基於 Rust 的資訊竊取程式濫用 GitHub 程式碼空間

分析報告

Rust-Based Info Stealers Abuse GitHub Codespaces

目錄

惡意程式名稱

本次分析對象並非真實惡意程式，而是 DeltaStealer C2 行為的模擬 Agent。此 Agent 旨在安全重現惡意流量，以便進行 IDS/IPS 偵測測試。

惡意程式參考來源：

DeltaStealer — Rust-based Information Stealer （Trend Micro）

Suricata 規則

以下為本事件所使用的偵測規則：

DNS Lookup 規則

alert dns $HOME_NET any -> any any (msg:"ET MALWARE DeltaStealer CnC Domain (deltaproject .us) in DNS Lookup"; dns.query; dotprefix; content:".deltaproject.us"; nocase; endswith; classtype:domain-c2; sid:2045784; rev:1;)

alert dns $HOME_NET any -> any any (msg:"ET MALWARE DeltaStealer CnC Domain (deltastealer .xyz) in DNS Lookup"; dns.query; dotprefix; content:".deltastealer.xyz"; nocase; endswith; classtype:domain-c2; sid:2045785; rev:1;)

alert dns $HOME_NET any -> any any (msg:"ET MALWARE DeltaStealer CnC Domain (deltastealer .gq) in DNS Lookup"; dns.query; dotprefix; content:".deltastealer.gq"; nocase; endswith; classtype:domain-c2; sid:2045786; rev:1;)

TLS SNI 規則

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Observed DeltaStealer Domain (deltaproject .us) in TLS SNI"; flow:established,to_server; tls.sni; dotprefix; content:".deltaproject.us"; endswith; sid:2045787; rev:1;)

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Observed DeltaStealer Domain (deltastealer .xyz) in TLS SNI"; flow:established,to_server; tls.sni; dotprefix; content:".deltastealer.xyz"; endswith; sid:2045788; rev:1;)

alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Observed DeltaStealer Domain (deltastealer .gq) in TLS SNI"; flow:established,to_server; tls.sni; dotprefix; content:".deltastealer.gq"; endswith; sid:2045789; rev:1;)

MD5

MD5 : B8A1423E1B29D99F0DCE1F9F2C84AEFC

封包內容

本次測試 Agent 重現的惡意 C2 流量包含：

1. DNS Query
    - 查詢目標
        - deltaproject.us
        - deltastealer.xyz
        - deltastealer.gq
    - 查詢類型：A record
    - 使用系統 DNS 或自訂 DNS Server
2. TLS ClientHello 與 SNI
    - 目的：模擬 DeltaStealer 與 C2 建立 HTTPS 握手
    - 於 TLS SNI 欄位填入上述 domain
    - 不傳送任何加密 payload

3. 回報封包

前往中繼站 /report 回傳 JSON，則內容包含：

```
{
   "timestamp": "...",
   "hostname": "...",
   "internal_ip": "...",
   "public_ip": "...",
   "os": "Windows ..."
}
```

封包特徵

此用於表示 IDS/IPS 偵測所依賴的行為特徵

1. DNS 層級特徵

可觀察指標

- Query Name 出現特定 C2 Domain
- Dot-prefix
- Domain 結尾（endswith）
- 來源為本機
- UDP 53（多數情況）

特徵摘要

Query Name: deltaproject.us

Query Name: deltastealer.xyz

Query Name: deltastealer.gq

Protocol: DNS / UDP 53

Behavior: 可疑 C2 初始化查詢

2. TLS 層級特徵（SNI）

主要特徵

- TLS ClientHello → SNI 包含可疑 Domain
- TCP 443
- Direction: to_server
- 無 application data（代表為初始握手）

SNI 值

deltaproject.us

deltastealer.xyz

deltastealer.gq

用途

此為許多惡意 C2 常見的隱蔽連線手法，用於加密後的 C2 溝通。

Malware 內的重要 function

因本研究不執行真正的惡意程式，而是模擬其行為，因此功能依照 Trend Micro 的分析做安全還原：

1. DNS Resolver Function

- 目的：解析 C2 Domain
- 行為：向系統或 8.8.8.8 發送查詢
- 特徵：大量 Query 或固定 C2 名稱

2. TLS Connection Function

- 建立 HTTPS 連線
- SNI 指向 C2 Domain
- C2 接收到握手後，後端通常會要求認證或傳輸資料
  （本測試 Agent 未實作資料傳輸，以避免風險）

3. C2 Communication 模擬 function

你的 Agent 實作方式（簡化版）為：

- 建立 ClientHello → 帶 SNI
- 等候數毫秒
- 中斷連線，避免造成真實外聯

惡意程式執行流程

以下流程為 DeltaStealer 的行為邏輯＋本 Agent 的模擬方式：

[1] 啟動程式

[2] 初始化網路模組

[3] 解析硬編碼 C2 Domain（DNS Query）

[4] 使用解析結果建立 TLS 連線

[5] 在 TLS SNI 中傳遞 C2 Domain

[6] 等候伺服器回應

[7] 若為真實惡意程式：傳送竊取資料

[8] 在模擬 Agent：不傳送任何資訊，立即斷線

結論：本 Agent 目的在於安全地重現第 3~5 步

製作 Agent

步驟 1：蒐集 IOC 與流量分析

- 來源：Trend Micro DeltaStealer 報告
- 取得以下 IOC：
  - → deltaproject.us
  - → deltastealer.xyz
  - → deltastealer.gq
- 分析 DNS / TLS 流量特徵
- 確認 Suricata 規則需求
- 規劃需要模擬的封包種類（DNS + TLS）

步驟 2：撰寫封包模擬程式

2-1 DNS 模擬

- 使用 socket 產生 UDP 53 封包
- 自行組裝 DNS Query Header + QNAME
- 支援 retry、timeout、delay

2-2 TLS ClientHello 模擬

方法可包含：

- Python ssl library + server_hostname=xxx
- 自製 raw TLS ClientHello

包含欄位：

- SNI
- TLS Version

- Cipher Suites
- Extension

2-3 可選：POST 回報紀錄

中繼站需要 log，可送：

- timestamp
- hostname
- public IP / internal IP
- OS info

步驟 3：測試與驗證

3-1 測試 Suricata 是否正確觸發

- 開啟 Suricata
- 執行 Agent
- 觀察 fast.log / eve.json

3-2 常見 Alert

ET MALWARE DeltaStealer CnC Domain in DNS Lookup

ET MALWARE Observed DeltaStealer Domain in TLS SNI

3-3 驗證流量是否符合規則條件

- dotprefix
- endswith
- to_server
- tls.sni