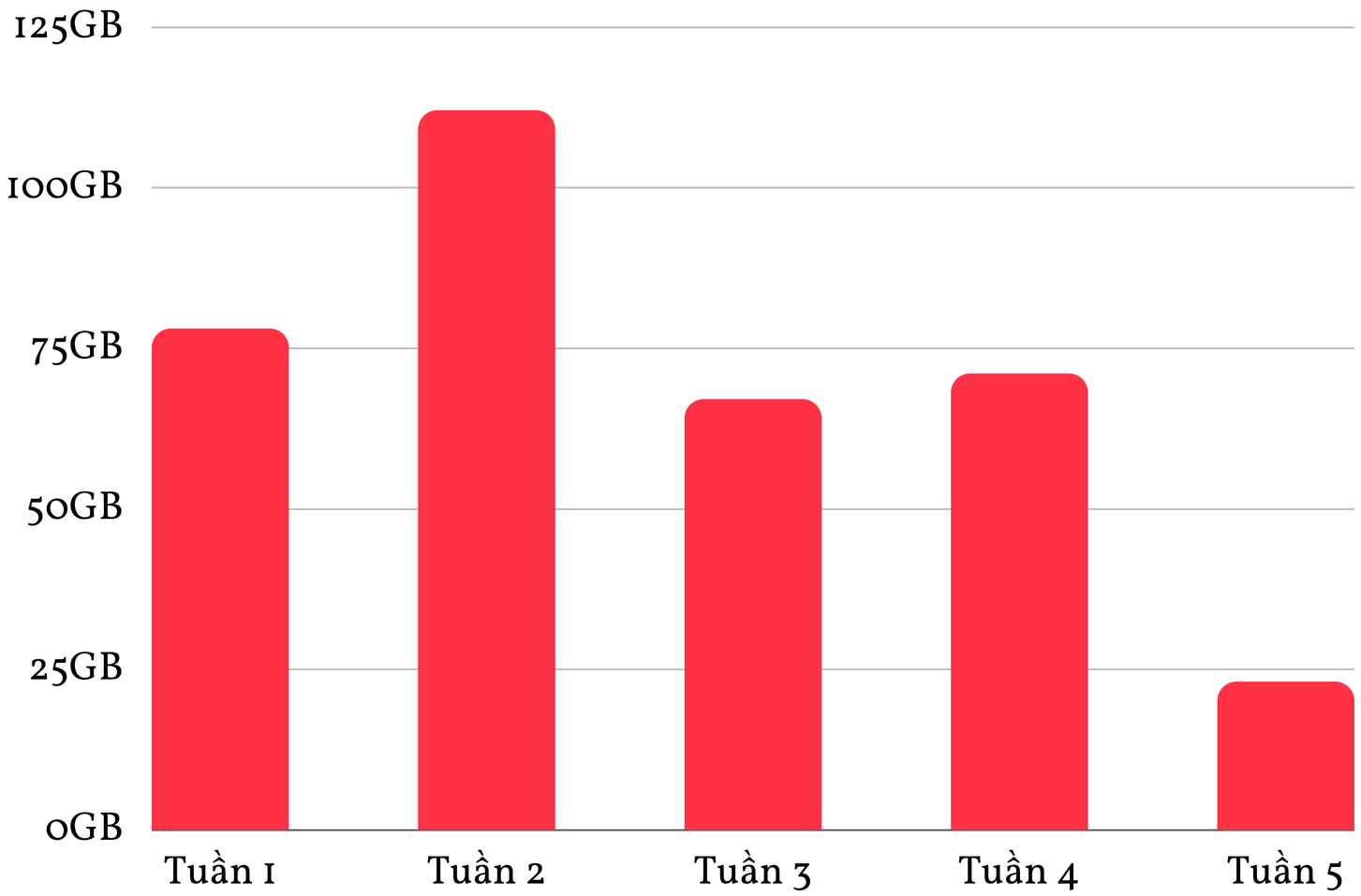
- Biểu đồ tròn mô tả tỉ lệ dữ liệu lộ lọt thường được rao bán và chia sẻ trên một số các nền tảng phổ biến hiện nay.
- Instant Messenging - như Telegram - là nền tảng được phát hiện được sử dụng để rao bán và chia sẻ Logs phổ biến nhất do tính bảo mật cao và dễ dàng sử dụng.
- Dark Web và IRC Network cũng là một trong nền tảng phổ biến để chia sẻ dữ liệu lộ lọt.
- Ngược lại Clear Web và Social Media không thường được sử dụng để chia sẻ các thông tin lộ lọt không chính thống.

viettel security

STEALER

Khả năng ảnh hưởng của mối đe dọa

Threat Actor Capabilities

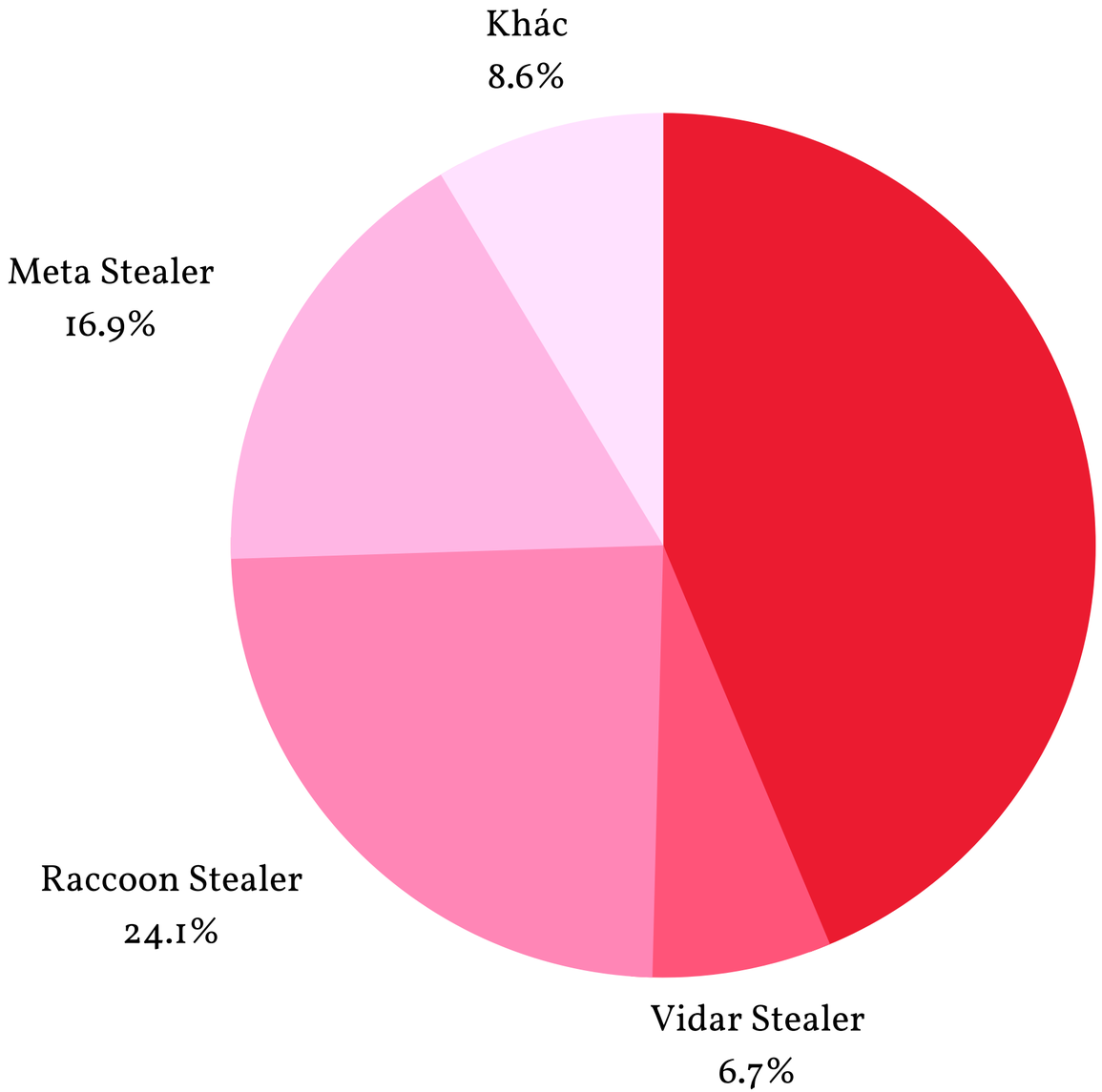


- Biểu đồ mô tả dữ liệu thu thập được trong tháng gần nhất (Tháng 8) lên tới hơn **350GB** dữ liệu.
- Tuần thứ hai trong tháng được coi là những tuần cao điểm vì số lượng logs được kẻ tấn công chia sẻ rất đều đặn.

viettel security

STEALER

Khả năng ảnh hưởng của mối đe dọa



Threat Actor Capabilities

- Redline Stealer vẫn là loại mã độc đánh cắp thông tin được sử dụng phổ biến nhất.
- Do được nâng cấp phiên bản mới nên số lượng logs bị lộ lọt bởi Raccoon Stealer đang nhiều trở lại.
- Meta Stealer - một chủng mã độc mới được phát hiện đã gây lộ lọt nhiều tài khoản tại Việt Nam.
- Vidar Stealer và một số các loại mã độc đánh cắp thông tin khác không gây ảnh hưởng lớn tại Việt Na

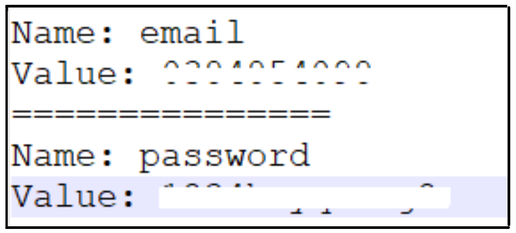
viettel security

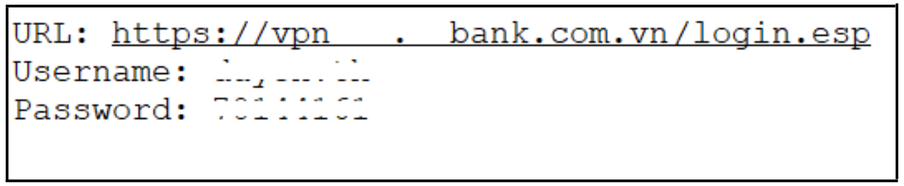
STEALER

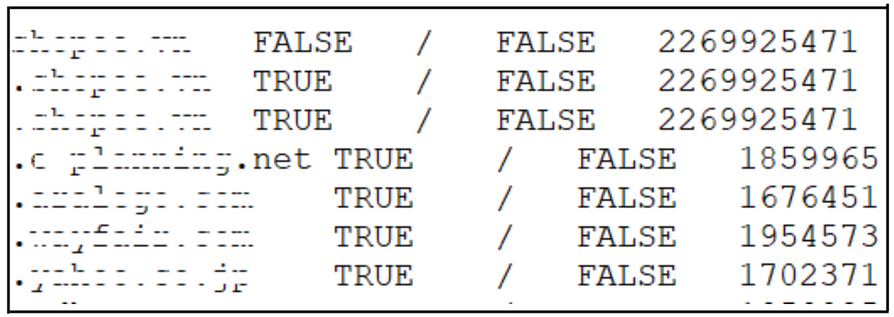
Khả năng ảnh hưởng của mối đe dọa

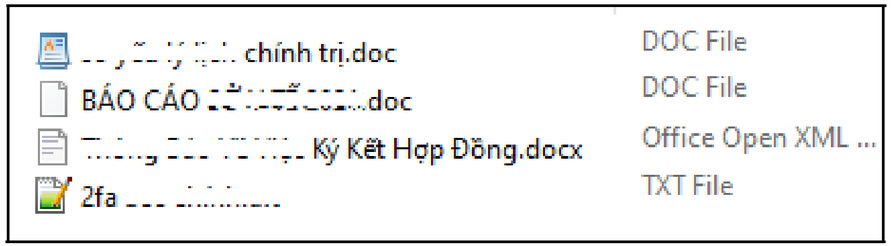
Threat Actor Capabilities

- Việc để lộ ra các dữ liệu nhạy cảm như tài khoản mật khẩu được lưu trên trình duyệt, các tài liệu mật được lưu trong máy là điều cực kỳ nghiêm trọng.
- Kẻ tấn công sử dụng các tài khoản được lưu trên trình duyệt, Cookies hoặc Autofill để xâm nhập trái phép vào các hệ thống.
- Với các tập tin bị đánh cắp, kẻ tấn công có thể có các tập tin nhạy cảm hoặc trích xuất được một số thông tin mà người dùng lưu trong các tập tin văn bản as a note.
- Mọi hành động xâm nhập trái phép này sẽ trực tiếp gây ảnh hưởng tới cá nhân hoặc doanh nghiệp đồng thời làm thất thoát tài sản của các bên bị lộ lọt thông tin.









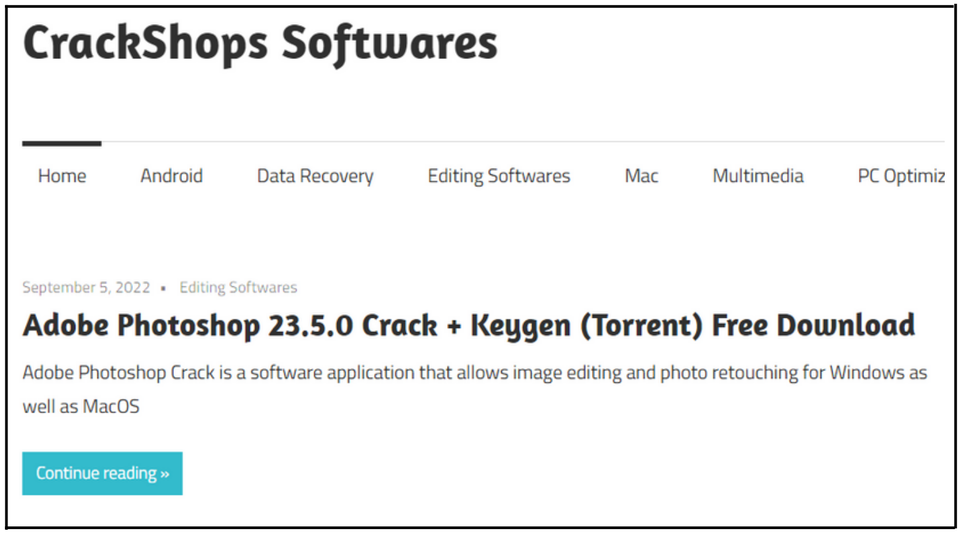
viettel security

STEALER

Nguyên nhân gây ra mối đe dọa

Threat Actor Root Cause

- Các phần mềm crack trôi nổi trên KGM. Kẻ tấn công thiết kế các trang web chuẩn SEO nhằm đưa trang web xuất hiện trong top đầu các kết quả tìm kiếm trên các công cụ tìm kiếm.
- Tạo thành những chiến dịch cụ thể, kẻ tấn công phân tán mã độc qua nhiều hình thức như thư điện tử, chạy quảng cáo...
- Mã độc được nâng cấp để qua mặt các phần mềm diệt virus hiện nay bằng cách sử dụng một số chứng chỉ nhận dạng (signing files certificate).
- Tuy nhiên, việc bị lây nhiễm hay không phụ thuộc phần lớn vào nhận thức của người dùng.
  - Bỏ qua các cảnh báo ứng dụng không rõ nguồn gốc
  - Vô hiệu hóa các phần mềm diệt virus.



viettel security

STEALER

Nguyên nhân gây ra mối đe dọa

Threat Actor
Root Cause

- Trong một số trường hợp người dùng đã có nhận thức về ANM tuy nhiên lại để người thân hoặc bạn bè sử dụng máy cá nhân và vô tình cài đặt các phần mềm chứa mã độc.
- Rất nhiều trường hợp để con cái vô tình cài đặt mã độc khiến các thông tin đăng nhập các hệ thống nhạy cảm của các bậc cha mẹ bị lộ lọt.
- Một số khác do tính chất công việc có tiếp xúc với các loại mã độc và vô tình thực thi mã độc trên máy cá nhân.
- Chủ quan, quá tin tưởng vào một số trang web cung cấp các phần mềm crack tại Việt Nam.
"Phải biết cách tải Crack, mình toàn tải có sao đâu"

- Cá nhân đã có trải nghiệm thú vị với các tình huống này.

viettel security

STEALER

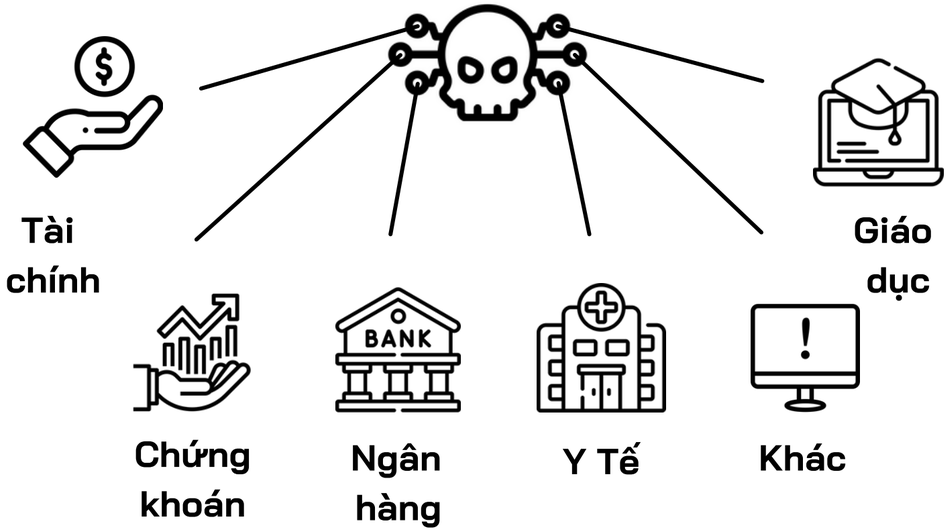
Mức độ ảnh hưởng của mối đe dọa

Threat Actor Impact

- Chỉ trong năm 2021 và đầu năm 2022, Redline Stealer đã được sử dụng để đánh cắp hơn 100.000.000 tài khoản đăng nhập tại Việt Nam
- Các lĩnh vực bị ảnh hưởng mạnh bởi Redline Stealer bao gồm : Ngân hàng & Tài chính, Chứng khoán, Y tế, Giáo dục và một số ngành khác.
- Dữ liệu lộ lọt bao gồm các tài khoản thuộc các tổ chức trong lĩnh vực này (CBNV) hoặc người dùng công khai chỉ sử dụng dịch vụ của tổ chức đó.
- Các dữ liệu lộ lọt này chứa các tài khoản đăng nhập vào một số các hệ thống trọng yếu của các tổ chức và doanh nghiệp như Email nội bộ, VPN, SSO...

Lưu ý: Đây là các tài khoản lộ lọt do cá nhân bị nhiễm mã độc, không phải từ các hệ thống bị tấn công.

Lĩnh vực ảnh hưởng

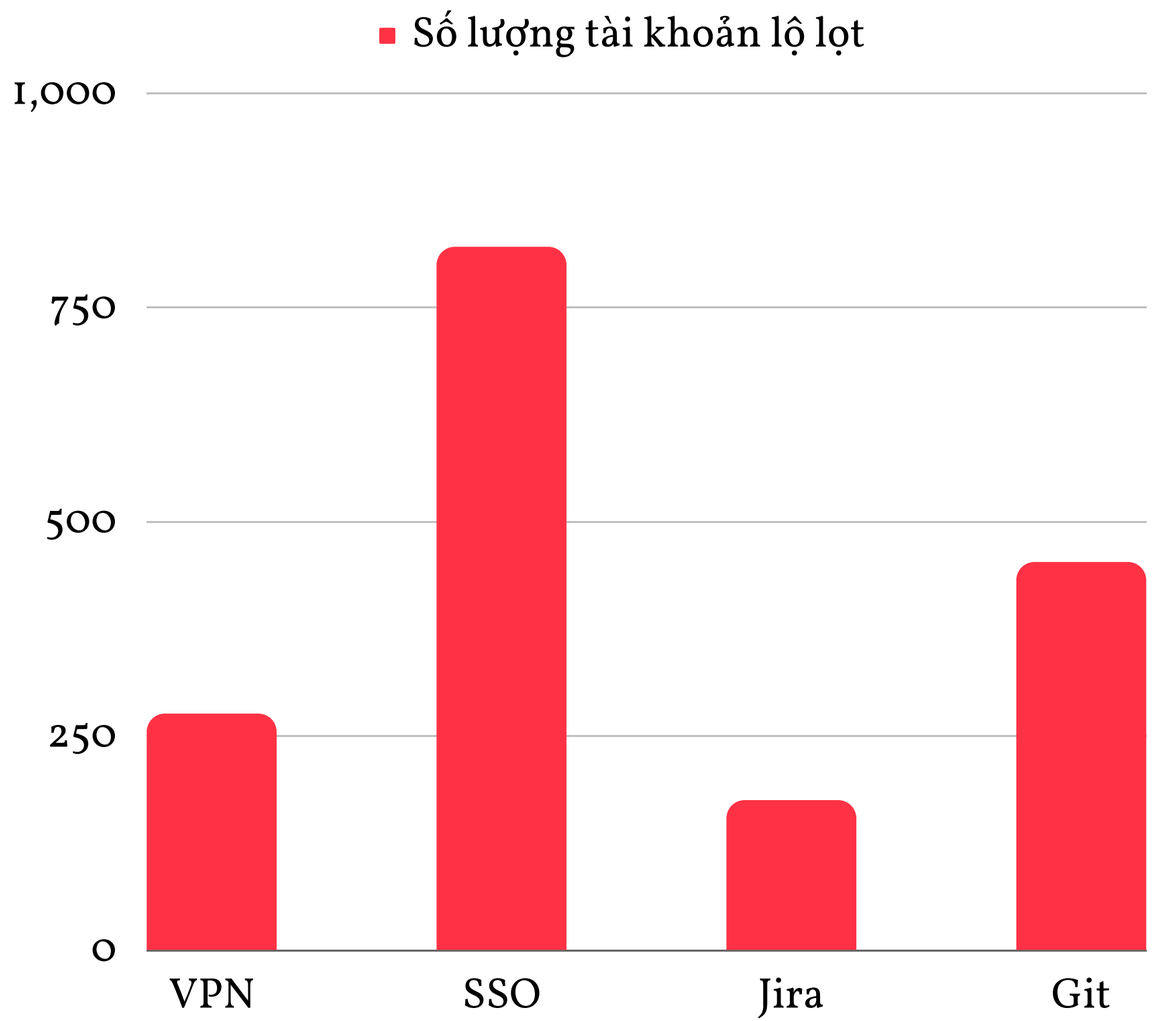


Hệ thống ảnh hưởng

viettel security

STEALER

Mức độ ảnh hưởng của mối đe dọa



Threat Actor Impact

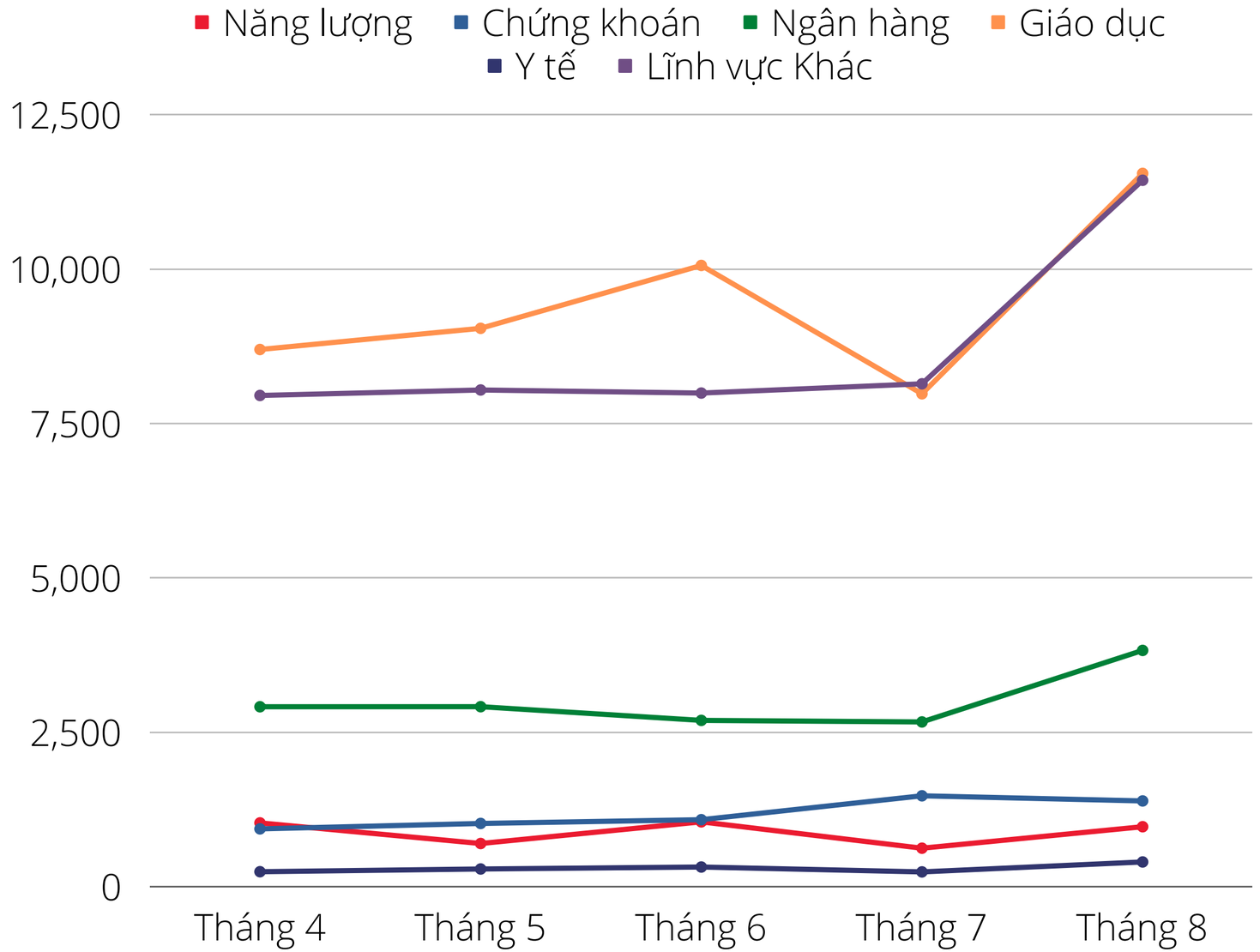
- Số liệu mô tả số lượng các tài khoản đăng nhập vào các hệ thống trọng yếu được phát hiện trong năm 2022..

VPN	SSO	Jira	Git
275	820	174	452

- Đây chỉ là 4 trong rất nhiều các hệ thống có mức độ nhạy cảm lớn. => **NGHIÊM TRỌNG.**
- Tập trung nhiều ở các tổ chức và doanh nghiệp có mức độ ảnh hưởng lớn.

viettel security

Mức độ ảnh hưởng của mối đe dọa



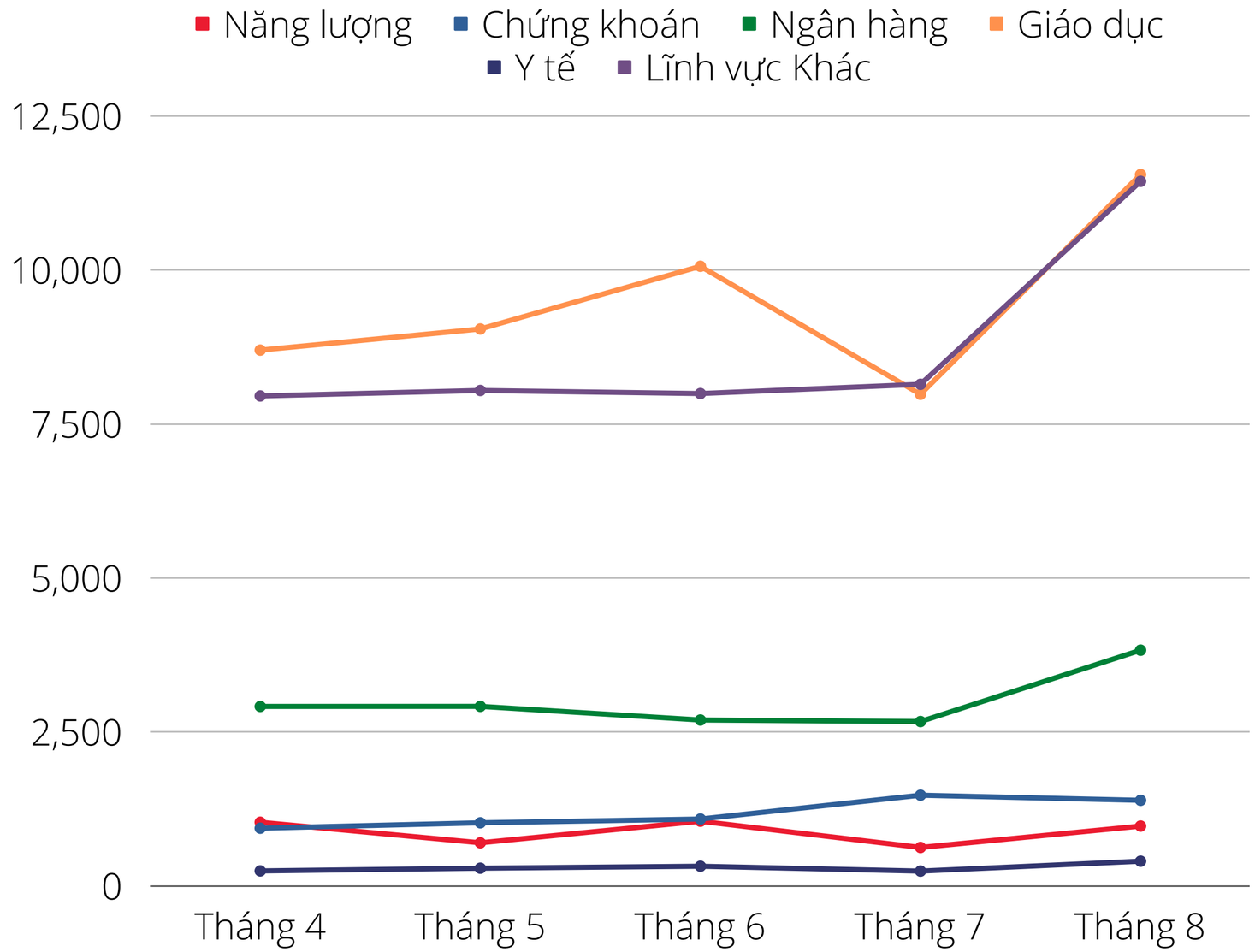
- Biểu đồ cột mô tả số liệu về số lượng tài khoản lộ lọt theo lĩnh vực trong những tháng đầu và giữa năm 2022.
- Lĩnh vực giáo dục (edu.vn) chiếm số lượng tài khoản lộ lọt lớn nhất và có xu hướng tăng gần 3000 tài khoản từ Q1 tới Q3.

T4	T5	T6	T7	T8
8696	9039	10058	7978	11549

Bảng 1. Lĩnh vực giáo dục (Education)

- Đa số là các tài khoản đăng nhập của sinh viên, giáo viên và giảng viên ở các trường tại Việt Nam

Mức độ ảnh hưởng của mối đe dọa



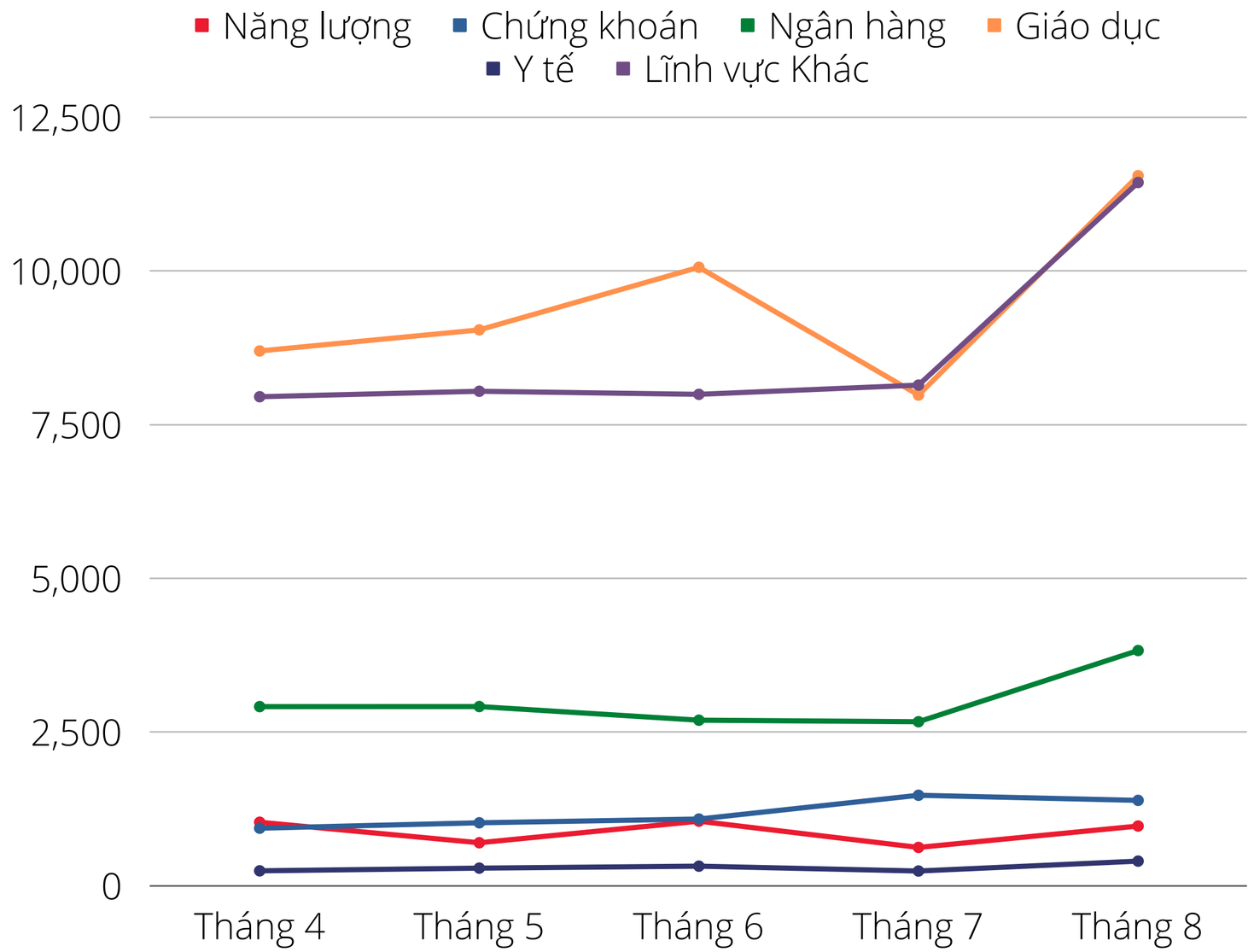
- Lĩnh vực tài chính & ngân hàng (Banking & Finance) đứng thứ hai về số lượng tài khoản lộ lọt.

T4	T5	T6	T7	T8
2907	2908	2686	2661	3820

Bảng 2. Lĩnh vực tài chính & ngân hàng (B&F)

- Số liệu bao gồm các tài khoản lộ lọt của người dùng và các tài khoản đăng nhập nội bộ của tất cả các doanh nghiệp trong lĩnh vực này.

Mức độ ảnh hưởng của mối đe dọa



Lĩnh vực liên quan tới chứng khoán (Stock) và Năng lượng (Energy) cũng đang gây chú ý với số lượng lộ lọt lượng tài khoản tăng theo thời gian.

T4	T5	T6	T7	T8
928	1016	1077	1464	1381

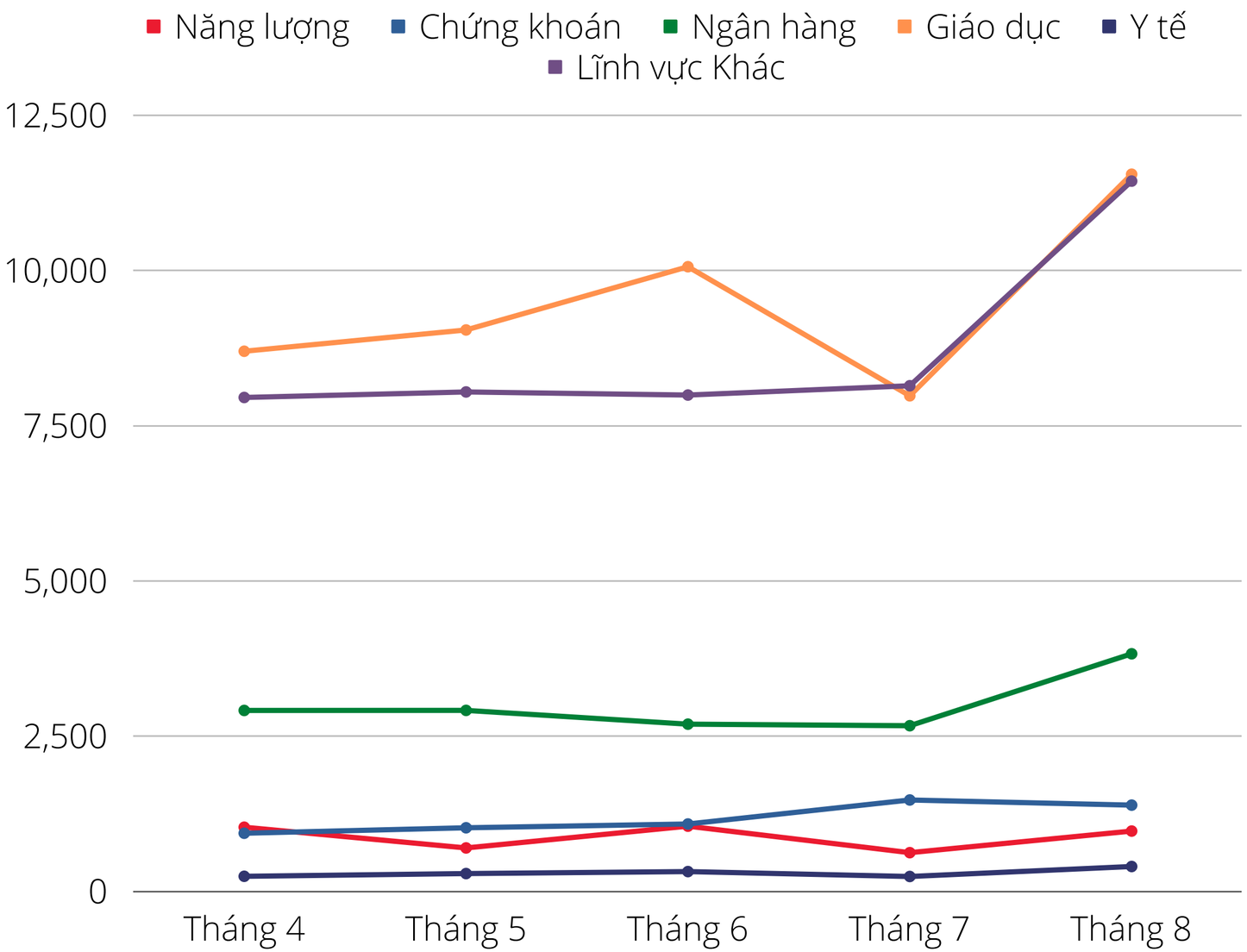
Bảng 3. Lĩnh vực chứng khoán (Stock)

T4	T5	T6	T7	T8
1025	691	1042	615	963

Bảng 4. Lĩnh vực năng lượng (Energy)

STEALER

Mức độ ảnh hưởng của mối đe dọa



Threat Actor Impact

- Lĩnh vực Y Tế qua thời điểm dịch bệnh Covid-19 cũng chứng kiến được nhiều dữ liệu lộ lọt liên quan.

T4	T5	T6	T7	T8
234	278	310	231	392

Bảng 5. Lĩnh vực Y tế (Health)

- Số lượng tài khoản thuộc một số lĩnh vực nhạy cảm khác cũng bị ảnh hưởng bởi các loại mã độc đánh cắp thông tin.

T4	T5	T6	T7	T8
7951	8040	7990	8140	11438

Bảng 6. Lĩnh vực Khác (Others)

viettel security

STEALER

Các khuyến cáo nhằm ngăn ngừa mối đe dọa

Recommendations

- KHÔNG/Hạn chế tải các phần mềm không rõ nguồn gốc tiềm ẩn nguy cơ chứa mã độc.
- Sử dụng mật khẩu khi muốn cài đặt các phần mềm để tránh người thân hoặc bạn bè vô tình khiến bạn mang họa vào thân.
- Hạn chế sử dụng tính năng lưu mật khẩu trên trình duyệt. Thay vào đó sử dụng các phần mềm có tính năng tương tự như: Keypass hoặc AnyPassword...
- Không lưu các dữ liệu quan trọng trong các tập tin văn bản ngoài các thư mục công khai như Desktop, Document,.. Các văn bản quan trọng hãy lưu trữ trên các dịch vụ lưu trữ đám mây như OneDrive,..

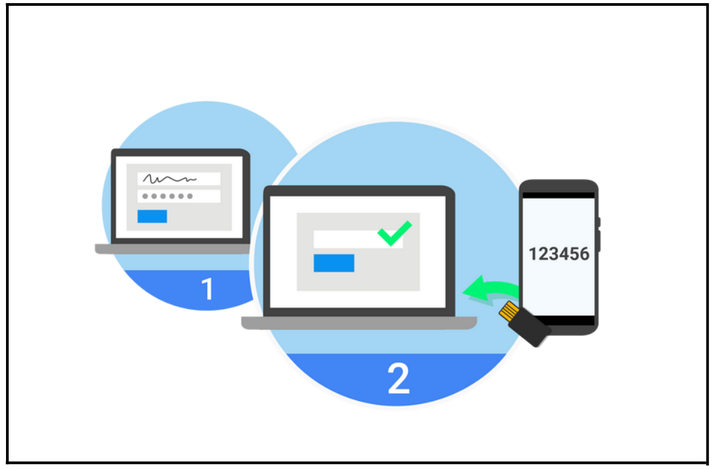
viettel security

STEALER

Các khuyến cáo nhằm ngăn ngừa mối đe dọa

Recommendations

- Không sử dụng mật khẩu mặc định. Thay đổi mật khẩu thường xuyên ít nhất 3 tháng một lần.
- Không thay đổi mật khẩu có sự tương đồng hoặc có quy luật giống như mật khẩu cũ.
- Hạn chế sử dụng lại mật khẩu trên nhiều nền tảng khác nhau.
- Bật tính năng đa xác thực cho tài khoản đăng nhập (nếu có)
- Phân quyền, giới hạn quyền cho mỗi tài khoản trong tổ chức một cách hợp lý.



viettel security

Cảm ơn đã lắng nghe

viettel security