

Ứng dụng Cyber Threat Intelligence trong bảo đảm ATTT cho Cloud và ứng dụng SaaS

Công ty An ninh mạng Viettel



ABOUT ME



TRẦN MINH QUẢNG

GIÁM ĐỐC SẢN PHẨM

Công ty An ninh mạng Viettel

KINH NGHIỆM

- **15 năm kinh nghiệm** trong ngành An toàn thông tin
- Tham gia ứng cứu **100+ sự cố** An toàn thông tin của các Bộ, Ban, Ngành, cơ quan nhà nước, các doanh nghiệp lớn
- **10.000+ giờ nghiên cứu** dịch ngược phần mềm, mã độc, lỗ hổng bảo mật, xử lý sự cố và điều tra số, tri thức nguy cơ an toàn thông tin
- **Diễn giả thường xuyên** tại các hội thảo trong và ngoài nước (Security World, Security Summit, CIO/CSO, Security Bootcamp, botconf, tetcon, tradahacking...)
- **Thành viên Mạng lưới** ứng cứu sự cố an toàn thông tin mạng quốc gia
- **Chứng chỉ quốc tế**: GIAC Cyber Threat Intelligence (GCTI), GIAC Certified Forensic Analyst (GCFA), Certified Threat Intelligence Analyst (C|TIA), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Incident Handler (ECIH), Certified Ethical Hacker (CEH)...

Nội dung chính

01

NGUY CƠ ĐỐI VỚI CLOUD & SAAS

02

HƯỚNG TIẾP CẬN TỪ THREAT INTELLIGENCE

03

MỘT SỐ USE-CASE

04

DEMO





NGUY CƠ ĐỐI VỚI CLOUD SAAS



Lộ lọt dữ liệu

- Lộ lọt dữ liệu nhạy cảm
- Tác động nghiêm trọng về mặt tài chính, pháp lý và danh tiếng
- Trong một số trường hợp, hậu quả từ việc lộ lọt dữ liệu có thể đe dọa sự tồn tại của một tổ chức



Truy cập trái phép

- Rủi ro tăng cao về chiếm quyền tài khoản người dùng
- Thu thập thông tin đăng nhập người dùng thông qua dark web
- Nằm vùng lấy cắp thông tin hoặc rao bán tổng tiền



API không an toàn

- Một số API có thể thiếu cơ chế kiểm soát truy cập
- Dẫn đến việc truy cập không được ủy quyền vào dữ liệu nhạy cảm
- Cần quản lý lỗ hổng & phân quyền API



Shadow IT

- Các hệ thống, thiết bị, ứng dụng và dịch vụ được nhân viên hoặc các bộ phận sử dụng mà không được biết đến và giám sát bởi bộ phận IT, an ninh thông tin và pháp lý
- Rủi ro về các đầu vào cho tấn công không được quản lý



Quản lý lỗ hổng

- Các tổ chức khách hàng phụ thuộc vào các nhà cung cấp SaaS để thực hiện quản lý lỗ hổng hiệu quả
- Ngay cả một lỗ hổng duy nhất trong các công cụ SaaS cũng là cửa ngõ cho các kẻ tấn công vào dữ liệu của tổ chức

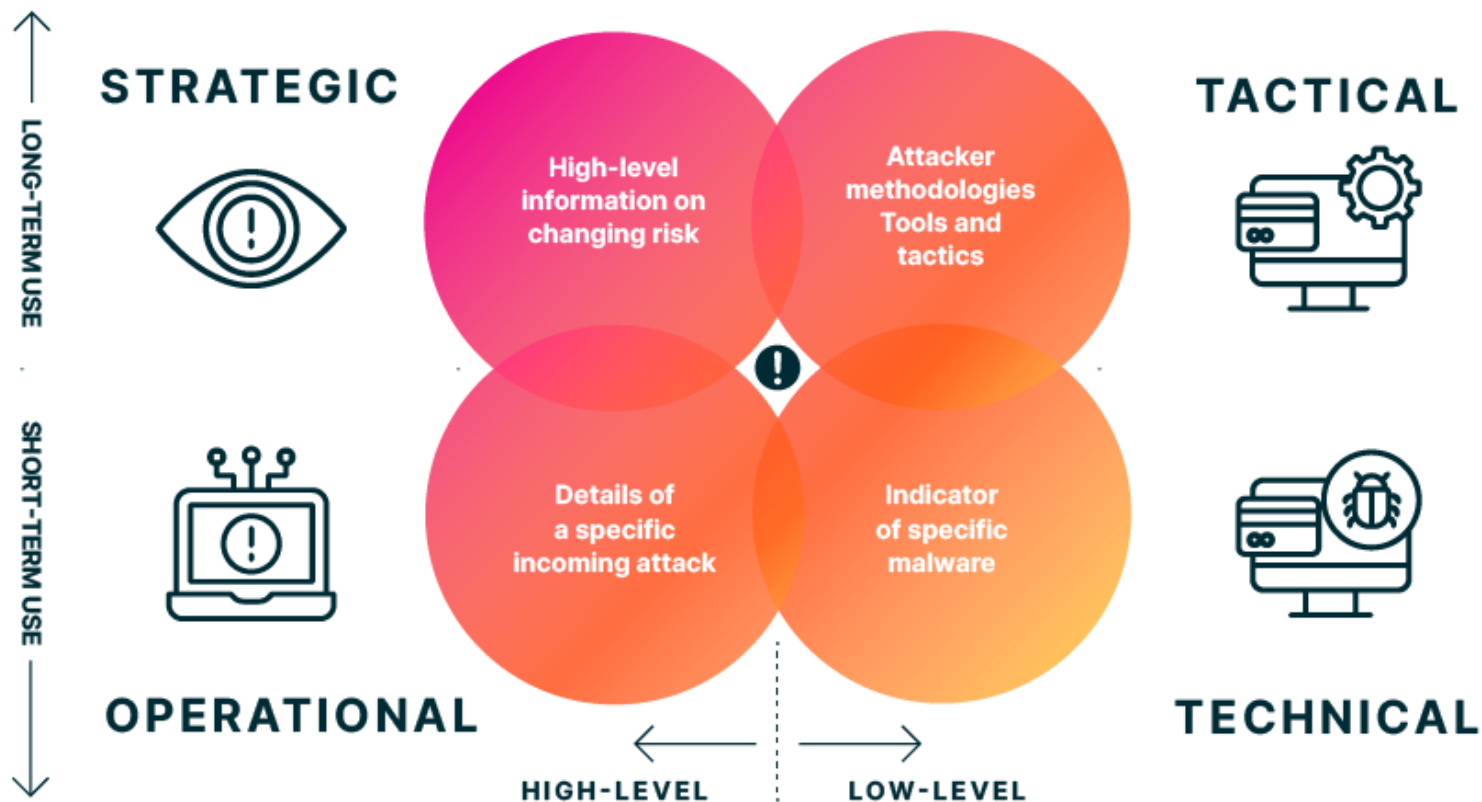


Rủi ro từ bên thứ ba

- Đánh giá rủi ro từ bên thứ ba để đánh giá và theo dõi rủi ro từ bên thứ ba
- Nhiều nhà cung cấp SaaS không chịu trách nhiệm trả lời các bảng câu hỏi về bảo mật
- Tổ chức sử dụng dịch vụ SaaS thường phải chấp nhận thông tin rủi ro ít chi tiết hơn



HƯỚNG TIẾP CẬN TỪ CYBER THREAT INTELLIGENCE



Chủ động phát hiện nguy cơ

- Cung cấp thông tin thời gian thực về các nguy cơ
- Chủ động phát hiện và giảm thiểu nguy cơ tiềm ẩn

Nâng cao khả năng phản ứng

- Phản ứng nhanh chóng và hiệu quả.
- Cung cấp ngữ cảnh về cuộc tấn công, các chiến thuật được sử dụng, và các dấu hiệu nhận biết xâm nhập (IoCs)

Cập nhật chính sách bảo mật

- Điều chỉnh chính sách an ninh dựa trên bối cảnh nguy cơ hiện tại
- Tự động cập nhật và điều chỉnh các giải pháp bảo mật



Phòng chống mã độc và phishing

- Xác định và chặn các URL, tên miền và địa chỉ email độc hại
- Tích hợp thông tin nguy cơ vào các giải pháp bảo mật cho email và web

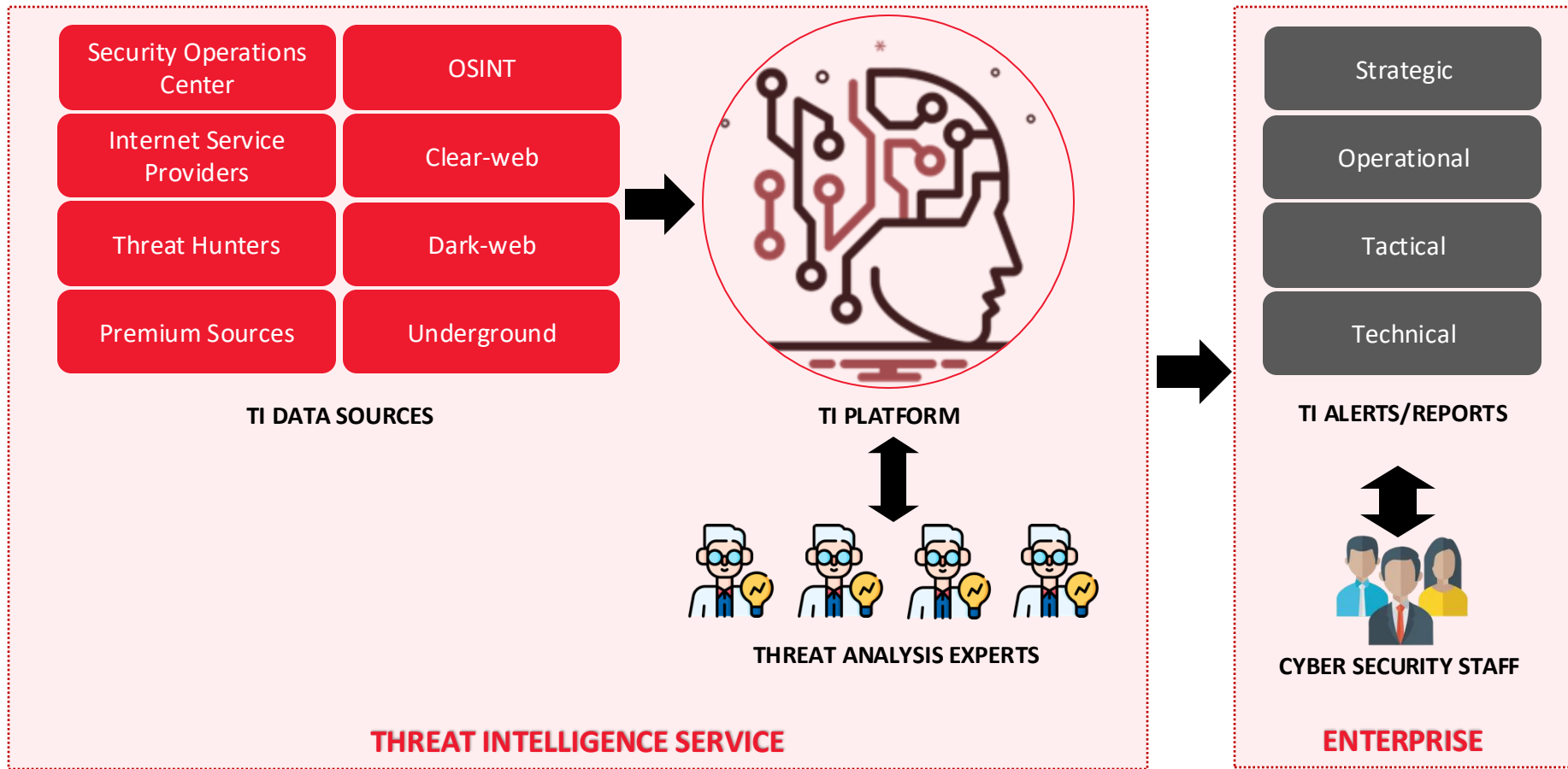
Bảo vệ dữ liệu khách hàng

- Phát hiện sớm và xử lý dữ liệu lộ lọt
- Tăng niềm tin của khách hàng và giữ cho tổ chức tuân thủ các quy định về bảo mật dữ liệu

Quản lý rủi ro bên thứ ba

- Cập nhật thông tin nguy cơ của các đối tác thứ ba của tổ chức
- Giúp tổ chức đánh giá và quản lý rủi ro từ các bên thứ ba

MÔ HÌNH CYBER THREAT INTELLIGENCE



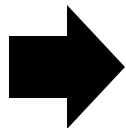


MỘT SỐ USE-CASE

USE CASE #1 – MACHINE READABLE TI



TI THREAT FEED



TI PLATFORM



SIEM



EDR



NSM



FIREWALL

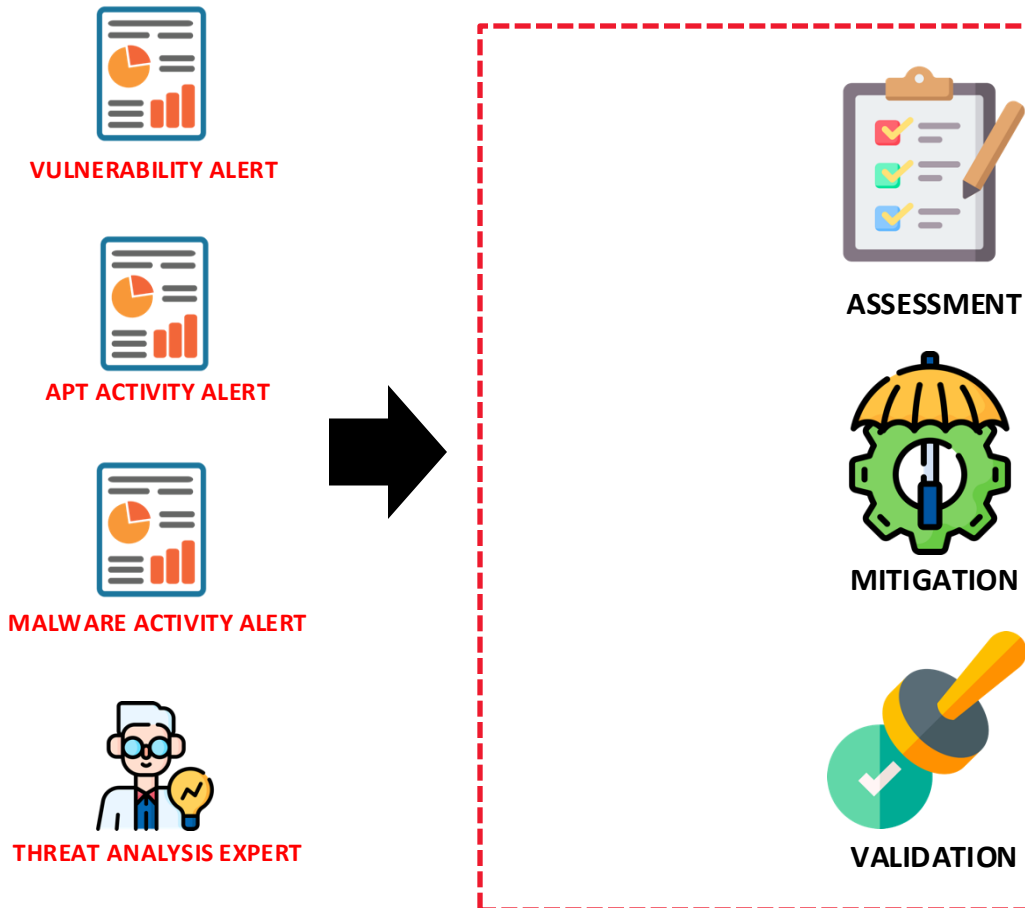


ANTIVIRUS



PROXY

USE CASE #2 – GENERIC THREATS ALERT



USE CASE #3 – BRAND PROTECTION



LEAKED DATA ALERT



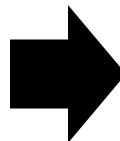
LEAKED CREDENTIALS ALERT



PHISHING ALERT



IMPERSONATION ALERT



THREAT RESPONDER



VERIFICATION



ENTERPRISE RESPONSE

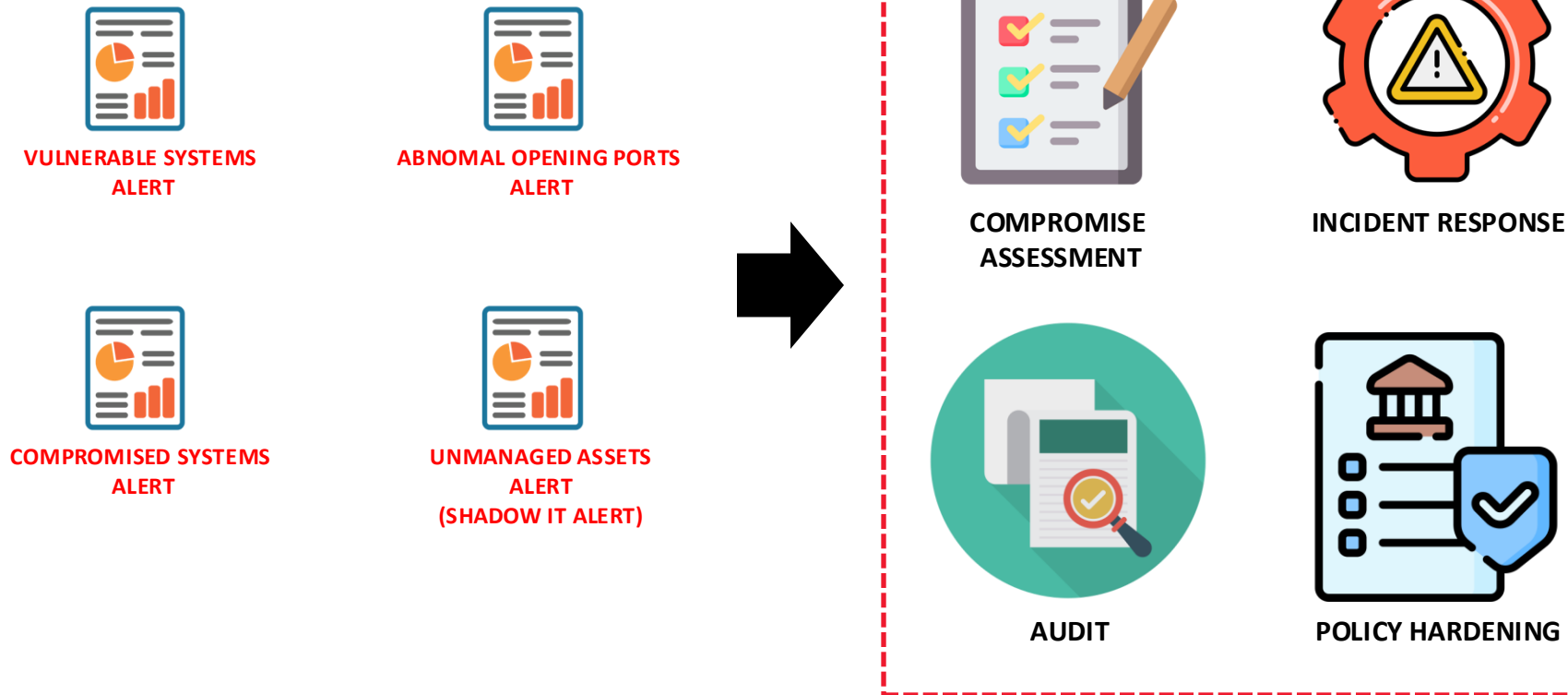


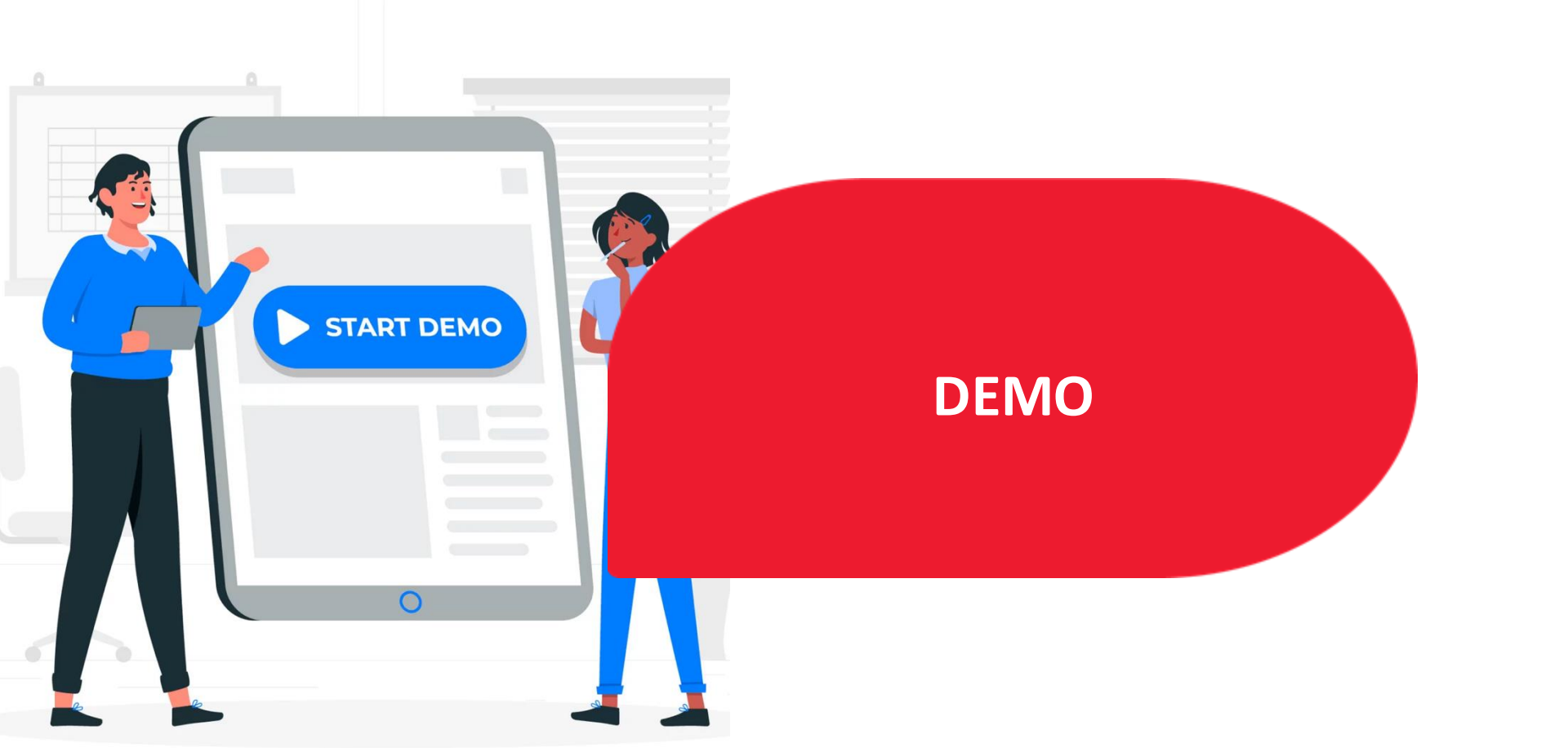
TAKEDOWN



REPORT & CLAIM

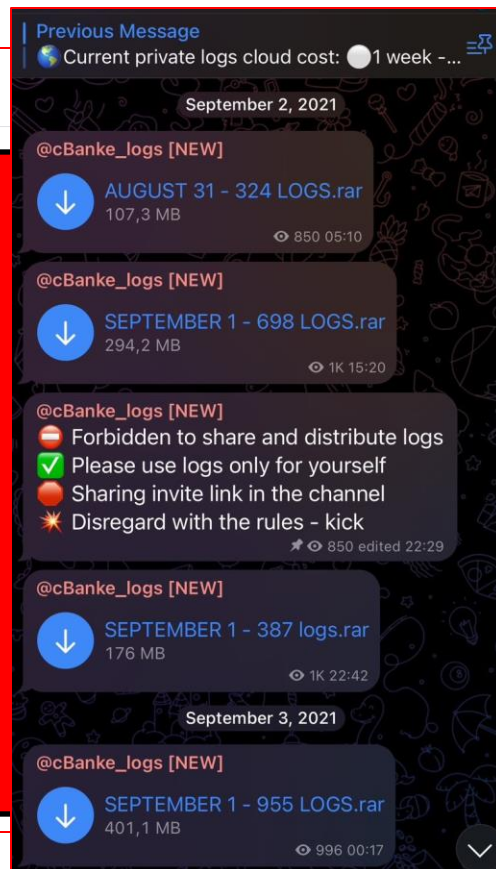
USE CASE #4 – EXTERNAL ATTACK SURFACE MANAGEMENT





DEMO – LEAKED CREDENTIALS

<input type="checkbox"/>	No.	Alert Time	Link
<input type="checkbox"/>	1	02:29:33 06/11/2023	https://online.
<input type="checkbox"/>	2	02:29:33 06/11/2023	https://online.
<input type="checkbox"/>	3	02:29:33 06/11/2023	https://online.
<input type="checkbox"/>	4	02:29:33 06/11/2023	https://online.
<input type="checkbox"/>	5	02:29:33 06/11/2023	https://online.
<input type="checkbox"/>	6	02:29:33 06/11/2023	https://online.
<input type="checkbox"/>	7	02:29:33 06/11/2023	https://online.
<input type="checkbox"/>	8	02:29:33 06/11/2023	https://online.
<input type="checkbox"/>	9	02:29:33 06/11/2023	https://online.
<input type="checkbox"/>	10	02:29:33 06/11/2023	https://online.



Password	Source
Piu*****	Stealer
Maj*****	Stealer
Tn2*****	Stealer
Azh*****	Stealer
097*****	Stealer
thu*****	Stealer
834*****	Stealer
Hie*****	Stealer
Hoa*****	Stealer
Anh*****	Stealer

DEMO – LEAKED DATA

The image is a screenshot of a Telegram chat window. On the left, there is a profile card for a user named 'facebooksec'. The card features an anime-style avatar of a girl with purple hair and a black bow. Below the avatar, it says 'MVP User' with a green dot. At the bottom of the card, there is a green 'S' icon and a list of statistics: Posts: 8, Threads: 3, Joined: Aug 2023, and Reputation: 20. The chat area shows a conversation. At the top, it says '13 minutes ago'. A message from 'facebooksec' says 'facebooksec Wrote:'. Below it, a message from 'xungzzz' says 'xungzzz Wrote: Can you provide me with proof that you have 1.7 million customer data?'. A red rectangular box highlights a series of messages. The first message in the box is from 'facebooksec' and says 'delete post, please check'. The second is from 'xungzzz' and says 'thank bro, i see it'. The third is from 'facebooksec' and says 'let me know when you're ready tomorrow'. The fourth is from 'xungzzz' and says 'can you send me source of data?'. The fifth is from 'facebooksec' and says 'tomorrow, i'll send 45 XMR other.' Each message in the red box has a checkmark icon to its right. The background of the chat is dark grey.

DEMO – LEAKED SOURCE-CODE

<> Code Issues Pull requests Actions Projects Security Insights

fakebill [REDACTED] Public

main

Go to file

Branches Tags

first commit

css

js

mb

path

vendor

.rescache

README.md

index.html

Your commit message here

fakebill [REDACTED] BANK

[REDACTED] Add files via upload 84f63b0 last week 4 commits

Cấu hình ITom.docx	Add files via upload	last week
F5 - Virtual Server and iRules Configu...	Add files via upload	last week
HƯỚNG DẪN CÀI ĐẶT AGENT ITOM....	Add files via upload	last week
HƯỚNG DẪN TẠO POLICY NETSTAT ...	Add files via upload	last week
HƯỚNG DẪN TẠO POLICY NETSTAT ...	Add files via upload	last week
Hướng dẫn cấu hình giám sát cho IT...	Add files via upload	last week
ITOM	Create ITOM	last week
KPI 1st 6 month 2023_thaitd2.xlsx	Add files via upload	2 weeks ago
OBM_How to edit process monitor p...	Add files via upload	last week
README.md	Initial commit	2 weeks ago
Sitescope - Cài đặt, cấu hình, tích hợ...	Add files via upload	last week
[REDACTED] BANK- OBM Hướng dẫn triển khai...	Add files via upload	last week
[REDACTED] Bank - IT Create User - ITOM Guid...	Add files via upload	last week
[REDACTED] Bank - IT Service Perfection - ITOM...	Add files via upload	last week

DEMO – PHISHING DOMAINS

Affected Victim

Banking

Nâng Hạn Mức Thẻ Tín Dụng - EMS

Tư vấn tài chính · 1 người theo dõi · 2 bài viết trong 2 tuần qua

Theo dõi



Trung Tâm Nâng Hạn Mức Thẻ Tín Dụng 247

Agency quảng cáo · 1.5 km · 10 người theo dõi

Theo dõi

Nâng Hạn Mức Thẻ Tín Dụng - Ưu Tiên Từ Thẻ Tín Dụng

Dịch vụ tài chính · 2 người theo dõi · 2 bài viết trong 2 tuần qua

Theo dõi



Nâng Cấp Hạn Mức

Dịch vụ tư vấn tín dụng · 1 bài viết trong 2 tuần qua

Theo dõi

Nâng Hạn Mức Thẻ Tín Dụng - Ưu Tiên Từ Thẻ Tín Dụng SME

Dịch vụ tài chính

Dịch Vụ Xét Hạn Nâng Hạn Mức Thẻ Tín Dụng

Dịch vụ tài chính · 2 bài viết trong 2 tuần qua

Thẻ tín dụng hạn mức cao , nâng hạn mức thẻ tín dụng vp

Tư vấn tài chính · 4 người theo dõi · Hơn 10 bài viết trong 2 tuần qua
Tư vấn mở thẻ tín dụng hạn mức cao , nâng thẻ Vpbank , vay tín chấp cá nhân và doanh nghiệp ạ 🍀🍀🍀

Dịch Vụ Xét Hạn Nâng Hạn Mức Thẻ Tín Dụng

lúc 11:21 · 🌐

🔥 LỖ CHI TIÊU QUÁ TAY 🔥

🔥 THẺ CHỈ CÒN S.O.S HẠN MỨC 🔥

🔥 Bạn đã biết đến dịch vụ nâng hạn mức chỉ trong 1 NỐT NHẠC chưa ?

Điều kiện nâng hạn chỉ cần **BẠN ĐANG SỞ HỮU THẺ TÍN DỤNG** (Visa, Master, Jcb, Amex)

👉 **THỦ TỤC** vô cùng đơn giản chỉ cần không trả chậm thẻ và có giao dịch phát sinh trong 1 tháng gần nhất.

👉 **Hỗ trợ nâng TẤT CẢ** các dòng thẻ của tất cả các ngân hàng

👉 **Nâng tối đa 3 lần** hạn mức được cấp lúc đầu

👉 **Thủ tục đơn giản** phí chỉ 5%

👉 **An toàn**, bảo mật thông tin chủ thẻ tuyệt đối.

👉 **Có hỗ trợ online** cho khách tỉnh

✅ **Giải ngân hạn mức** sau 30p

Liên hệ ngay để được hỗ trợ

☎ Hotline/Zalo :

#nanghanmuc #nanghanmucthetindung #nanghanmucthetoanquoc #sangngangthetindung



Sản phẩm/Dịch vụ

Theo dõi

Chương trình nâng HẠN MỨC THẺ TD khủng

📌 RA THẺ 300 - 500TR + thêm Thấu Trì 200tr

📌 TỔNG GIẢI NGÂN LÊN TỚI 1 TỶ

>> Điều kiện đơn giản:

- Có 1 thẻ nhỏ sử dụng trên 2 tháng

- Không trả chậm, Nợ xấu

- Bao hồ sơ A - Z

- Giải ngân & nhận thẻ trong 30 - 45 ngày

Lưu ý: Chỉ hỗ trợ 100 khách hàng liên hệ sớm nhất

📌 Comment hoặc nhắn tin để được tư vấn & hướng dẫn cụ thể



10

14:24:33 15/11/2023

Domain

nanmuctne-nangnanmuc247.com

Banking

[Mã độc] Cảnh báo dòng mã độc của nhóm tấn công APT32

Mức độ: **TRUNG BÌNH**

Threat ID : VTI_2023_5404

Nguồn: Viettel Threat Intelligence

Thời gian : 17/

Thông tin kỹ thuật

Tổng quan

VCS-TI cảnh báo nhóm mã độc APT32 tấn công một số Spectralviper, P8loader và Powerseal nhằm thay đổi quy trình tấn công thường tấn công vào lĩnh vực tổ chức, doanh nghiệp thông tin và kịp thời đưa ra phương án để ngăn ngừa.

Thông tin mã độc, chiến dịch tấn công

- Tên mã độc: SPECTRALVIPER
- Dòng mã độc: Trojan
- Nhóm tấn công: APT32
- Quy mô/ đối tượng ảnh hưởng: Lĩnh vực tổ chức,

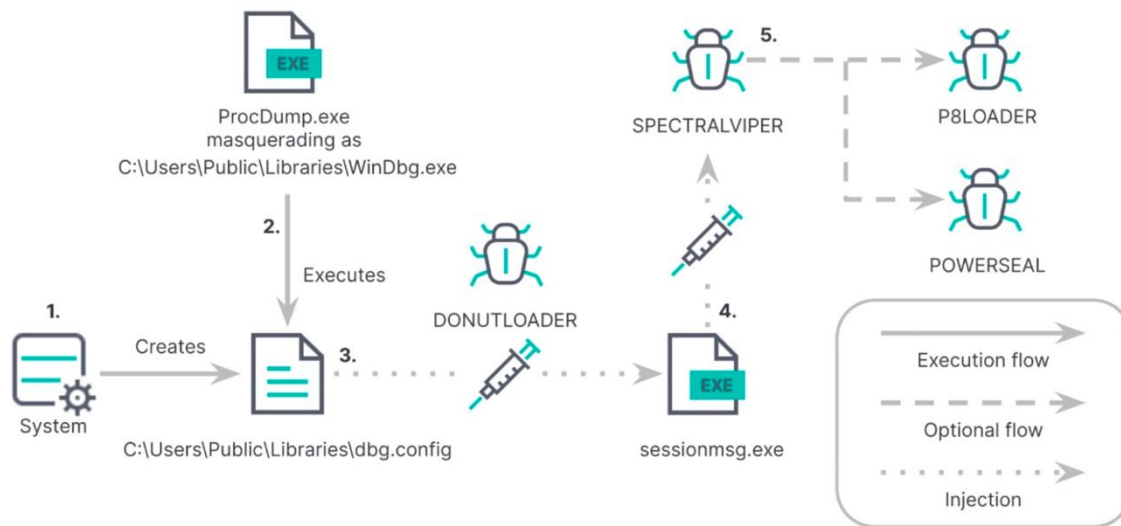
Nội dung

Dựa trên các tiêu chí:

- Chiến dịch tấn công APT nhằm vào các doanh nghiệp
- Nhóm tin tặc có tiền sử nhắm vào Việt Nam.
- Chiến dịch tấn công đã diễn ra trên thời gian dài.

VCS-TI nhận định đây là nguy cơ mức độ **Trung bình**.

Chuỗi tấn công của nhóm mã độc APT32 được mô tả thông qua sơ đồ dưới đây:



Trong chiến dịch tấn công, nhóm tin tặc APT32 đã sử dụng một số mã độc bao gồm mã độc Donutloader, Spectralviper, P8loader và Powerseal. Chuỗi tấn công của mã độc bắt đầu bằng payload Donutloader có tên `dbg.config` được tải lên máy nạn nhân thông qua SMB từ một hệ thống đã bị tin tặc xâm nhập từ trước đó. Sau đó nhóm tấn công sử dụng tiến trình ProcDump trong bộ công cụ SysInternals của Microsoft để tải payload mã độc `dbg.config` và inject vào mã độc vào tiến trình `sessionmsg.exe`. Nhằm tránh bị phát hiện, nhóm tấn công đã đổi tên công cụ ProcDump thành Windbg.

[Mã độc] C

Mức độ: CAO
Threat ID : VT

Tổng quan

VCS-TI cảnh báo
dùng giả mạo có
Quản trị viên cần

Thông tin

- Quy mô/ đ

Nội dung

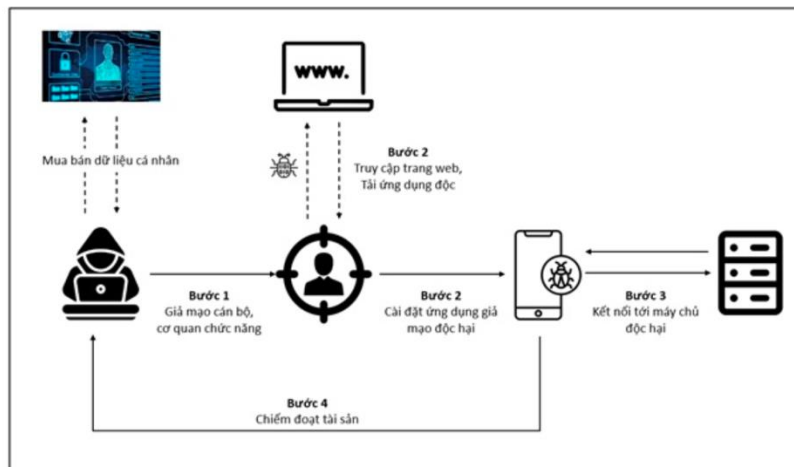
Dựa trên các tiêu

- Chiến dịch
- Mã độc ph
- Chiến dịch

VCS-TI nhận đ

Kịch bản tấn công:

Sơ bộ các bước lừa đảo được mô tả trong hình:



(Nguồn: Viettel Threat Intelligence)

1. Đối tượng mạo danh cán bộ, công chức, viên chức, người có thẩm quyền yêu cầu nạn nhân cung cấp thông tin phục vụ nghiệp vụ. Sau đó hướng dẫn nạn nhân truy cập đường dẫn độc hại để cài đặt ứng dụng giả mạo nhằm mục đích lừa đảo.
2. Nạn nhân truy cập đường dẫn, tải và cài đặt ứng dụng giả mạo về điện thoại.
3. Ứng dụng giả mạo yêu cầu cấp quyền Accessibility, nạn nhân bấm "Cho phép", ứng dụng có quyền truy cập, đánh cắp thông tin trên điện thoại của nạn nhân.
4. Ứng dụng rà soát các ứng dụng hợp lệ trong máy nạn nhân để tìm kiếm ứng dụng ngân hàng và các thông tin nhạy cảm, đánh cắp thông tin tài khoản ngân hàng, SMS, ... gửi về cho đối tượng tấn công, từ đó đối tượng có thể chiếm đoạt tài sản của nạn nhân.

phủ

lặt các ứng
t bị nạn nhân.

viettel
security

***Trân trọng cảm
ơn!***