

# Báo cáo nghiên cứu: Ransomware (Tổng quan)

Tác giả: [Bùi Việt Dũng] | Đơn vị: [CHỮ TOÀN CHỮ] | Ngày: [23/03/2025]

**Tuyên bố sử dụng hợp pháp:** Tài liệu này phục vụ mục đích **nghiên cứu bảo mật, nâng cao phòng thủ và ứng phó sự cố**. Nội dung không nhằm hướng dẫn phát triển hay phát tán phần mềm độc hại.

## Mục lục

1	Giới thiệu	1
2	Cấu trúc thành phần điển hình	2
3	Kỹ thuật thường gặp	4
3.1	Vector xâm nhập	4
3.2	Dropper/Loader	4
3.3	Payload chính	5
3.4	Persistence	6
3.5	Liên lạc chỉ huy & điều khiển (C2)	6
3.6	Né tránh & Chống phân tích (Evasion & Anti-Analysis)	7
4	Hành vi quan sát được	7
5	Chỉ số nhận diện (IoCs) — ví dụ định dạng báo cáo	8
6	Kết luận	9
A	Phụ lục A — Checklist ứng phó sự cố (IR) rút gọn	9
B	Phụ lục B — Thuật ngữ	11
C	Phụ lục C — Ánh xạ chiến thuật MITRE ATT&CK (rút gọn)	11
D	Phụ lục D — Telemetry & Nhật ký nên bật/soi	12
E	Phụ lục E — Mẫu biểu IoC (điền nhanh)	12
F	Phụ lục F — Khung Timeline điều tra (tham khảo)	13
G	Phụ lục G — Phân biệt Locker vs. Crypto Ransomware (nhanch)	13

## 1 Giới thiệu

Ransomware là phần mềm độc hại nhằm mã hoá dữ liệu của nạn nhân và yêu cầu tiền chuộc để khôi phục. Trong những năm gần đây, ransomware trở thành mối đe dọa nổi bật trên toàn cầu, gây gián đoạn vận hành và thiệt hại tài chính đáng kể cho cá nhân, doanh nghiệp và tổ chức. Báo cáo này tổng hợp *tổng quan* về cấu trúc thành phần, kỹ

thuật, hành vi và các biện pháp phòng thủ cấp cao, phục vụ mục tiêu phòng ngừa và ứng phó.

## 2 Cấu trúc thành phần điển hình

Một mẫu ransomware hiện đại thường không chỉ đơn giản là một đoạn mã độc hại, mà được thiết kế thành nhiều thành phần riêng biệt phối hợp nhịp nhàng. Các thành phần này đảm nhận từ khâu xâm nhập, triển khai, gây hại, duy trì sự tồn tại, cho đến che giấu hành vi và đối phó với phân tích. Cấu trúc điển hình bao gồm:

- **Vector xâm nhập:** Đây là con đường để mã độc xâm nhập ban đầu vào hệ thống nạn nhân. Có rất nhiều kỹ thuật được sử dụng, điển hình như: *email lừa đảo/phishing* với file đính kèm độc hại hoặc macro, khai thác lỗ hổng zero-day hoặc các dịch vụ public-facing (RDP brute force, VPN exploit, lỗ hổng web), lộ lọt thông tin xác thực từ các chợ ngầm, cấy ghép trong phần mềm crack/ứng dụng giả mạo, hoặc thông qua chuỗi cung ứng (supply chain attack). Một số ransomware còn tận dụng kỹ thuật *malvertising* hoặc drive-by-download để tăng tốc độ lây nhiễm.
- **Dropper/Loader:** Đây là giai đoạn trung gian, thường là các tệp thực thi nhỏ gọn. Chúng có thể thực hiện kiểm tra môi trường (sandbox detection, VM check, anti-debug) để đảm bảo an toàn trước khi triển khai payload chính. Dropper/Loader thường giải nén, tải về từ xa, hoặc giải mã payload ẩn trong chính nó. Đặc biệt, nhiều ransomware hiện đại sử dụng *fileless techniques* (PowerShell, WMI, reflective DLL injection) khiến chúng không cần ghi file lên ổ đĩa mà hoạt động trực tiếp trong bộ nhớ, từ đó tránh bị phát hiện.
- **Payload chính:** Thành phần cốt lõi đảm nhận chức năng phá hoại và tống tiền, gồm nhiều module:
  - (i) *Crypto*: mã hóa dữ liệu/tài nguyên trên máy nạn nhân, thường dùng thuật toán lai ghép (AES + RSA/ECC) để vừa nhanh vừa an toàn.
  - (ii) *Stealer/Exfiltration*: đánh cắp dữ liệu nhạy cảm (tài khoản, cookies, email, tài liệu) để phục vụ mô hình tống tiền kép hoặc bán cho bên thứ ba.
  - (iii) *Ransom Note/Ransom Screen*: hiển thị thông báo tống tiền, hướng dẫn cách thanh toán, thậm chí khóa toàn bộ màn hình (lock screen).
  - (iv) *Worm/Propagator*: tự động lây lan trong mạng nội bộ qua SMB, RDP, USB hoặc email.
  - (v) *Killer/Disabler*: tìm và vô hiệu hóa tiến trình antivirus, EDR, backup, shadow copies nhằm ngăn khôi phục dữ liệu.
- **Persistence:** Để đảm bảo sự tồn tại qua nhiều phiên làm việc, ransomware thường áp dụng hàng loạt kỹ thuật duy trì: (i) tạo *Registry Run Keys* hoặc *Scheduled Tasks*, (ii) cài đặt dưới dạng *Windows Service* hoặc *Kernel Driver*, (iii) sao chép vào thư mục **Startup**, (iv) *DLL hijacking* hoặc *process injection* vào tiến trình hợp pháp, (v) chỉnh sửa *Winlogon*, (vi) cài đặt bootkit/rootkit để có quyền kiểm soát từ tầng kernel, (vii) vô hiệu hóa hoặc xóa *Shadow Copies/Backup*, xóa restore point. Tổ hợp kỹ thuật này giúp ransomware bám trụ dai dẳng và khó bị gỡ bỏ.

- **Liên lạc chỉ huy & điều khiển (C2):** Ransomware thường cần liên lạc với máy chủ C2 để: tải xuống module bổ sung, gửi thông tin hệ thống, nhận khóa mã hóa, hoặc nhận lệnh điều khiển khác. Để che giấu kênh này, chúng dùng *HTTPS*, *Tor*, *I2P*, *domain generation algorithm (DGA)*, *fast-flux DNS*, hoặc *DNS tunneling*. Gói tin thường được mã hóa, nhiều khi còn giả mạo lưu lượng hợp pháp để tránh bị IDS/IPS phát hiện.
- **Né tránh/Chống phân tích (*Evasion & Anti-Analysis*):** Đây là thành phần then chốt để ransomware “sống sót” và kéo dài thời gian tồn tại. Có thể chia thành:
  - **Evasion** (né tránh phát hiện):
    - \* Kiểm tra sandbox, VM, driver ảo (*environment checking*).
    - \* Trì hoãn thực thi (*sleep obfuscation*, *API hammering*).
    - \* Lợi dụng công cụ hợp pháp (*Living off the Land*: PowerShell, WMI, CertUtil, mshta).
    - \* *Process hollowing*, *reflective DLL injection*, *APC injection*, *thread hijacking*.
    - \* *Fileless execution* chỉ hoạt động trong RAM.
    - \* Nạp driver kernel, rootkit để ẩn tiến trình, file, network.
    - \* Né tránh mạng: *DGA*, *fast-flux*, *DNS tunneling*.
    - \* Giao tiếp C2 mã hóa (*HTTPS*, custom protocol, *Tor/I2P*).
    - \* Lợi dụng chữ ký số giả mạo (*code signing abuse*).
    - \* Bypass UAC, privilege escalation.
    - \* Vô hiệu hóa bảo mật: kill AV/EDR process, xóa backup, log tampering.
  - **Anti-Analysis** (chống phân tích):
    - \* *Obfuscation*, *packing*, *multi-layer encryption*.
    - \* *Anti-disassembly*: overlapping instructions, invalid opcodes, control flow rối.
    - \* *Anti-debugging*: API (IsDebuggerPresent, NtQueryInformationProcess), timing checks (RDTSC), exception tricks, anti-breakpoint.
    - \* *Anti-monitoring*: phát hiện và chặn ProcMon, Wireshark, TCPView, Sysinternals tools.
    - \* *Anti-dumping*: hook API (ReadProcessMemory), ngăn memory dump.
    - \* *Polymorphism/Metamorphism*: thay đổi shellcode, mutation liên tục.
    - \* *Self-destruct*: tự xóa nếu bị phân tích.
    - \* *Anti-virtualization*: kiểm tra MAC address, BIOS string, device ID.
    - \* *API hashing*, *dynamic API resolution* để che giấu hàm Windows.
    - \* *Control flow flattening*, *opaque predicates* làm rối CFG.
    - \* *Anti-forensic*: xóa artifact, xóa log, vô hiệu hóa ETW.
    - \* *Hardware breakpoint detection*, thao tác DRx registers.
    - \* *Anti-snapshot*: phát hiện memory snapshot forensic.
    - \* *Side-channel checks*: timing, CPU counters để phát hiện debug.

Những kỹ thuật này kết hợp giúp ransomware không chỉ tránh né AV/EDR mà còn gây cực kỳ nhiều khó khăn cho chuyên gia phân tích.

## 3 Kỹ thuật thường gặp

Phần này mô tả chi tiết các kỹ thuật điển hình mà ransomware sử dụng, tập trung vào cơ chế hoạt động thực tế (cách chúng được khai thác/triển khai), dấu hiệu để nhận biết, và gợi ý phòng thủ/dò tìm. Cấu trúc bám theo các thành phần ở Mục 2.

### 3.1 Vector xâm nhập

- **Phishing Email (macro, LNK, PDF exploit).** *Mục tiêu:* đạt thực thi ban đầu trên endpoint người dùng. *Cách hoạt động:* email mạo danh (hoá đơn, HR, IT) kéo người dùng mở tài liệu có macro/Active Content hoặc shortcut .LNK chứa lệnh bị che giấu; PDF/Office có thể nhúng kỹ thuật kích hoạt script tải *loader* từ máy chủ điều khiển. *Dấu hiệu:* tiến trình ứng dụng văn phòng khởi tạo trình thông dịch (script interpreter), truy cập mạng bất thường ngay sau khi mở file; chuỗi hành vi *Office* → *script* → *net* → *new process*. *Phòng thủ:* chặn macro-by-default, hardening file-type, EDR rule trên chuỗi tiến trình, bảo vệ mail gateway (sandbox tệp đính kèm), huấn luyện nhận diện social engineering.
- **Tấn công dịch vụ công khai (RDP/VPN/Web).** *Mục tiêu:* xâm nhập thẳng hệ thống nội bộ. *Cách hoạt động:* mật khẩu yếu/credential rò rỉ → đăng nhập RDP/VPN; hoặc khai thác lỗ hổng dịch vụ web/mail để thực thi code gián tiếp (webshell) rồi thả *dropper*. *Dấu hiệu:* phiên đăng nhập từ ASN lạ, khung giờ bất thường; chuỗi *webserver* → *shell* → *loader*; thay đổi cấu hình bảo mật ngay sau khi đăng nhập. *Phòng thủ:* MFA cho RDP/VPN, tách vùng (segmentation), WAF/patch sớm, giám sát failed logins, honeypot/honeynet biên.
- **Credential Theft/Stuffing.** *Mục tiêu:* chiếm quyền tài khoản hợp pháp để né kiểm soát. *Cách hoạt động:* dùng dữ liệu rò rỉ hoặc keylogging/stealer để tái sử dụng trên RDP, email, SaaS; sau đó triển khai *loader*. *Dấu hiệu:* đăng nhập thành công từ thiết bị/IP mới, hành vi nâng đặc quyền sớm sau đăng nhập. *Phòng thủ:* MFA/conditional access, cảnh báo impossible travel, rotation secret, theo dõi sign-in risk.
- **Drive-by/Malvertising.** *Mục tiêu:* kích hoạt mã tại trình duyệt. *Cách hoạt động:* chuỗi redirect/iframe độc hại, lạm dụng plug-in hoặc tải “trình cài đặt” giả → *dropper*. *Dấu hiệu:* trình duyệt sinh tiến trình con bất thường; tải xuống nhị phân không phổ biến. *Phòng thủ:* hardening trình duyệt, cách ly (browser isolation), filter quảng cáo độc hại, chặn thực thi từ thư mục tải về.
- **Chuỗi cung ứng/Ứng dụng giả mạo.** *Mục tiêu:* phát tán ở quy mô lớn. *Cách hoạt động:* trojan hoá bộ cài/phần mềm; khi triển khai, script hậu cài đặt kích hoạt *loader*. *Dấu hiệu:* cùng một phiên bản phần mềm mới cài đặt khởi tạo kết nối ngoài dự kiến, sinh thêm dịch vụ/tác vụ theo lịch. *Phòng thủ:* xác minh chữ ký, SBOM, kiểm soát nguồn gốc phần mềm, allowlist nhà cung cấp.

### 3.2 Dropper/Loader

- **Environment/Sandbox Checks.** *Mục tiêu:* tránh bị phân tích. *Cách hoạt động:* kiểm tra process/driver ảo hoá, BIOS string, số core RAM/CPU bất thường, thời gian hoạt động ngắn, công cụ phân tích đang chạy; nếu nghi ngờ → thoát/đổi hành vi. *Dấu hiệu:* nhị phân gọi nhiều API truy vấn môi trường trước khi liên lạc mạng/giải nén

payload. *Phòng thủ*: EDR rule cho chuỗi kiểm tra đồ hình máy ảo, theo dõi access tới các chỉ báo ảo hoá.

- **Giải nén/giải mã nhiều tầng (staged deployment).** *Mục tiêu*: che giấu payload chính. *Cách hoạt động*: loader chứa blob mã hoá/packed; chỉ giải mã khi thoả điều kiện (thời gian, người dùng, địa chỉ IP, AD context). *Dấu hiệu*: tiến trình thực hiện vòng lặp giải mã/bom bộ nhớ, sau đó sinh module mới trong RAM/đĩa tạm. *Phòng thủ*: giám sát entropy cao, API giải nén/mã hoá gọi dồn dập, Memory scan heuristic.
- **Fileless & LOLBins.** *Mục tiêu*: giảm dấu vết trên đĩa, né AV. *Cách hoạt động*: thực thi trong bộ nhớ (reflective loading), lạm dụng công cụ sẵn có (PowerShell, WMI, *mshta*, *rundll32*) để tải/khởi động payload. *Dấu hiệu*: công cụ hệ thống sinh lưu lượng mạng và tiến trình con trái ngữ cảnh. *Phòng thủ*: AMSI/ETW bật đầy đủ, hạn chế script host, AppLocker/WDAC, giám sát parent-child process bất thường.
- **Signed Binary Proxy/DLL Side-Loading.** *Mục tiêu*: mượn uy tín nhị phân ký số. *Cách hoạt động*: đặt DLL giả vào vị trí được ưu tiên trong *search order*, ép tiến trình đã ký nạp DLL độc hại. *Dấu hiệu*: tiến trình có chữ ký hợp lệ nhưng nạp module đến từ thư mục không chuẩn. *Phòng thủ*: block side-loading đường dẫn người dùng, theo dõi LoadLibrary vào DLL ngoài whitelist.

### 3.3 Payload chính

- **Crypto (mã hoá lai ghép).** *Mục tiêu*: gây gián đoạn dữ liệu để tống tiền. *Cách hoạt động*: chọn file theo bộ lọc (phần mở rộng/thư mục), dùng thuật toán đối xứng (AES/ChaCha) để mã hoá nội dung, sau đó mã hoá khoá đối xứng bằng khoá công khai (RSA/ECC) nhúng/cấp từ C2; tối ưu tốc độ bằng mã hoá từng phần, ưu tiên file lớn/nhạy cảm; đổi tên, thêm hậu tố, và ghi ransom note. *Dấu hiệu*: spike I/O đọc–ghi hàng loạt, tạo nhiều file note, đổi đuôi đồng loạt, truy cập shadow storage. *Phòng thủ*: EDR theo dõi mẫu I/O bất thường, canary file, chặn xoá shadow copies, backup bất biến (immutable), EKM/HSM cho dữ liệu trọng yếu.
- **Stealer/Exfiltration.** *Mục tiêu*: tống tiền kếp/bán dữ liệu. *Cách hoạt động*: thu thập bí mật (trình duyệt, ví, SSH, email), tra cứu kho chia sẻ nội bộ, zip/chia nhỏ, gửi ra ngoài qua HTTPS/Tor/cloud API; có thể đọc bộ nhớ tiến trình bảo mật để lấy thông tin xác thực. *Dấu hiệu*: đột biến lưu lượng ra ngoài (đặc biệt trước giai đoạn mã hoá), truy cập kho dữ liệu tập trung, nén file diện rộng. *Phòng thủ*: DLP, egress filtering, giám sát hành vi nén diện rộng, cảnh báo khi endpoint truy cập dữ liệu vượt ngưỡng bình thường.
- **Ransom Note/Screen.** *Mục tiêu*: hướng dẫn trả tiền/đe dọa công khai dữ liệu. *Cách hoạt động*: tạo file note (TXT/HTML) ở mỗi thư mục hoặc hiển thị toàn màn hình; chèn ID nạn nhân, URL Tor, thời hạn, ví tiền số. *Dấu hiệu*: sinh hàng loạt file note, thay đổi wallpaper/lockscreen. *Phòng thủ*: rule phát hiện tạo file note theo mẫu, theo dõi sửa registry phần hình nền/lock policies.
- **Worm/Propagator & Di chuyển ngang.** *Mục tiêu*: khuếch tán trong mạng nội bộ. *Cách hoạt động*: dò chia sẻ SMB, tái dùng thông tin xác thực lấy được, lạm dụng công cụ quản trị từ xa; trong môi trường AD có thể lạm dụng chính sách nhóm để đẩy payload. *Dấu hiệu*: kết nối SMB dày đặc giữa máy người dùng, tạo dịch vụ/tác

vụ hàng loạt, đăng nhập liên máy bất thường. *Phòng thủ*: phân đoạn mạng, hạn chế admin lateral, honeypot share, giám sát tạo dịch vụ/tác vụ quy mô lớn.

- **Killer/Disabler (Vô hiệu hoá bảo vệ).** *Mục tiêu*: giảm khả năng phục hồi/phát hiện. *Cách hoạt động*: cố dừng dịch vụ AV/EDR/backup, xoá shadow copies/restore points, tắt logging; một số biến thể cố gắng can thiệp thành phần giám sát sự kiện. *Dấu hiệu*: chuỗi thao tác ngay trước/đang mã hoá: dừng dịch vụ bảo mật, sửa policy, lỗi bất thường của agent. *Phòng thủ*: bảo vệ *self-defense* cho agent, quyền tối thiểu, giám sát hành vi dừng dịch vụ nhạy cảm, bảo vệ snapshot bất biến.

### 3.4 Persistence

- **Registry Run Keys / Startup.** *Cách hoạt động*: thêm mục tự khởi động theo phiên/khởi động máy để tự chạy lại payload. *Dấu hiệu*: thay đổi khoá run, tạo shortcut vào thư mục khởi động. *Phòng thủ*: giám sát thay đổi autostart, so khớp chữ ký/đường dẫn đáng tin.
- **Scheduled Tasks/Services.** *Cách hoạt động*: tạo tác vụ theo lịch hoặc dịch vụ hệ thống để khởi chạy định kỳ/ở quyền cao. *Dấu hiệu*: xuất hiện tác vụ/dịch vụ mới tên ngẫu nhiên, parent process bất thường. *Phòng thủ*: kiểm soát tạo dịch vụ/tác vụ, cảnh báo khi có entity mới có quyền cao.
- **DLL Hijacking / Side-Loading.** *Cách hoạt động*: lợi dụng trật tự tìm DLL để ép tiến trình hợp pháp nạp module độc. *Dấu hiệu*: tiến trình hợp pháp nạp DLL từ thư mục người dùng/tạm. *Phòng thủ*: bật *Safe DLL Search Mode*, block load từ đường dẫn rủi ro, inventory module.
- **WMI Event Subscription / Logon Scripts.** *Cách hoạt động*: đăng ký sự kiện hệ thống (khởi động/dăng nhập) hoặc script đăng nhập để auto-exec. *Dấu hiệu*: WMI repository có subscription lạ; script logon mới trong domain. *Phòng thủ*: auditing WMI, kiểm soát GPO/logon script thay đổi.
- **Kernel Driver/Bootkit (nâng cao).** *Cách hoạt động*: nạp driver không đáng tin/can thiệp chuỗi khởi động để ẩn và bám trụ sâu. *Dấu hiệu*: driver không ký số/hết hạn; thay đổi thành phần khởi động. *Phòng thủ*: Secure Boot/WDAC, chỉ cho phép driver ký hợp lệ, EDR kernel telemetry.

### 3.5 Liên lạc chỉ huy & điều khiển (C2)

- **Giao thức & mã hoá.** *Cách hoạt động*: beacon theo chu kỳ với jitter, dùng HTTPS/TLS hoặc kênh ẩn (DNS/ICMP tunneling); tải lệnh/payload, gửi telemetry/khóa. *Dấu hiệu*: mẫu kết nối định kỳ tới domain mới đăng ký/CDN lạ, *JA3/JA3S* khác thường. *Phòng thủ*: TLS fingerprinting, DNS monitoring, chặn egress theo nguyên tắc tối thiểu.
- **Ẩn danh & Khả dụng.** *Cách hoạt động*: Tor/I2P, domain generation algorithm (DGA), fast-flux để xoay hạ tầng; *dead drop resolver* (paste sites) làm điểm trung gian. *Dấu hiệu*: truy vấn DNS nhiều tên ngẫu nhiên, TTL thấp, lưu lượng tới nod Tor. *Phòng thủ*: block Tor/I2P, phát hiện DGA bằng thống kê/ML, list deny domain non-corporate cho máy người dùng.

### 3.6 Né tránh & Chống phân tích (Evasion & Anti-Analysis)

- **Evasion (né phát hiện).** *Mục tiêu:* giảm khả năng bị EPP/EDR nhìn thấy. *Cách hoạt động:* (i) *Environment checking* (VM/sandbox/debug); (ii) *Sleep/Delay Obfuscation* (trì hoãn, chia nhỏ API call); (iii) *LOLBins* (PowerShell, WMI, *mshta*, *rundll32*); (iv) *Process Injection* (hollowing, reflective loading, APC, thread hijack, map view of section); (v) *AMSI/ETW tampering* (giảm khả năng ghi giám sát); (vi) *Code signing abuse*; (vii) *UAC bypass/privilege escalation*; (viii) *Service/Backup tampering*. *Dấu hiệu:* chuỗi hành vi “công cụ hệ thống → mạng → sinh tiến trình con/inject”; tắt log/agent trước khi mã hoá. *Phòng thủ:* harden chính sách script, EDR rule cho injection primitives, bảo vệ ETW/AMSI, principle of least privilege.
- **Anti-Analysis (chống phân tích).** *Mục tiêu:* làm chậm/sai lệch điều tra. *Cách hoạt động:* (i) *Packing/Obfuscation/Encryption* đa tầng; (ii) *Anti-disassembly* (opaque predicate, overlapping/invalid opcode) làm rối CFG; (iii) *Anti-debugging* (kiểm tra cờ PEB, timing check, exception trick); (iv) *API hashing/dynamic resolution* để che tên hàm; (v) *Anti-dumping* (bảo vệ vùng nhớ, unhook/rehook); (vi) *Polymorphism/Metamorphism* thay đổi mã giữa lần chạy; (vii) *Self-destruct/switch-off* khi phát hiện công cụ phân tích; (viii) *Anti-virtualization/snapshot* (truy vấn phần cứng, phát hiện ảnh chụp bộ nhớ). *Dấu hiệu:* nhiều kiểm tra môi trường trước khi thực thi chính; kỹ thuật điều khiển luồng lạ; thất bại khi dump memory. *Phòng thủ:* chạy phân tích trên sandbox “thật” (hardware-backed), bật anti-tamper EDR, kết hợp static + dynamic + memory forensics.

*Ghi chú:* Mô tả tập trung vào **cơ chế kỹ thuật, tín hiệu phát hiện, và biện pháp phòng thủ**, nhằm phục vụ mục đích phòng vệ số. Không bao gồm chỉ dẫn vận hành khai thác cụ thể.

## 4 Hành vi quan sát được

Trong quá trình phân tích các sự cố ransomware, có thể nhận diện nhiều đặc trưng hành vi giúp xây dựng kịch bản giám sát và phát hiện sớm. Những hành vi này thường lặp lại giữa nhiều họ ransomware khác nhau, mặc dù mức độ tinh vi có thể khác biệt.

- **Tạo tệp bất thường:** Sinh ra hàng loạt tệp mới với phần mở rộng lạ hoặc thêm hậu tố đặc trưng (ví dụ: *.locked*, *.encrypted*). Song song đó, kẻ tấn công cấy *ransom note* trong mỗi thư mục dữ liệu để truyền tải thông điệp đòi tiền chuộc.
- **Gia tăng tài nguyên hệ thống:** Xuất hiện đột biến trong mức tiêu thụ CPU, bộ nhớ và đặc biệt là disk I/O do quá trình mã hoá hàng loạt tệp. Sự tăng tốc độ đọc/ghi bất thường này thường là chỉ báo rõ rệt trong giám sát hành vi.
- **Tác động tới bản sao lưu và phục hồi:** Ransomware thường tìm cách xoá, vô hiệu hoá hoặc làm hỏng các bản sao lưu hệ thống (shadow copies, snapshot, agent backup). Hành vi này nhằm ngăn cản quá trình khôi phục dữ liệu thông thường, buộc nạn nhân phải cân nhắc trả tiền chuộc.
- **Vô hiệu hoá cơ chế bảo mật:** Thường ghi nhận nỗ lực dừng dịch vụ antivirus/EDR, chỉnh sửa registry hoặc chính sách bảo mật để giảm thiểu khả năng bị phát hiện và

ngăn chặn. Đây là một trong những bước chuẩn bị trước khi mã hoá diễn ra ở quy mô lớn.

- **Hoạt động liên lạc ra ngoài:** Tiến trình độc hại duy trì kênh liên lạc định kỳ (beaconing) tới máy chủ điều khiển (C2) hoặc sử dụng hạ tầng hợp pháp (dịch vụ cloud, pastebin, API hợp pháp) để gửi siêu dữ liệu, khoá mã hoá hoặc trạng thái thực thi. Đặc trưng là chu kỳ truy vấn lặp lại, đích đến cố định hoặc danh sách IP/domain đáng ngờ.
- **Dấu hiệu giao diện bất thường (lock-screen):** Với các biến thể *locker ransomware*, thay vì mã hoá, tiến trình sẽ hiển thị một cửa sổ toàn màn hình “luôn ở trên cùng”, che toàn bộ desktop, vô hiệu tổ hợp phím hoặc task manager. Đây là hành vi khoa giao diện người dùng, tạo cảm giác hệ thống bị “bắt giữ”.

Tập hợp các hành vi trên, khi được soi chiếu đồng thời, có thể cung cấp *chỉ số hành vi tấn công* (Indicators of Attack – IoA) phục vụ cho hệ thống SIEM/EDR trong việc phát hiện sớm ransomware.

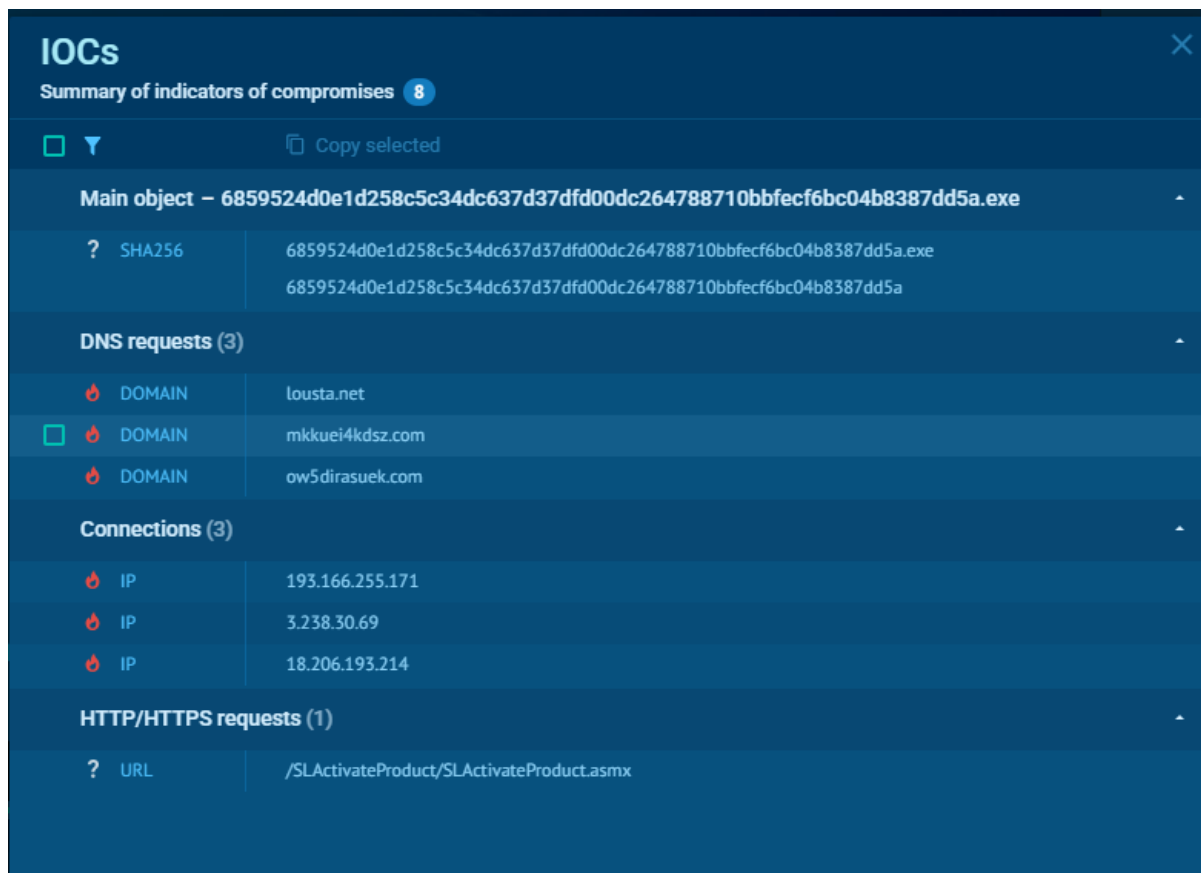
## 5 Chỉ số nhận diện (IoCs) — ví dụ định dạng báo cáo

Các *Indicators of Compromise* (IoCs) đóng vai trò như bằng chứng kỹ thuật, giúp truy vết, phát hiện và phong tỏa sự hiện diện của ransomware trong hạ tầng. Bảng dưới đây minh họa một số dạng IoC phổ biến, có thể xuất hiện trong quá trình điều tra sự cố:

Loại	Giá trị (ví dụ minh họa)	Nguồn/ghi chú
Hash (SHA256)	a3f1b8...9c2e7d	Trích xuất từ mẫu nhị phân
Tên tệp / thư mục	README_RECOVER_FILES.txt, thư mục C:\Users\Public\decrypt	Quan sát trên máy nạn nhân
Miền / IP liên lạc	hxxps://data-sync[.]top, 185.77.22.44	Nhật ký firewall / proxy
Tiêu đề ransom note	“All your files are encrypted”, “How_to_restore_data.txt”	Tập tin để lại sau khi mã hóa
Chuỗi (string) đặc trưng	-lockall -shadowdelete	Kết quả phân tích nhị phân
Registry / Service	Khóa: HKCU\Software\LockScreen, dịch vụ giả: winhelp_svc	Thu thập từ endpoint
Artefact mạng khác	User-Agent bất thường: Mozilla/5.0 (Ransom)	Nhật ký IDS/IPS
Mốc thời gian	Hoạt động đồng loạt lúc 02:35 GMT	So sánh với log tập trung



**Lưu ý:** Các giá trị trên chỉ là ví dụ minh họa, không đại diện cho biến thể cụ thể. Khi triển khai trong thực tế, cần trích xuất IoC trực tiếp từ mẫu mã độc, hệ thống giám sát mạng và nhật ký endpoint để đảm bảo tính chính xác và cập nhật.  
Một ví dụ trên anyrun.com :



IOCs	
Summary of indicators of compromises 8	
Main object – 6859524d0e1d258c5c34dc637d37dfd00dc264788710bbfecf6bc04b8387dd5a.exe	
SHA256	6859524d0e1d258c5c34dc637d37dfd00dc264788710bbfecf6bc04b8387dd5a.exe 6859524d0e1d258c5c34dc637d37dfd00dc264788710bbfecf6bc04b8387dd5a
DNS requests (3)	
DOMAIN	lousta.net
DOMAIN	mkkuei4kdsz.com
DOMAIN	ow5dirasuek.com
Connections (3)	
IP	193.166.255.171
IP	3.238.30.69
IP	18.206.193.214
HTTP/HTTPS requests (1)	
URL	/SLActivateProduct/SLActivateProduct.asmx

Hình 1: Enter Caption

## 6 Kết luận

Ransomware là mối đe dọa phức tạp với cấu trúc đa tầng và kỹ thuật đa dạng. Hiểu biết về thành phần, hành vi và hướng phòng thủ giúp tổ chức tăng khả năng phát hiện sớm, giảm thiểu tác động và phục hồi nhanh hơn. Báo cáo tổng quan này cung cấp khung trình bày để tùy biến theo từng tình huống thực tế.

## A Phụ lục A — Checklist ứng phó sự cố (IR) rút gọn

### A.1. Pha Phát hiện & Đánh giá ban đầu

Kích hoạt quy trình IR; chỉ định Incident Commander (IC).

Xác nhận chỉ báo: tăng I/O bất thường, ransom note/screen, kết nối egress lạ.

Phân loại mức độ/ảnh hưởng: hệ thống bị ảnh hưởng, dữ liệu nhạy cảm, phạm vi người dùng.

Lập *timeline* sơ bộ (sự kiện, tài khoản, host, mốc thời gian).

## A.2. Pha Khoanh vùng & Ngăn chặn tạm thời

Cô lập endpoint nghi nhiễm (network quarantine), khoá tài khoản bất thường.

Ngăn chặn kênh egress/C2 nghi vấn (proxy/firewall), chặn Tor/I2P theo chính sách.

Giữ bằng chứng: *do not wipe*; ảnh đĩa/bộ nhớ theo thủ tục pháp chứng.

## A.3. Pha Điều tra chi tiết

Thu thập: log tập trung (SIEM), EDR telemetry, Windows Event, Sysmon, network flow.

Xác định *patient zero*, vector xâm nhập, cơ chế bám trụ (*persistence*).

Kiểm tra exfiltration (khối lượng, đích đến, cửa sổ thời gian).

## A.4. Pha Khôi phục & Tăng cường

Phục hồi từ **backup sạch/immutable**; *không* gắn trực tiếp vào môi trường nhiễm.

Xoay khoá/bí mật, reset mật khẩu, rà soát quyền đặc biệt (admin).

Vá lỗ hổng, siết MFA/Conditional Access, áp dụng *least privilege*.

## A.5. Pha Hậu kiểm

Post-mortem: nguyên nhân gốc (root cause), điểm yếu, bài học, kế hoạch cải tiến.

Cập nhật playbook, *detection content*, bảng deny/allow, quy tắc sao lưu.

*Lưu ý:* Checklist chỉ bao quát mức cao, cần điều chỉnh theo thực tế hạ tầng & ràng buộc pháp lý của đơn vị.

## B Phụ lục B — Thuật ngữ

Thuật ngữ	Mô tả ngắn
C2	Kênh chỉ huy/điều khiển, trao đổi lệnh và dữ liệu điều khiển.
IoC	<i>Indicator of Compromise</i> — dấu vết kỹ thuật phục vụ phát hiện/truy vết.
IoA	<i>Indicator of Attack</i> — chỉ dấu hành vi, hướng phát hiện sớm theo ngữ cảnh.
EDR	Giải pháp phát hiện & đáp ứng điểm cuối dựa trên hành vi/telemetry.
LOLBins	<i>Living-off-the-land binaries</i> : công cụ hợp pháp bị lạm dụng (PowerShell,...).
ATT&CK	Ma trận chiến thuật/kỹ thuật MITRE cho hành vi đối kháng.
Immutable Backup	Bản sao lưu bất biến/không thể sửa xoá trong thời hạn đặt trước.

## C Phụ lục C — Ánh xạ chiến thuật MITRE ATT&CK (rút gọn)

Pha	Kỹ thuật (mô tả ngắn)	ID tham chiếu
Xâm nhập ban đầu	Phishing, khai thác dịch vụ public (RDP/VPN/Web)	T1566, T1190
Thực thi	Script/Interpreter, Proxy thực thi bằng nhị phân ký số	T1059, T1218
Bám trụ	Run Keys/Startup, Scheduled Task, Service	T1547, T1053, T1031
Leo thang	Bypass UAC, Abuse Token/Privilege	T1548, T1134
Tránh né	Obfuscation/Untrusted DLL, Tamper AV/EDR	T1027, T1562
Truy cập thông tin	Credential Dumping	T1003
Di chuyển ngang	SMB/Remote Services/RDP	T1021
Thu thập & Nén	Archive Collected Data	T1560
Rò rỉ dữ liệu	Exfiltration over Web/Tor/Cloud	T1041, T1567
Tác động	Mã hoá dữ liệu, Vô hiệu khôi phục	T1486, T1490

## D Phụ lục D — Telemetry & Nhật ký nên bật/soi

### D.1. Windows Event ID (mức nền tảng)

Event ID	Ý nghĩa gợi ý dò tìm
4624/4625	Đăng nhập thành công/thất bại; tìm bất thường theo ASN, thời gian, nguồn.
4672	Đăng nhập với đặc quyền cao.
4698	Tạo Scheduled Task.
7045	Cài đặt dịch vụ mới.

### D.2. Sysmon (nếu có)

Sysmon ID	Ý nghĩa gợi ý dò tìm
1 (Process Create)	Chuỗi <i>Office/Browser</i> → <i>script host</i> → <i>net</i> → tiến trình con.
7 (Image Loaded)	Nạp DLL ở đường dẫn bất thường (side-loading).
11 (File Create)	Tạo hàng loạt file đuôi lạ / ransom note.
13 (Registry Set)	Thay đổi khoá Run/Winlogon (persistence).
22 (DNS Query)	Truy vấn domain lạ/DGA; TTL thấp; đích Tor gateway.

### D.3. Mạng & Proxy/Firewall

- Lưu lượng định kỳ (*beacon*) đến domain mới đăng ký/CDN không dùng nội bộ.
- Tăng đột biến egress/HTTPS trước khi xuất hiện mã hoá (dấu exfiltration).
- Chặn/ghi nhận Tor/I2P, *paste sites* dùng như *dead-drop resolver*.

## E Phụ lục E — Mẫu biểu IoC (điền nhanh)

Loại	Giá trị	Nguồn
Hash (SHA256)		Mẫu nhị phân/EDR
Tên tệp/thư mục		Endpoint/DFIR
Miền/IP/C2		Proxy/Firewall/DNS
User-Agent/JA3		IDS/Netflow
Registry/Service		Windows/Sysmon
Ransom note title		Endpoint/FS scan
Mốc thời gian		SIEM timeline

## F Phụ lục F — Khung Timeline điều tra (tham khảo)

Thời điểm (UTC)	Thành phần	Sự kiện/nhận định
YYYY-MM-DD hh:mm	Endpoint A	Người dùng mở tệp đính kèm → WINWORD.exe sinh powershell.exe.
YYYY-MM-DD hh:mm	Mạng	Egress HTTPS tới domain mới đăng ký.
YYYY-MM-DD hh:mm	AD/IDP	Đăng nhập bất thường, cấp quyền cao.
YYYY-MM-DD hh:mm	Endpoint B	Tạo Scheduled Task & dịch vụ mới.
YYYY-MM-DD hh:mm	Hệ thống tệp	Tăng I/O, tạo ransom note hàng loạt.

## G Phụ lục G — Phân biệt Locker vs. Crypto Ransomware (nhanh)

	Locker (khóa màn hình)	Crypto (mã hoá tệp)
Triệu chứng chính	Cửa sổ toàn màn hình, chặn phím tắt/Task Manager.	Đổi đuôi tệp, note xuất hiện trong nhiều thư mục.
Tác động dữ liệu	Không nhất thiết mã hoá tệp.	Mã hoá nội dung tệp.
Chỉ báo kỹ thuật	Tiến trình GUI chiếm focus; registry/policy khóa shell.	Spike I/O; tạo/đổi tên tệp hàng loạt; chạm shadow copies.
Ưu tiên xử lý	Gỡ/thoát UI trong môi trường cô lập, xoá persistence.	Cô lập, bảo toàn bằng chứng, kiểm tra exfil, khôi phục từ backup sạch.

*Khuyến nghị:* cập nhật định kỳ nội dung Phụ lục theo bối cảnh mối đe dọa của tổ chức (TTP đang nổi, hạ tầng mới, chính sách egress,...).