**Ví dụ về cấu trúc báo cáo phân tích mã độc**

Tùy thuộc vào định dạng báo cáo và đối tượng đọc, cấu trúc báo cáo sẽ khác nhau. Dưới đây là các chi tiết cần bao gồm trong các định dạng phổ biến.

**1. Báo cáo kỹ thuật (Technical Article)**

Đối tượng: Nhóm kỹ thuật (SOC, Incident Response Team, Malware Analysts).

**Nội dung cần có:**

1. **Thông tin mẫu mã độc (Sample details):**
   * Hashes: MD5, SHA1, SHA256.
   * Dấu thời gian biên dịch (Compilation timestamps).
   * Loại file và kích thước (File types and sizes).
   * Tên file được sử dụng trong thực tế (In-the-wild filenames).
   * Thông tin nhận diện từ các hãng AV (AV vendors’ detections).
2. **Mối quan hệ giữa các module (nếu có nhiều module):**
   * Sự liên kết giữa các module khác nhau trong mã độc (ví dụ: loader, payload, plugin).
3. **Chi tiết từng module:**
   * Mô tả chức năng chính.
   * Cơ chế duy trì sự hiện diện (**Persistence mechanisms**).
4. **Giao tiếp mạng (Network communications):**
   * Giao thức được sử dụng (Protocols).
   * Thuật toán mã hóa và các khóa mã hóa (Encryption algorithms and keys).
   * Chi tiết C&C (Command and Control):
     + Địa chỉ IP, tên miền, URL.
     + Thông tin Whois.
     + Quốc gia nơi máy chủ được lưu trữ.
5. **Các kỹ thuật chống phân tích ngược (Anti-reverse engineering techniques):**
   * Ví dụ: Obfuscation, Packing, Anti-debugging, Anti-VM.
6. **IoCs (Indicators of Compromise):**
   * Hashes, filenames, địa chỉ IP, tên miền liên quan.
7. **Quy tắc phát hiện (Detection rules):**
   * YARA, Snort, hoặc các quy tắc phát hiện khác.

**2. Bài viết dành cho công chúng (General-Public Article)**

Đối tượng: Người không chuyên về kỹ thuật (CISO, công chúng, báo chí).

**Nội dung cần có:**

1. **Mô tả chức năng tổng quan (High-level functionality):**
   * Tóm tắt cách mã độc hoạt động ở mức cao (không đi sâu vào kỹ thuật).
   * Tác động của mã độc (nguy cơ, thiệt hại).
2. **Quy mô của cuộc tấn công (The scale of the attack):**
   * Phạm vi và quy mô ảnh hưởng của cuộc tấn công.
   * Tổ chức, cá nhân hoặc ngành bị nhắm đến.
3. **Hồ sơ nạn nhân (Victim profile):**
   * Loại tổ chức bị tấn công (chính phủ, doanh nghiệp, cá nhân).
   * Địa lý của nạn nhân (Victims’ geolocation).
   * Ước tính thiệt hại (Loss estimates).
4. **Nguồn gốc tác nhân (Actor attribution):**
   * Sự tương đồng với các mẫu mã độc khác (Sample similarity).
   * IoCs khớp với các cuộc tấn công trước (hashes, filenames, network artifacts).
   * Chuỗi ngôn ngữ và codepages sử dụng.
   * Dấu thời gian biên dịch (Compilation timestamps).

**Ví dụ cấu trúc cho từng loại bài viết**

**Báo cáo kỹ thuật:**

markdown

Sao chépChỉnh sửa

### 1. Sample Details

- MD5: `<hash>`

- SHA256: `<hash>`

- File Type: PE32 Executable

- Compilation Timestamp: `2024-12-12 10:00:00 UTC`

### 2. Main Functionality

- Primary module downloads additional payload.

- Persistence achieved by modifying registry key: `HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`.

### 3. Network Communication

- Protocol: HTTPS

- C&C Server: `example[.]com`

- Encryption: Custom XOR-based encryption.

### 4. Anti-Reverse Engineering

- Packed using UPX.

- Employs anti-debugging checks with `IsDebuggerPresent`.

### 5. IoCs

- Hashes: `<list of hashes>`

- Domains: `malicious[.]com`

- YARA Rule: `<rule content>`

**Bài viết dành cho công chúng:**

markdown

Sao chépChỉnh sửa

### 1. Overview

This malware is designed to steal credentials from financial institutions and exfiltrate sensitive data.

### 2. Impact

- Targets include banks and financial services in Europe and North America.

- Estimated losses: $2 million USD.

### 3. Victim Profile

- Regions: USA, Germany, and France.

- Targeted organizations: Financial institutions.

### 4. Attribution

- Similarities with known APT groups targeting financial services.

- Language indicators suggest Eastern European origin.

**Tóm tắt**

* Báo cáo kỹ thuật nên chi tiết, tập trung vào IoCs, hành vi mã độc và các cơ chế chính.
* Bài viết dành cho công chúng nên dễ hiểu, tập trung vào tác động và thông tin tổng quan.
* Luôn điều chỉnh cấu trúc và mức độ chi tiết dựa trên đối tượng đọ