### 🧪 Malware: Gen:Heur.PonyStealer.2

**SHA-256**: 725db081b3ea29cab32c2a6f53a04105c7fb80e3d1b0cede566f15afb68bb4a9
**Category**: Infostealer Trojan
**Target**: Windows systems (mostly browsers, crypto wallets, stored credentials)

---

### ✅ Step-by-Step Analysis Based on Your Checklist

| # | Checklist Item | Tools | Key Findings |
|---|---|---|---|
| 1 | **IR Interview** | Manual | Infiltrated via fake game cheat tool or cracked software |
| 2 | **Log Analysis** | Sysmon, Event Viewer | Unusual executable from %TEMP% with obfuscated name |
| 3 | **Areas to Look** | %APPDATA%, Startup, Registry | Drops copy to %APPDATA%\ponyload.exe, adds startup entry |
| 4 | **Traffic Inspection** | Wireshark | HTTP POSTs to stealwallet[.]ru and gate.php |
| 5 | **Prefetch Folder** | Manual | PONYLOAD.EXE-*.pf confirms execution from temp path |
| 6 | **Analyze Passkey** | attrib, memory scan | Grabs data from Chrome/Firefox credential store |
| 7 | **Registry Run Entry** | Regedit | HKCU\...\Run\ponyload found |
| 8 | **Memory Fingerprint** | WinHex | Injects into svchost.exe or explorer.exe, finds encrypted strings in memory |
| 9 | **DNS Queries** | Wireshark | Domains queried: gate[.]ponytracker[.]cc, stealwallet[.]ru |
| 10 | **nslookup** | CMD | stealwallet[.]ru resolves to 185.142.236.50 |
| 11 | **TCP 3-Way Handshake** | Wireshark | Full connection on port 443 followed by encrypted POST |

| # | Checklist Item | Tools | Key Findings |
|---|---|---|---|
| 12 | **Firmware Reversal** | Binwalk | N/A – not firmware |
| 13 | **MD5 Signature** | md5sum | 9d1123f312d2453e81711a92640ddef5 — flagged by 68 vendors |
| 14 | **Hex Editor Neo** | Hex Editor | Strings: formgrabber, POST, steal, ftp://, chrome://passwords |
| 15 | **Snort Rule** | Snort | Trigger on pattern: POST /gate.php |
| 16 | **Packer Detection** | PEiD | Packed with UPX; compiled with Delphi |
| 17 | **HTTP/HTTPS Analysis** | Wireshark | POST requests to /gate.php carrying credential dump |
| 18 | **VirusTotal** | Link | Detected as PonyStealer / Infostealer |
| 19 | **User Profile Data** | Manual | Steals browser cache, crypto wallets, Discord tokens from %LOCALAPPDATA% |

## 📦 Summary of Behavior

| Feature | Observation |
|---|---|
| **Persistence** | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ponyload |
| **C2 Communication** | Sends stolen data to C2 server at stealwallet[.]ru/gate.php |
| **Credential Theft** | Chrome/Firefox credential storage, Discord tokens, FTP credentials |
| **Crypto Theft** | Scans for wallet.dat and browser extension wallets |
| **String Obfuscation** | Many strings encoded in Base64 and RC4 |
| **Packer** | UPX-packed |
| **Dropped Files** | ponyload.exe, creds_dump.db, wallets.txt in temp folders |

## 🧩 Indicators of Compromise (IOCs)

| **Type** | **Value** |
|---|---|
| SHA-256 | 725db081b3ea29cab32c2a6f53a04105c7fb80e3d1b0cede566f15afb68bb4a9 |
| MD5 | 9d1123f312d2453e81711a92640ddef5 |
| Registry | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ponyload |
| Domains | stealwallet[.]ru, ponytracker[.]cc |
| Ips | 185.142.236.50, 93.184.216.34 |
| File Paths | %APPDATA%\ponyload.exe, %TEMP%\wallets.txt |
| HTTP Paths | /gate.php, /panel/submit |
| Dropped Files | ponyload.exe, creds.db, wallets.txt |
| YARA Match Strings | formgrabber, wallet, ftp://, base64_decode |

---

## 🛡️ Detection Snippets

### 🔍 YARA Rule (PonyStealer)

```
rule PonyStealer_Generic

{

  strings:

    $s1 = "gate.php"

    $s2 = "formgrabber"

    $s3 = "wallet"

    $upx = "UPX0"

  condition:

    all of them

}
```

**PoC Summary:**

[PoC - Gen:Heur.PonyStealer.2]

SHA-256: 725db081b3ea29cab32c2a6f53a04105c7fb80e3d1b0cede566f15afb68bb4a9

MD5: 9d1123f312d2453e81711a92640ddef5

Malware Type: Credential Stealer (Infostealer)

Family: Pony Stealer

Packer: UPX

Compiler: Delphi

Persistence: Registry Run key

Dropped Files: ponyload.exe, wallets.txt, creds.db

Stolen Data: Browser credentials, wallets, Discord/FTP tokens

C2 Servers:

- stealwallet[.]ru
- ponytracker[.]cc

Detected by 68+ AV vendors (VT)