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

Công ty An ninh mạng Viettel

viettel security

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

viettel security

NGUY CƠ ĐỐI VỚI CLOUD SAAS

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 tống 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

**Nguồn: ISACA (isaca.org)*

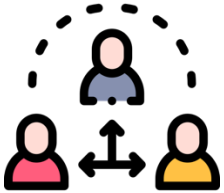
NGUY CƠ ĐỐI VỚI CLOUD & SAAS

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



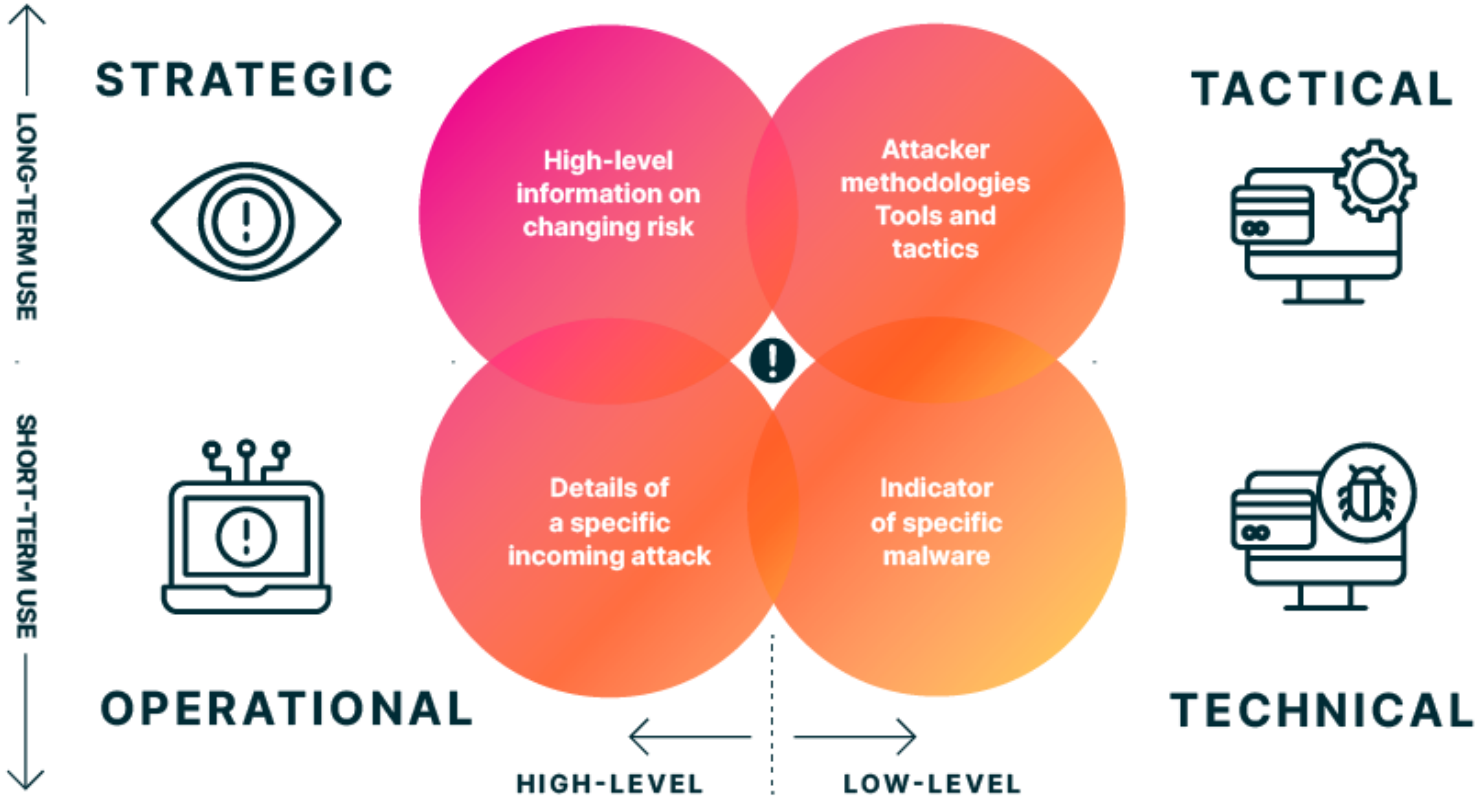
Rủi ro từ bên thứ ba

- 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

**Nguồn: ISACA (isaca.org)*

HƯỚNG TIẾP CẬN TỪ CYBER THREAT INTELLIGENCE

CYBER THREAT INTELLIGENCE



CYBER THREAT INTELLIGENCE

viettel security

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

viettel security

Security Operations Center

OSINT

Internet Service Providers

Clear-web

Threat Hunters

Dark-web

Premium Sources

Underground

TI DATA SOURCES

TI PLATFORM

THREAT ANALYSIS EXPERTS

THREAT INTELLIGENCE SERVICE

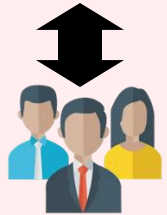
Strategic

Operational

Tactical

Technical

TI ALERTS/REPORTS



CYBER SECURITY STAFF

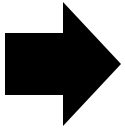
ENTERPRISE

MỘT SỐ USE-CASE

USE CASE #1 – MACHINE READABLE TI

viettel security

TI THREAT FEED



TI PLATFORM

SIEM

EDR

NSM

FIREWALL

ANTIVIRUS

PROXY

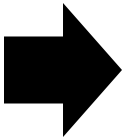
USE CASE #2 – GENERIC THREATS ALERT

VULNERABILITY ALERT

APT ACTIVITY ALERT

MALWARE ACTIVITY ALERT

THREAT ANALYSIS EXPERT



ASSESSMENT

MITIGATION

VALIDATION

USE CASE #3 – BRAND PROTECTION

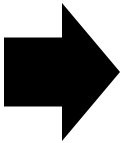
LEAKED DATA ALERT

LEAKED CREDENTIALS ALERT

PHISHING ALERT

IMPERSONATION ALERT

THREAT RESPONDER



VERIFICATION

ENTERPRISE RESPONSE

TAKEDOWN

REPORT & CLAIM

USE CASE #4 – EXTERNAL ATTACK SURFACE MANAGEMENT

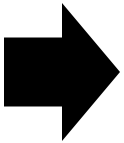
viettel security

VULNERABLE SYSTEMS ALERT

ABNOMAL OPENING PORTS ALERT

COMPROMISED SYSTEMS ALERT

UNMANAGED ASSETS ALERT (SHADOW IT ALERT)

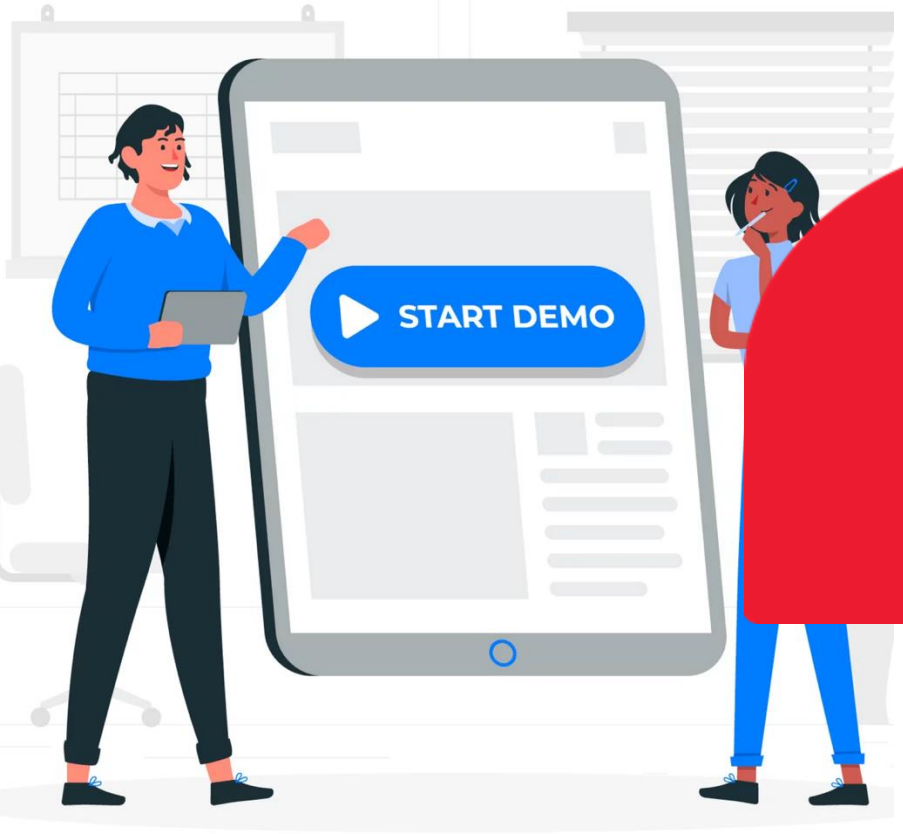


COMPROMISE ASSESSMENT

INCIDENT RESPONSE

AUDIT

POLICY HARDENING

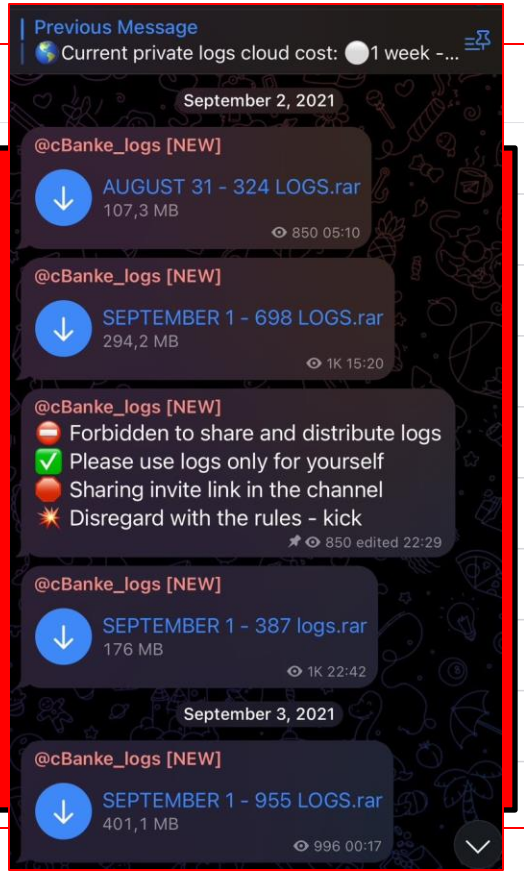


DEMO

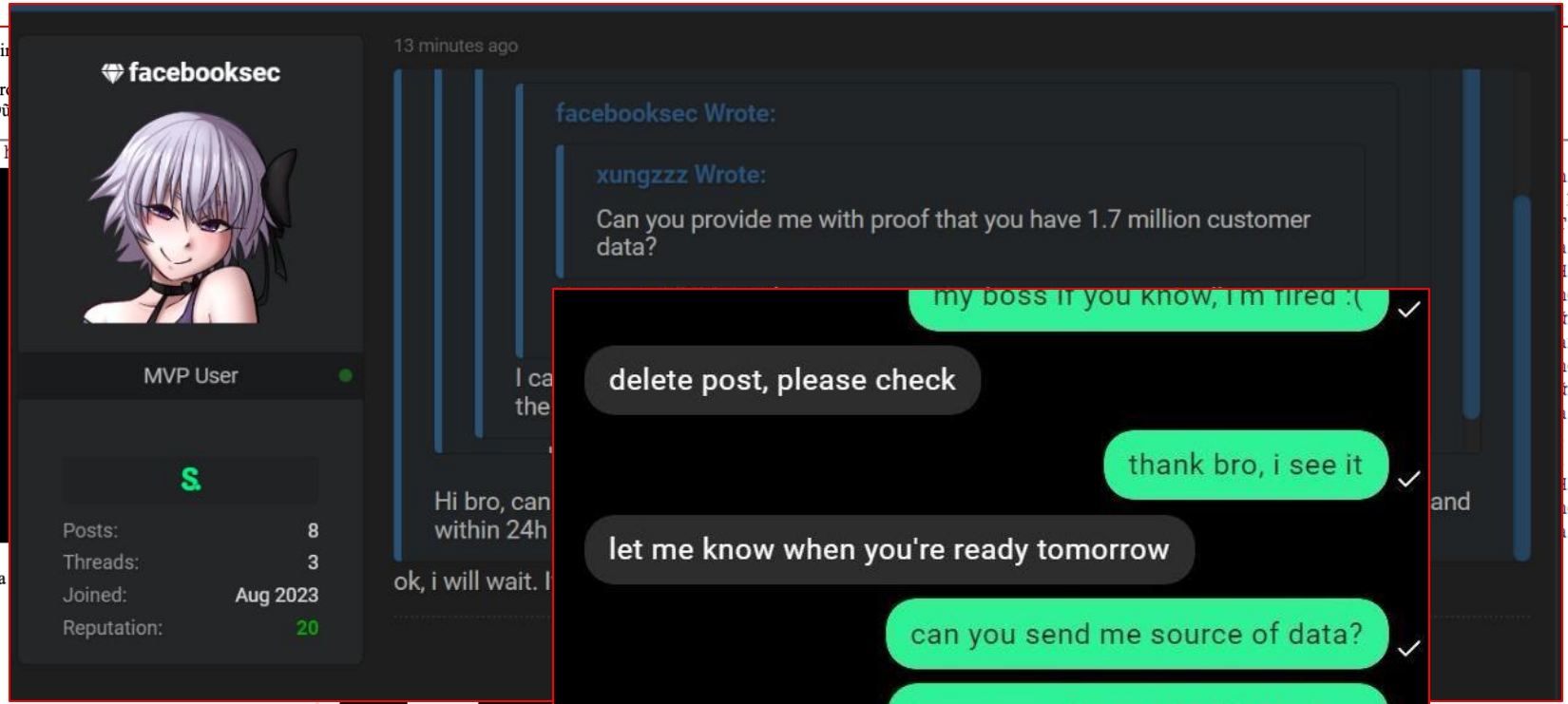
DEMO – LEAKED CREDENTIALS

viettel security

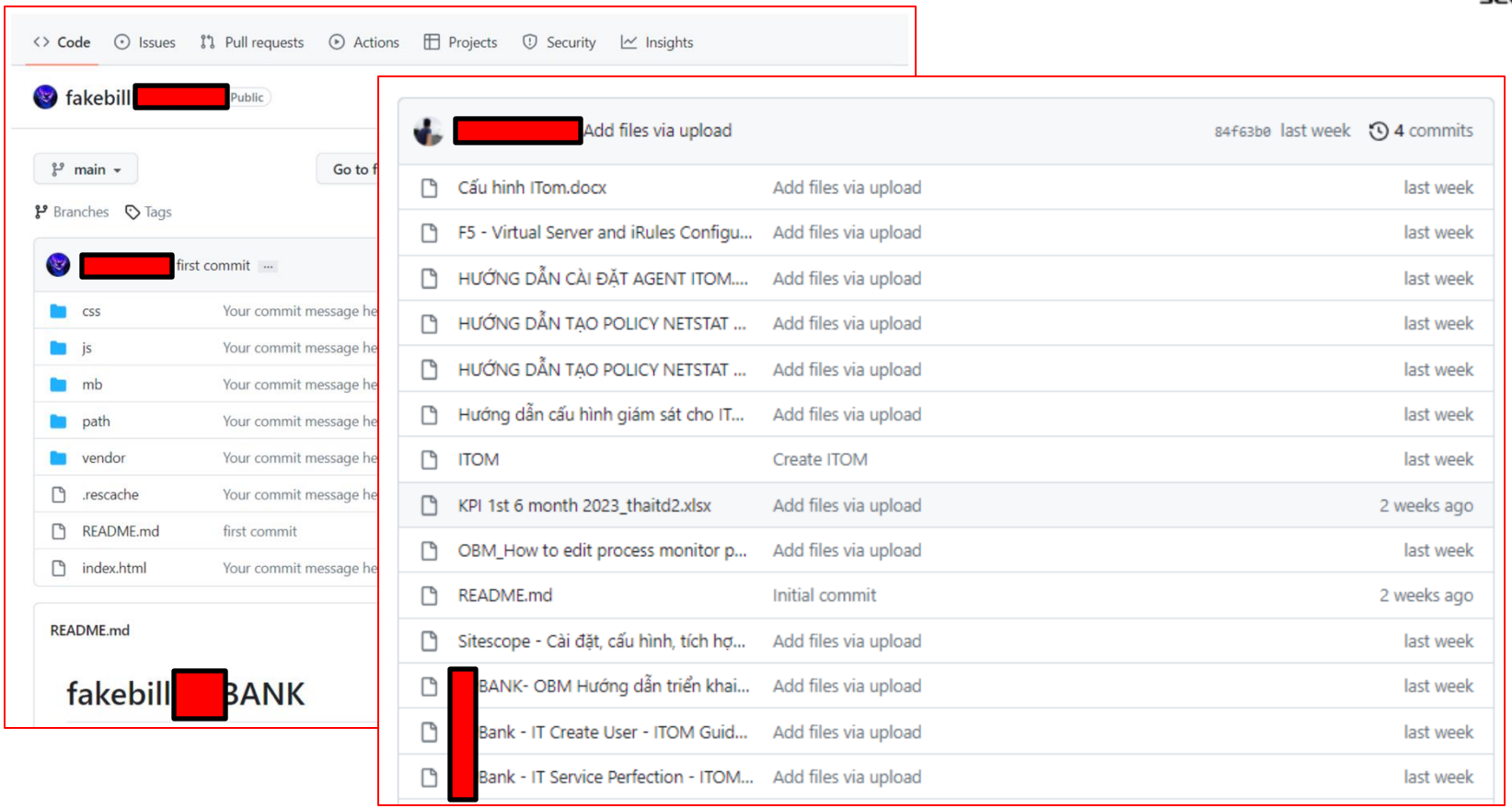
No.	Alert Time	Link	Password	Source
1	02:29:33 06/11/2023	https://online.	Piu*******	Stealer
2	02:29:33 06/11/2023	https://online.	Mai******************	Stealer
3	02:29:33 06/11/2023	https://online.	Tn2******	Stealer
4	02:29:33 06/11/2023	https://online.	Azh********	Stealer
5	02:29:33 06/11/2023	https://online.	097*******	Stealer
6	02:29:33 06/11/2023	https://online.	thu*******	Stealer
7	02:29:33 06/11/2023	https://online.	834**********	Stealer
8	02:29:33 06/11/2023	https://online.	Hie*****	Stealer
9	02:29:33 06/11/2023	https://online.	Hoa**********	Stealer
10	02:29:33 06/11/2023	https://online.	Anh*****	Stealer



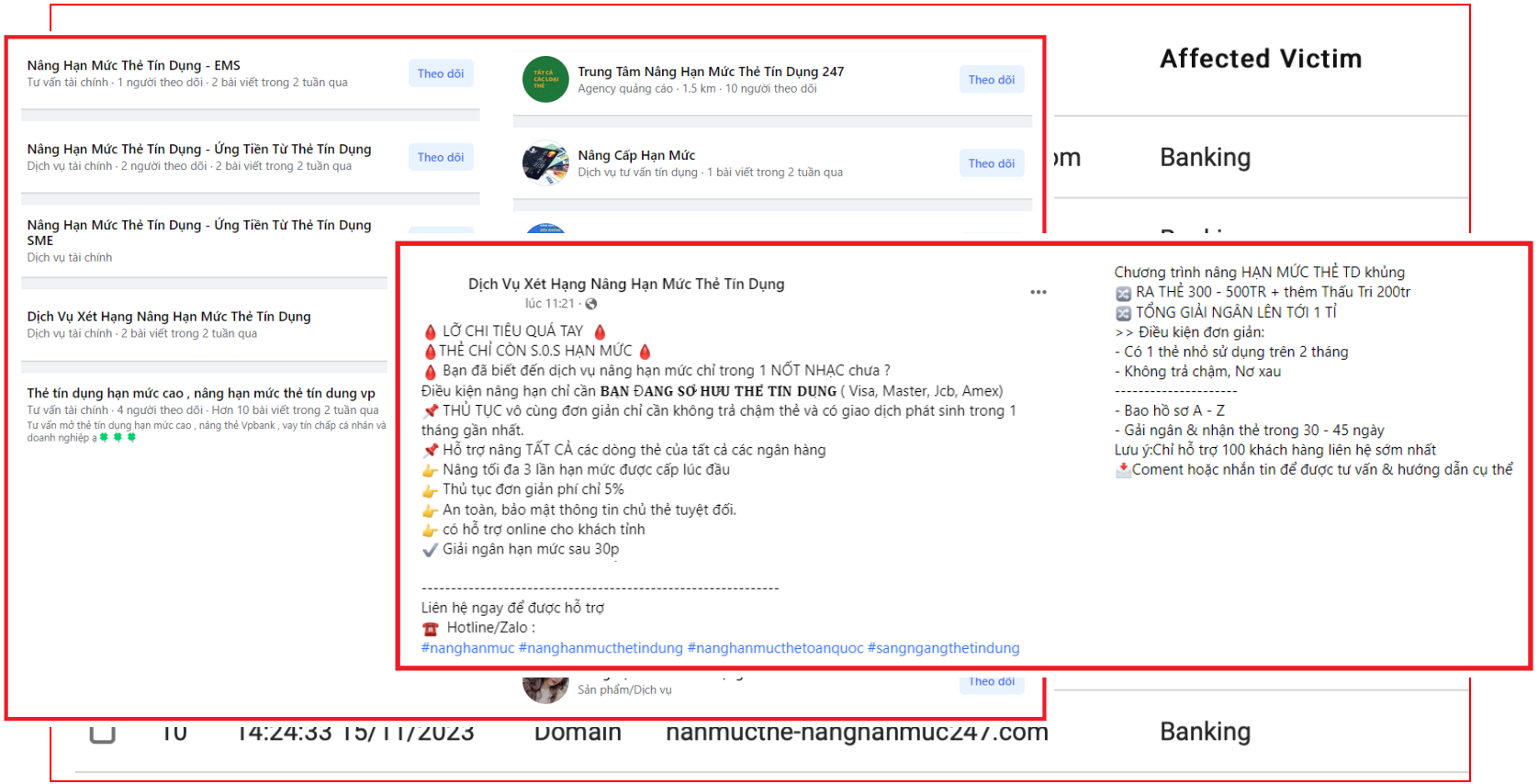
DEMO – LEAKED DATA



DEMO – LEAKED SOURCE-CODE



DEMO – PHISHING DOMAINS



DEMO – APT ATTACK

[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:

Tổng quan

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

Thông tin mã độc, chiến dịch tấn c

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

Nội dung

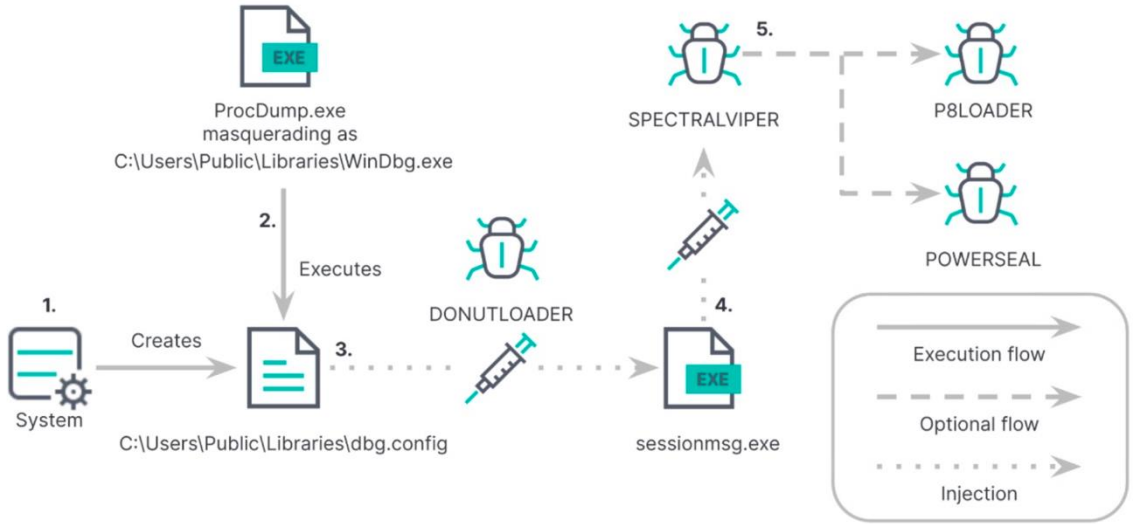
Dựa trên các tiêu chí:

- Chiến dịch tấn công APT nhắm vào các doanh ng
- 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.**

Thông tin kĩ thuật

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 SystInternals 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.

DEMO - MALWARE

[Mã độc] C

Mức độ: CAO
Threat ID : VT

Tổng quan

VCS-TI cảnh bá
dụng giả mạo có
Quản trị viên cầ

Thông tin

- Quy mô/ đ

Nội dung

Dựa trên các tiê

- Chiến dịch
- Mã độc ph
- Chiến dịch

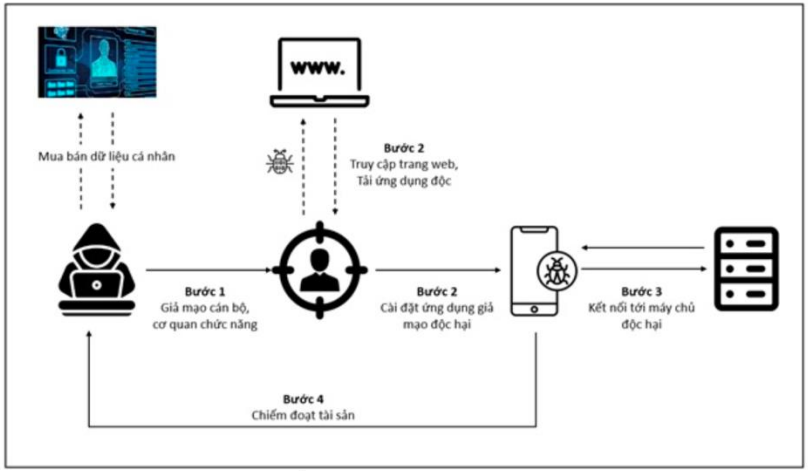
VCS-TI nhận đị

phủ

ặt các ứng
t bị nạn nhân.

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.

viettel
security

Trân trọng cảm ơn!