BLACKSWAN CYBERSECURITY

THREAT ADVISORY

DigiCert Compromise (April 2026)

May 7, 2026

Background/Summary

In early April 2026, DigiCert, a major global Certificate Authority (CA), suffered a targeted social engineering attack against its customer support operations. A threat actor posed as a customer via the support chat channel and delivered a malicious ZIP file disguised as a screenshot. The archive contained a .scr (Windows screensaver) executable embedding a malicious payload.

The attack succeeded in compromising two support analyst endpoints (ENDPOINT1 on ~April 2 and ENDPOINT2 on ~April 4). The second compromise went undetected for nearly two weeks due to gaps in endpoint security (e.g., CrowdStrike sensor issues). Attackers used the compromised endpoints to access DigiCert's internal support portal. They leveraged a proxy feature allowing support staff to view customer accounts from the customer's perspective, gaining access to initialization codes for approved but pending Extended Validation (EV) Code Signing certificate orders.

This enabled the issuance of legitimate-looking EV Code Signing certificates. DigiCert identified the incident through third-party reports of certificates used in malware, leading to the revocation of 60 certificates by April 17 (27 explicitly linked to the attacker, including 11 used to sign malware; the rest were precautionary). Pending orders were canceled. No broader compromise of validation systems, other certificate types, or customer account management was identified. The exploited certificates were linked to the **Zhong Stealer** malware family (associated with Chinese GoldenEyeDog / APT-Q-27) used for credential theft and cryptocurrency targeting.

No broader PKI or customer data compromise occurred.

Threat

Financially motivated e-crime actors (consistent with Chinese cybercrime groups) are targeting code-signing certificates for malware evasion. The campaign exploits support channels and leverages signed binaries to bypass defenses like SmartScreen.

Risk

High for any environment trusting code-signed executables. Signed Zhong Stealer variants increase infection success, persistence, and stealth, particularly in fintech/crypto sectors.

Impact

- 60 certificates revoked (from DigiCert and affiliated CAs).
- At least 11 used to sign Zhong Stealer payloads.
- Temporary disruption for certificate holders; broader trust in signed software is affected.
- Overlap with unrelated Microsoft Defender false positives on DigiCert roots.

THREAT ADVISORY

DigiCert Compromise (April 2026)

May 7, 2026

IOCs

Attacker / Certificate Installation IPs (from DigiCert report):

82.23.186.8
154.12.185.32
45.144.227.12
203.160.68.2
154.12.185.30
62.197.153.45
45.144.227.29.

Zhong Stealer / Signed Malware IOCs (examples from analysis of samples signed with compromised certificates; monitor VirusTotal and EDR for full lists):

- **File Hashes** (representative from affected signed samples; see Gist for additional certificate-linked hashes):
  - SHA256 examples associated with Zhong Stealer campaigns:
    - 02244934046333f45bc22abe6185e6ddda033342836062afb681a583aa7d827f
    - 1abffe97aafe9916b366da57458a78338598cab9742c2d9e03e4ad0ba11f29bf
  - Additional signed samples tied to compromised cert thumbprints (partial):
    - 3e4229f39f1764b2e504ff2ba116895fb53cd76e23f107b6a47fb0a162422c7c
    - 56b6571ded7d34c7d3adccc46a116f2960d7a2d77a7a4caa70abd23c99602eb7
    - f76c31ecdafb59279833f17f350d9c2b1317da269823097e8dd1736c72449c88

- **Behavioral / Malware Family IOCs**:
  - Malicious .scr files inside ZIP archives (disguised as screenshots).
  - Persistence via scheduled tasks, registry Run keys; binaries like k3.exe, updat.exe, uuu.exe, VideoManager.exe in AppData/Public.
  - C2 communication: Connections to Hong Kong-based Alibaba Cloud servers (e.g., over non-standard ports like 1131); domains/infrastructure such as uu.goldeyeuu.io or similar GoldenEyeDog-linked hosts.
  - Credential harvesting from browsers (especially Edge), extension data exfiltration.

Certificate Indicators: Monitor/revoke any remaining references to the 60 revoked EV Code Signing certificates (full serials/thumbprints in DigiCert's Mozilla Bugzilla report #2033170).

TTPs

- Social engineering via support chat + malicious .scr delivery.
- Endpoint compromise and abuse of legitimate proxy tools.
- Use of stolen EV certificates to sign stealer/RAT payloads for evasion.
- MITRE ATT&CK: T1566 (Phishing), T1204 (User Execution), T1553 (Subvert Trust Controls - Code Signing), etc.

THREAT ADVISORY

DigiCert Compromise (April 2026)

May 7, 2026

Recommendations

1. **Immediate Actions**:
   - Scan for and block the listed IOC IPs and Zhong Stealer indicators.
   - Verify code-signing certificates in your environment; reissue any from affected DigiCert CAs.
   - Update EDR/signature databases (post-Microsoft false positive fixes).
2. **Defensive Measures**:
   - **Endpoint Security**: Enforce strict application control (e.g., AppLocker, WDAC) to block .scr and unexpected executables. Harden EDR coverage and monitoring.
   - **Support/Helpdesk**: Train staff on attachment risks; restrict file types/uploads in chat portals. Implement strict MFA and session monitoring for support tools.
   - **Code Signing Hygiene**: Use hardware security modules (HSMs) for keys; monitor for anomalous signing activity; prefer strict policies (e.g., EV where possible) and timely revocation checking.
   - **Network**: Block or alert on the listed IPs; segment support systems; enhance logging for portal/proxy access.
3. **Longer-Term**:
   - Adopt certificate transparency and pinning where feasible.
   - Regular CA vendor risk assessments and incident response playbooks for PKI incidents.
   - Promote least-privilege in internal tools (e.g., mask sensitive codes in proxy views, as DigiCert implemented).
   - Community vigilance: Report suspicious signed binaries promptly to CAs.

Contact Blackswan Cybersecurity at 855-BLK-SWAN or
Contact@BlackswanCybersecurity.com