QuartzLine Infostealer Campaign

In early October 2026, an eCrime campaign launched a malvertising campaign to lure users into downloading a malicious PDF reader. Threat actors distributed **QuartzLine**, a trojanized PDF reader with backdoor functionality designed to steal browser credentials, cookies, and browsing history while establishing persistence.

In response, MCNC Cybersecurity Operations identified infected hosts, placed blocks on known Indicators of Compromise (IOCs), and deployed an automated/manual remediation strategy.

Key Campaign Findings & Attack Vector

- **Primary Delivery Vector:** Search engine malvertising. Users searching for PDF software were redirected through malicious domain chains to payload-hosting infrastructure.
- **Impact & Scope:** Broad multi-sector targeting, with a focus on the education sector.
- **Malware Capabilities:**
  - Masquerades as a legitimate PDF viewer/reader decoy.
  - Establishes persistence using Windows Scheduled Tasks.
  - Exfiltrates targeted web browser data (credentials, cookies, history).
  - Drops additional secondary payloads onto disk.

Remediation Steps

While perimeter blocking and detection rules prevent new executions, previously infected environments require systematic cleanup. A **6-Step Cleanup Process** is utilized to ensure full remediation without triggering task-scheduler persistence loops:

1. **Remove Auto-Start Triggers:** Terminate and delete scheduled tasks (Task Scheduler).
2. **Kill Malware Processes:** End active malicious processes in Task Manager.
3. **Delete Malware Directories:** Permanently remove malicious files stored in AppData\Local.
4. **Remove Original Installers:** Delete malicious download payloads.
5. **Browser Cleanup:** Reset hijacked settings, remove unapproved extensions, and clear stored session cookies/data.
6. **Identity & Session Sign-Off:** Perform mandatory password resets, revoke active cloud/SSO sessions, and re-establish secure network access.

Key Takeaway: The cybersecurity tool space is actively updating their joint position against this attack to successfully flag and/or prevent new QuartzLine executions. Sectigo has revoked the cert used to sign this software. Existing infections can be remediated through the 6-step recovery process and automated scripts exist to eliminate infected endpoints.

To prevent future attacks such as these, train your users to avoid downloading software off the internet and to engage local IT for approved software solutions. This software installs into the User Space so that even environments with Admin privileges locked down can be impacted.

Full Remediation Steps

Follow these **6 steps in exact order**. Doing Step 1 before Step 2 is critical. If you kill the processes before deleting the Scheduled Tasks, the task might restart the program while you are trying to delete the folders.

Step 1: Remove the Auto-Start Triggers (Task Scheduler)

1. Press `Win + R`, type `taskschd.msc`, and press **Enter** (or search Start for **Task Scheduler** and run as Administrator).
2. In the left sidebar, click directly on the top folder: `Task Scheduler Library`.
3. In the middle pane, look for any of the following task names. If found, **Right-Click** → **End**, then **Right-Click** → **Delete**:
    - [ ] `QuartzlineUpdateCheck`
    - [ ] `CairaServiceCheck`
    - [ ] `IronbarkUpdateCheck`
    - [ ] `HostHealthCacheCheck-...` *(followed by a 32-character code)*
    - [ ] `HostHealthCacheCleanup-...` *(followed by a 32-character code)*
4. **Check for Renamed/Mutated Tasks:** While still in `Task Scheduler Library`, click each remaining non-Microsoft task one by one and click the `Actions` tab at the bottom.
    - [ ] Look at the **Details** column (`Start a program`). If *any* task points to `AppData\Local\<FolderName>` **AND** has `--uid=` or `--check` or `--update-check` at the end, **Write down that** `<FolderName>`, then **End** and **Delete** that task.

Step 2: Kill the Running Malware Processes (Task Manager)

1. Press `Ctrl + Shift + Esc` to open **Task Manager** (click *More details* if in compact view).
2. On the **Processes** (or **Details**) tab, sort by Name and look for any of the following. If running, **Right-Click** → **End task**:
    - [ ] `quartzline.exe`
    - [ ] `caira.exe`
    - [ ] `ironbark.exe`
    - [ ] `hosthealth.exe`
    - [ ] `updater-helper.exe`
    - [ ] `payload.exe`
    - [ ] Any `.exe` matching a new folder name you found in Step 1.4.

Step 3: Delete the Malware Folders (AppData\Local)

1. Press `Win + R`, type `%localappdata%` (or navigate to `C:\Users\<InfectedUsername>\AppData\Local`), and press **Enter**.
2. *(Note: If the tech logged in with their own Admin account instead of the user's account, they must manually browse to* `C:\Users\<InfectedUsername>\AppData\Local`*).*
3. Look for and **Shift + Delete** (permanently delete) any of these folders:
    - [ ] `QuartzLine`
    - [ ] `Caira`
    - [ ] `IronBar`
    - [ ] `HostHealthCache`
    - [ ] `DevicePerfCache`
    - [ ] Any new folder name you wrote down in Step 1.4.
    - *(If Windows says "Folder in Use", go back to Step 2—the process inside that folder is still running).*

Step 4: Delete the Original Installer (Downloads Folder)

1. Open `C:\Users\<InfectedUsername>\Downloads`.
2. Sort by **Date modified** (look around the date of initial infection, or search for `*.exe`).
3. **Shift + Delete** any installer files matching:
    - [ ] `QuartzLine_*.exe` *(e.g.,* `QuartzLine_1.2006.34.exe` *or* `QuartzLine_1.4577.33.exe`*)*
    - [ ] `Caira_*.exe`
    - [ ] `IronBark_*.exe`
    - [ ] Any questionable "free template / PDF reader / calendar" `.exe`
4. Empty the Windows **Recycle Bin**.

Step 5: Clean Up Google Chrome & Microsoft Edge

Because `ironbark.exe` modifies browser settings and hijacks sessions:

1. Open **Google Chrome** on the user's profile:
    - [ ] Go to `chrome://extensions` and **Remove** any unfamiliar or unapproved extensions.
    - [ ] Go to `chrome://settings/reset` → Click **Restore settings to their original defaults** → **Reset settings** (this clears hijacked startup pages and `Secure Preferences` modifications without deleting bookmarks).
    - [ ] Go to `chrome://settings/clearBrowserData` → Select **Cookies and other site data** and **Cached images and files** (*Time range: All time*) → **Clear data**.
2. Repeat the exact same check in **Microsoft Edge** (`edge://extensions` and `edge://settings/reset`).

Step 6: Identity & Network Sign-Off (Helpdesk / Admin)

- [ ] **Reset User Password:** Force an Active Directory / Entra ID password reset for the user.
- [ ] **Revoke Active Sessions:** In Microsoft 365 / Entra ID / Google Workspace, click **Revoke all active sessions / Sign out everywhere** so any session cookies stolen by `ironbark.exe` before cleanup are invalidated.

    - **Treat anything saved in a browser password as compromised**
- [ ] **Release Containment:** If the laptop was placed in CrowdStrike Network Containment, release it and verify normal network connectivity.

URLs to Block

- alberfine[.]s3[.]us-east-2[.]amazonaws[.]com
- beatramiro[.]com
- biggerworldclassstandard[.]com
- cdn[.]pdfmaestro[.]ai
- chrome-history-backup[.]s3[.]us-east-2[.]amazonaws[.]com
- commonhedgehogs[.]com
- duskhollow[.]s3[.]us-east-2[.]amazonaws[.]com
- guessgooseberries[.]com
- healskills[.]com
- leolin15[.]s3[.]us-east-2[.]amazonaws[.]com
- molehawks[.]com
- motherotters[.]com
- pdfmaestro[.]ai
- softwareslizards[.]com
- tabbyottercub[.]com
- thankyou[.]molehawks[.]com
- topsmagnificentgrade[.]com
- westbeavers[.]com

Collected IOCs

An exhaustive list of Indicators of Compromise (IOCs) associated with the QuartzLine / PaperLine campaign, including cryptographic hashes, code-signing certificates, host artifacts, and network infrastructure.

- **Last Updated:** 2026-10-15
- **Associated Threat Names:** QuartzLine, PaperLine, FieldDesk, PageStone, Caira, IronBark, PDFMaestro, Zenith Backdoor, CLOUDHAZE, PinkHugeSearch

---

1. Cryptographic Hashes

SHA-256 Hashes (Executables & Droppers)

- `74aaa6b54133bbb2e77b2ae874e9900a907c269058f798a0a1197288ba1f7124` — `caira.exe` (`\AppData\Local\Caira\caira.exe`)

- 7f1db334fd3302cf98dd4afddf6f90e98e2a496fe7e86bf1832b89d02f3d73c3 — quartzline.exe / paperline.exe (~7.89 MB Rust/Slint PDF Viewer + Zenith implant)
- 25ea334b75beede8dcab4c4460313c3013c35e55c16cd066231d80ecfe4c0653 — Initial dropper / installer (<25MB in Downloads)
- 3c813ea19ff2e3e2cf566ec69753ba637bb243b4b4e8416dc8ebf68e93016a1d — Initial dropper / installer
- 0fa4082c6fda0c2885eade0e4f63a2abfeaa26581f903e6784682f5fbd9d0d77 — Initial dropper / installer
- 90ddbf4be95b271de76384f4939eb6f165aa9461f8383a6e6f000f9256b34f97 — Initial dropper / installer

Additional Hashes (Primary Sample)

- **MD5:** d62d4b7811e37ce789b40ff9343e3458
- **SHA-1:** 3b00f51e00d8e10bf513414a13a4da96c4abfc32
- **SHA3-384:** b552c4a170faf4fb68f6e5a41ee819d88d04803a96fa05516dc0a8c967378a201f2956e31cef644ac724d8c3f69a45c3
- **ImpHash:** e2af0eaf9f3adfecfc89acd422170d75

---

2. Code-Signing Certificate Indicators

- **Subject Organization:** Guangzhou Guoying Communication Technology Co., Ltd.
- **Issuer Common Name:** Sectigo Public Code Signing CA EV R36
- **Certificate Type:** Extended Validation (EV) Code Signing (sha256WithRSAEncryption)
- **SHA-256 Thumbprint:** EA277BE59F1F1854B1BEDBA0439A011FCFB0A23D90DBB8A99F5AE87512A17470
- **Serial Number:** 1B56CB4E99FB9444645A1CE7FFC0A46B
- **Validity Period:** 2026-04-01 to 2027-04-01
- **Revocation Status:** Revoked 2026-10-09 (Privilege Withdrawn)
- **Spoofed Metadata:** Summit Works / Paperline Document Viewer / QuartzLine

---

3. Filenames, Directories & Host Artifacts

Primary Lure & Implant Binaries

- quartzline.exe / caira.exe / ironbark.exe / paperline.exe / fielddesk.exe / pagestone.exe / pdfmaestro.exe
- **Versioned Installers Pattern:** QuartzLine_1.4577.33.exe, QuartzLine_1.3177.99.exe, etc.
- **Staging & Helper Binaries:** hosthealth.exe, updater-helper.exe, payload.exe, previous.exe
- **Configuration & Data Files:** terrain.dat, plan.b64, deployApp.ps1, complete.json

Directory Paths

- %LOCALAPPDATA%\QuartzLine\
- %LOCALAPPDATA%\Caira\
- %LOCALAPPDATA%\IronBark\
- %LOCALAPPDATA%\PaperLine\
- %LOCALAPPDATA%\HostHealthCache\
- %LOCALAPPDATA%\DevicePerfCache\

Scheduled Tasks & CLI Signatures

- **QuartzlineUpdateCheck:** `%LOCALAPPDATA%\QuartzLine\quartzline.exe --update-check --uid=<UUID>`
- **CairaServiceCheck:** `%LOCALAPPDATA%\Caira\caira.exe --check --uid=<UUID>`
- **IronbarkUpdateCheck:** `%LOCALAPPDATA%\IronBark\ironbark.exe --update-check --uid=<UUID>`

---

4. Network & C2 Infrastructure

Rotating Domains & AWS Buckets

- beatramiro[.]com
- westbeavers[.]com
- motherotters[.]com
- healskills[.]com
- molehawks[.]com
- chrome-history-backup[.]s3[.]us-east-2[.]amazonaws[.]com
- alberfine[.]s3[.]us-east-2[.]amazonaws[.]com
- duskhollow[.]s3[.]us-east-2[.]amazonaws[.]com

Active Check-In Endpoints

- hxxps://westbeavers[.]com/quarry/vein
- hxxps://westbeavers[.]com/quarry/deposit
- hxxps://motherotters[.]com/quarry/vein
- hxxps://healskills[.]com/quarry/vein

---

5. Associated IP Addresses

- 104.21.84.219 — westbeavers[.]com (Cloudflare)
- 104.21.80.21 — motherotters[.]com (Cloudflare)

172.67.207.40 — healskills[.]com (Cloudflare)