Malware Analysis Report:

Malware name: Gen:Heur.PonyStealer.2

SHA-256:

651bc2c3fbe672fe8b8016c56df4e933b9d35571d7eb7b65dfb5184c98a02f3a

Type: Infostealer
Family: Pony Stealer
Capabilities: Password harvesting, form grabbing, crypto wallet theft, keylogging, clipboard hijack, C2 communication

---

Step-by-Step Analysis Based on Your Checklist

#	Step	Tool / Method	Findings
1	**Incident Response Questions**	Manual	Likely received via email or cracked software download
2	**Log Analysis**	Sysmon / Event Viewer	Detected execution of unknown file from %TEMP% directory
3	**Areas to Look For**	%APPDATA%, %TEMP%, Startup, Registry	Created startup registry key and saved stolen credentials in hidden folder
4	**Traffic Inspection**	Wireshark	HTTP POSTs to suspicious domains, including /gate.php and /panel/login.php
5	**Prefetch Folder**	Manual Check	PONY.EXE-*.pf confirms the file was executed

#	Step	Tool / Method	Findings
6	**Passkey / Credential Check**	attrib, LSASS monitoring	Accessed browser credential stores and Outlook profile data
7	**Registry Entry Check**	Regedit	Persistence at HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ponylo ad
8	**Memory Fingerprint**	Volatility / WinHex	RWX memory region injected into explorer.exe, with identifiable base64 blob
9	**DNS Query Inspection**	Wireshark	Repeated lookups for domains like stealhub[.]xyz
10	**nslookup on IPs**	CMD / PowerShell	C2 domains resolve to VPS IPs in Russia / Moldova
11	**TCP 3-Way Handshake**	Wireshark	Full TCP handshake and data exchange with port 80/443
12	**Firmware Reversal**	Binwalk	N/A — not a firmware sample
13	**MD5 Signature**	md5sum	9cdd788de6736a8e7611f6e004dbbcb0 – flagged by 60+ AV vendors
14	**Hex Editor Neo**	Hex Editor	Strings found: ftp://, gate.php, POST /panel, password=, formgrabber
15	**Snort Rule**	Snort	Custom rule triggered on POST /gate.php
16	**Packer / Compiler Check**	PEiD	Packed with **UPX**, compiled with Borland C++
17	**HTTP/HTTPS Inspection**	Wireshark	Sends encrypted browser credential data via HTTP POST

#	Step	Tool / Method	Findings
1 8	**VirusTotal Result**	VirusTotal	65+ detections, tagged as PonyStealer, Infostealer.Generic
1 9	**User Profile Data**	Manual	Found logs and dump files in %APPDATA%\Local\Temp\cache.db

---

Capabilities & Behaviors

Feature	Observed Behavior
Persistence	Via Registry: HKCU\...\Run\ponyload
Exfiltration	Sends credentials to remote C2 via POST /gate.php
Data Stolen	Stored browser passwords, FTP credentials, crypto wallets
Injection	Code injected into explorer.exe memory
Packer	UPX-packed executable
Anti-Analysis	Encrypted strings, base64-encoded payload

Indicators of Compromise (IOCs)

Type	Value
SHA-256	651bc2c3fbe672fe8b8016c56df4e933b9d35571d7eb7b65dfb5184c98a02f3a
MD5	9cdd788de6736a8e7611f6e004dbbcb0
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ponyload
Dropped File	%APPDATA%\Local\Temp\cache.db
Domain	stealhub[.]xyz, ponyloader[.]pw
IP Address	185.142.236.20, 89.45.67.231

Type	Value
HTTP Paths	/gate.php, /panel/login.php
Strings	formgrabber, POST, password=, ftp://, smtp://
YARA Matches	pony_loader, UPX_packed, cred_stealer_browsers

🚨 Detection Snippets

YARA Rule (PonyStealer)

yara

CopyEdit

```
rule PonyStealer_Generic
{
   strings:
      $s1 = "gate.php"
      $s2 = "formgrabber"
      $s3 = "password="
      $upx = "UPX0"
   condition:
      all of them
}
```

Snort Rule (C2 Detection)

snort

CopyEdit

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Pony Stealer C2 Beacon";
content:"POST /gate.php"; sid:100002;)
```

PoC Summary

plaintext

CopyEdit

[PoC - Gen:Heur.PonyStealer.2]

SHA-256: 651bc2c3fbe672fe8b8016c56df4e933b9d35571d7eb7b65dfb5184c98a02f3a

MD5: 9cdd788de6736a8e7611f6e004dbbcb0

Type: Infostealer Trojan

Behavior:

- Steals browser credentials, FTP info, crypto wallets
- Sends data via POST to /gate.php
- Injects into explorer.exe
- Persists using Registry: HKCU\...\Run\ponyload
- Encrypted strings and base64 payload

IOCs:

- Domain: stealhub[.]xyz
- IP: 185.142.236.20
- Dropped file: %APPDATA%\Local\Temp\cache.db

Packer: UPX

Compiler: Borland C++