Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

EMERGING THREAT ADVISORY
QUARTZLINE MALWARE CAMPAIGN

16 OCT 2026

Executive Summary

The Cal-CSIC in coordination with CDT has become aware of an on-going QuartzLine malware campaign affecting higher education and Government sectors at least since September 2026. Public analysis identifies a working PDF viewer that conceals a backdoor, enabling remote control and changes to browser data. Cal-CSIC assesses that the software poses a risk to sensitive information and trusted use of affected systems, even when it appears to function normally. Organizations should identify and contain affected devices, preserve evidence, and review associated account activity, browser extensions, settings, and profile changes for signs of unauthorized access, malware-related modifications, and potential exposure of sensitive information.

Anatomy of Attack

Execution

QuartzLine is a Rust-based Windows backdoor with a functional PDF parser and viewer. Launching it also starts the embedded zenith backdoor. File metadata identifies Paperline Document Viewer / Summit Works; its EV signer is a different company.

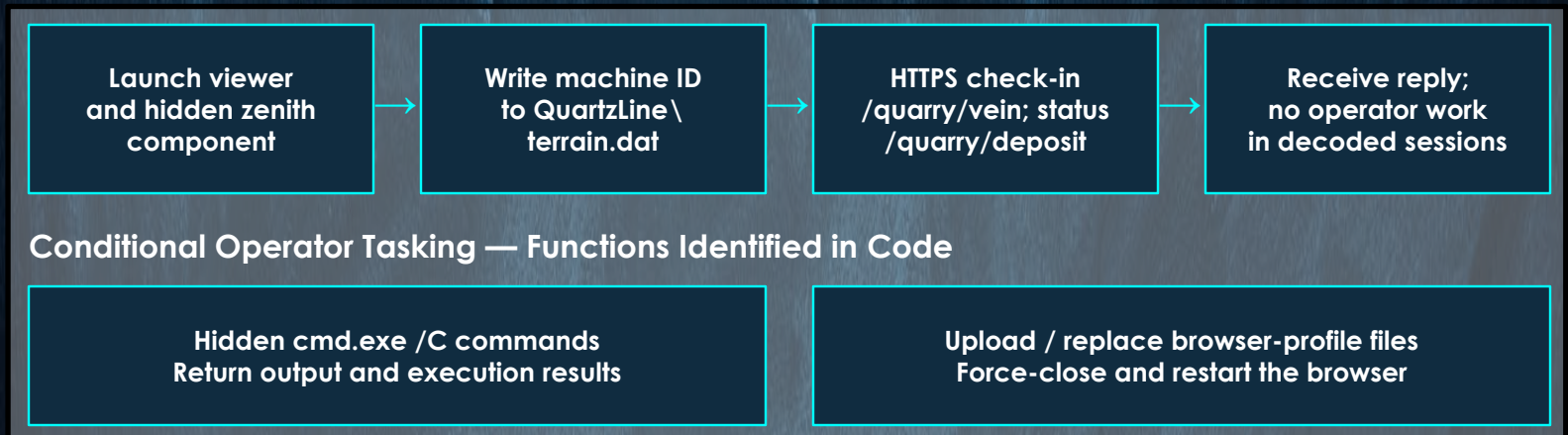


Figure 1. QuartzLine lifecycle. The upper sequence was observed in published sandbox analysis; the lower functions were identified in code. [1]

Cal-CSIC Analyst Comment

A valid digital signature and functional software do not guarantee that a utility is safe, as legitimate tools may contain or be used to execute unauthorized remote-control capabilities. Verify the software's publisher and signature, examine endpoint activity for suspicious execution or persistence, and review associated network connections for communications with unauthorized or malicious infrastructure. The following techniques are cataloged in MITRE ATT&CK version 20. [1]

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and is TLP:GREEN. Except for TLP: CLEAR, all designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

EMERGING THREAT ADVISORY
QUARTZLINE MALWARE CAMPAIGN

16 OCT 2026

Observed TTPs and Technical Analysis

Host Identification

The backdoor stores its machine identifier in %LOCALAPPDATA%\QuartzLine\terrain.dat, alongside settings-style entries and a final zenith=<uuid> line. This retains an identifier; it does not itself establish automatic execution at startup. [1]

Command and Control

HTTPS POST traffic carries check-in and status messages. The check-in includes the implant version, build/tag, executable path, and machine ID. Messages pass through gzip, chained XOR, bit rotation, seeded shuffling, and Base64 encoding. Four decoded sandbox sessions received "no work" replies; two ten-minute runs showed no repeat contact. The Cal-CSIC recommends hunting for brief startup traffic rather than assuming a fixed beacon interval. [1]

MITRE ATT&CK Technique	Evidence	QuartzLine Procedure
T1071.001 — Web Protocols	Sandbox	HTTPS POST check-in and status traffic.
T1132.001 — Standard Encoding	Sandbox / code	Base64 wraps transformed C2 messages.
T1059.003 — Windows Command Shell	Code capability	Run server-supplied commands with cmd /C.
T1564.003 — Hidden Window	Code capability	Run the command shell without a visible window.
T1005 — Data from Local System	Code capability	Read browser-profile files selected by the server.
T1041 — Exfiltration Over C2 Channel	Code capability	Upload selected profile files to the tasking server.

Analytic mappings based on the reported procedures; code capabilities were not observed as live tasks. [1–5]

Cal-CSIC Assessment

Cal-CSIC assesses that QuartzLine provides a foothold for unauthorized control and browser-data manipulation. Confidence is moderate, based on one detailed reverse-engineering report with supporting sandbox traffic. Check-ins establish C2 contact; the command and browser actions remain code-derived capabilities. [1]

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and is TLP:GREEN. Except for TLP: CLEAR, all designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

EMERGING THREAT ADVISORY
QUARTZLINE MALWARE CAMPAIGN

16 OCT 2026

Indicators of Compromise

Artifact	Reported Value / Context [1]
File hashes	SHA-256: 7f1db334fd3302cf98dd4afddf6f90e98e2a496fe7e86bf1832b89d02f3d73c3 MD5: d62d4b7811e37ce789b40ff9343e3458
Observed Filenames	paperline.exe; QuartzLine_1.3177.99.exe; QuartzLine_1.9758.76.exe; QuartzLine_1.9740.56.exe
C2 Domains	westbeavers[.]com; motherotters[.]com; healskills[.]com
Observed HTTPS Paths	/quarry/vein — check-in /quarry/deposit — status
Host Artifacts	%LOCALAPPDATA%\QuartzLine\terrain.dat Settings-style file ending in zenith=<uuid>
Protocol ilentifiers	Implant 6.1.3; build QNPVXZGJYUSLTREHK; tag QZRT07
Signing Certificate	Guangzhou Guoying Communication Technology Co., Ltd. Serial: 1b56cb4e99fb9444645a1ce7ffc0a46b Sectigo Public Code Signing CA EV R36; reported revoked.

Hunt Priorities and Pyramid of Pain

• Hashes and domains: scope quickly using exact matches, then correlate each result with the responsible process.
• Host and network artifacts: search terrain.dat, zenith=, the two /quarry/ paths, and product/signer mismatches.
• Tools and TTPs: prioritize viewer-to-shell execution and correlated browser-profile changes, termination, and restart. These detections can survive renaming or rebuilding.
• Apply domain-aware controls. The reported servers use Cloudflare; shared CDN addresses are unsuitable as blanket block indicators. [1, 5]

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and is TLP:GREEN. Except for TLP: CLEAR, all designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

EMERGING THREAT ADVISORY
QUARTZLINE MALWARE CAMPAIGN

16 OCT 2026

Hunt Package — Endpoint Telemetry

Microsoft Defender XDR advanced hunting. Adjust the dates to retained telemetry. Filename and behavior matches are leads for triage; the queries do not establish compromise alone. [1, 3, 4]

Hunt 1 — Sample and Host Artifacts

```
let Start = datetime(2026-09-01);
let End = datetime(2026-10-16);
let QuartzHash =
 "7f1db334fd3302cf98dd4afddf6f90e98e2a496fe7e86bf1832b89d02f3d73c3";
let QuartzMD5 = "d62d4b7811e37ce789b40ff9343e3458";
union DeviceFileEvents, DeviceProcessEvents
| where Timestamp >= Start and Timestamp < End
| where SHA256 =~ QuartzHash or MD5 =~ QuartzMD5
    or FileName =~ "paperline.exe"
    or FileName startswith "QuartzLine"
    or (FileName =~ "terrain.dat"
        and FolderPath contains @"\QuartzLine")
| project Timestamp, DeviceId, ActionType, FileName, FolderPath,
          SHA256, MD5, InitiatingProcessFileName
| order by Timestamp desc
```

Hunt 2 — Document Viewer Launching a Shell

```
DeviceProcessEvents
| where Timestamp >= datetime(2026-09-01)
    and Timestamp < datetime(2026-10-16)
| where FileName =~ "cmd.exe"
| where ProcessCommandLine matches regex @"(?i)(^|\s)/c(\s|$)"
| where InitiatingProcessFileName =~ "paperline.exe"
    or InitiatingProcessFileName startswith "QuartzLine"
| project Timestamp, DeviceId, ProcessId, ProcessCommandLine,
          InitiatingProcessFileName, InitiatingProcessCommandLine
| order by Timestamp desc
```

Triage

Validate hashes, signatures, paths, and parent/child process identity. Inspect terrain.dat for zenith= using approved collection tools. SHA-256 is often unpopulated in Defender; calculate it from a preserved sample when needed. These analyst-authored queries require validation in local telemetry. [3, 4]

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and is TLP:GREEN. Except for TLP: CLEAR, all designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

EMERGING THREAT ADVISORY
QUARTZLINE MALWARE CAMPAIGN

16 OCT 2026

Hunt Package — Network and Browser Activity

Hunt 3 — C2 Domain Correlation

```
DeviceNetworkEvents
| where Timestamp >= datetime(2026-09-01)
    and Timestamp < datetime(2026-10-16)
| extend ParsedUrl = parse_url(iff(RemoteUrl contains "://",
   RemoteUrl, strcat("https://", RemoteUrl)))
| extend Host = tolower(tostring(ParsedUrl.Host))
| where Host in ("westbeavers.com", "motherotters.com",
                 "healskills.com")
| project Timestamp, DeviceId, RemoteUrl, RemoteIP, RemotePort,
          InitiatingProcessFileName, InitiatingProcessCommandLine
| order by Timestamp desc
```

Proxy / Secure Web Gateway Logs

Correlate HTTPS POST requests to /quarry/vein or /quarry/deposit with the reported domains, endpoint process, and startup time. The sample omits a User-Agent header. HTTP paths, methods, and headers require logs that expose this detail; DeviceNetworkEvents alone does not provide them. [1, 5]

Browser-Profile Behavior

Hunt for an unfamiliar viewer modifying Chromium-style profile files, running taskkill /F against a browser, and restarting it with --user-data-dir. Correlate events on the same device and process lineage within a short interval. Investigate the selected files and replacement contents. This hunt targets the implemented task handler. [1]

Recommendations

- Isolate confirmed affected endpoints and preserve binaries, terrain.dat, process records, and relevant network logs.
- Remove unauthorized software and investigate any follow-on commands, browser-profile changes, or additional access.
- Review affected browser extensions, settings, and accounts; revoke sessions or reset credentials when exposure is indicated.
- Restrict unapproved utilities through application control and review publisher identity, revocation status, and product metadata.
- Block validated malicious domains and file indicators; retain behavior detections for renamed variants. [1]

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and is TLP:GREEN. Except for TLP: CLEAR, all designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

EMERGING THREAT ADVISORY
QUARTZLINE MALWARE CAMPAIGN

16 OCT 2026

Supplemental - Caira.exe Analysis

According to public reporting, many endpoints affected by variants of the quartzline malware, often have the payload Caira.exe. This payload executes through Windows Task Scheduler while being hidden in encoded Powershell deployment wrappers.

Static Analysis identifies:
- Rust executable with HTTPS taskings
- Command/download handlers
- Browser-profile operations
- Host information queries

Indicators of Compromise

Artifact	Reported Value / Context [1]
File Hash	SHA-256: 74aaa6b54133bbb2e77b2ae874e9900a907c269058f798a0a1197288ba1f7124
Decoded Endpoint Pool	hxxps://topsmagnificentgrade[.]com hxxps://tabbyottercub[.]com hxxps://flawlessgradecheered[.]com Recovered from sample configuration; paths and failover ordering unresolved.
C2 Domains	westbeavers[.]com
Host Artifact	%LOCALAPPDATA%\Caira\caira.exe %LOCALAPPDATA%\Caira\deployment-*\payload.exe deployApp.ps1.b64; deployApp.ps1; deployApp.ps1.result.json; plan.b64; conf.upd (binary string

Priority Evidence to Preserve

When threat hunting for Caira.exe:

- Collect task XML
- Task name
- Triggers and registration history
- Any recoverable scripts/results
- Caira configuration
- Child-Parent Process relationships
- DNS/proxy/network records
- Browser extension and profile changes

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and is TLP:GREEN. Except for TLP: CLEAR, all designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

EMERGING THREAT ADVISORY
QUARTZLINE MALWARE CAMPAIGN

16 OCT 2026

Sources

1. Rogue Authority — A signed PDF viewer that quietly takes orders: the QuartzLine "zenith" backdoor. 9 October 2026.
2. MITRE ATT&CK
3. Microsoft Learn — DeviceFileEvents advanced hunting schema.
4. Microsoft Learn — DeviceProcessEvents advanced hunting schema.
5. Microsoft Learn — DeviceNetworkEvents advanced hunting schema.
6. David Bianco — The Pyramid of Pain.

SHARING, REPORTING, AND SUPPORT

Sharing information and intelligence to state, local, federal, and private partners will ensure organizations across California can be better informed and defended.

For questions, concerns, or support or are interested in sharing information or intelligence in any cyber related matter, contact the Cal-CSIC via:

916.636.2997

calcsic@caloes.ca.gov

Report suspicious or suspected foreign activity and incidents to:

Federal Officials at CISA and/or the FBI as applicable

Coordinate with your regional Fusion Center

SHARE information, intelligence, and IOCs with ISACs

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and is TLP:GREEN. Except for TLP: CLEAR, all designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.