INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-04 06:06 UTC

DigiCert EV Code-Signing Breach Enables Zhong Stealer Campaign; Microsoft Defender Misfires on Legitimate Root Certificates

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0266
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Defender (Windows), Windows AuthRoot certificate store, DigiCert EV Code Signing Certificates, Lenovo / Kingston / Shuttle Inc / Palit Microsystems (certificate holders)
Published	2026-05-03T14:11:25
Discovery Source	Rss

Executive Summary

A breach of DigiCert's customer support environment in early April 2026 allowed a Chinese APT-linked threat actor to obtain EV code-signing certificates, which were used to sign malware payloads in a campaign called Zhong Stealer. A separate incident occurred on April 30, 2026, when a Microsoft Defender signature update incorrectly flagged legitimate DigiCert root certificates as malware, removing them from enterprise trust stores and causing widespread operational disruption. Organizations relying on EV-signed software for trust verification and Windows endpoints running Defender are exposed to both malware infiltration risk and self-inflicted availability loss from the defensive overreach.

Technical Analysis

DigiCert's customer support environment was compromised in early April 2026, allowing a threat actor to extract initialization codes for approved EV code-signing certificate orders. Sixty certificates were revoked; 27 are confirmed linked to the Zhong Stealer campaign, a Chinese APT-attributed infostealer distributed via signed malicious payloads (per threat intelligence sources; verify against official DigiCert revocation list). EV code-signing status bypasses many security controls that rely on signature trust level as a risk signal (T1553.002, Code Signing). The campaign also uses phishing emails (T1566.001), ingress tool transfer (T1105), and command script execution (T1059). A secondary failure occurred on April 30, 2026: Microsoft Defender's signature update misidentified legitimate DigiCert root certificates as Trojan:Win32/Cerdigent.A!dha (T1562.001, Impair Defenses: Disable or Modify Tools), removing them from the Windows AuthRoot certificate

store on affected enterprise endpoints. Relevant CWE mappings: CWE-295 (Improper Certificate Validation), CWE-345 (Insufficient Verification of Data Authenticity), CWE-284 (Improper Access Control), CWE-693 (Protection Mechanism Failure). Affected certificate holders include Lenovo, Kingston, Shuttle Inc, and Palit Microsystems. No CVE has been assigned. Both issues are reported as largely contained. Source quality is moderate (T3 news sources predominate; one T1 Microsoft community thread confirmed).

Action Checklist

1. Step 1: Containment. Audit your software inventory for executables signed by any of the 60 revoked DigiCert EV certificates. Cross-reference against DigiCert's published revocation list. Temporarily block execution of newly signed binaries from affected certificate holders (Lenovo, Kingston, Shuttle Inc, Palit Microsystems) until signatures are re-validated against current trust chains.
2. Step 2: Detection. Check Windows Event Log and Defender quarantine logs for detections of Trojan:Win32/Cerdigent.A!dha. Query endpoint telemetry for certificate revocation events affecting DigiCert roots in the Windows AuthRoot store. Monitor for Zhong Stealer IOCs: look for unusual outbound connections, credential-store access patterns, and unsigned or recently signed executables executing from user-writable directories.
3. Step 3: Eradication. Apply the corrected Microsoft Defender signature update to restore legitimate DigiCert root certificates to the Windows AuthRoot trust store. Verify with Microsoft's published guidance at the confirmed T1 source: https://learn.microsoft.com/en-us/answers/questions/5610417/windows-defender-flagged-our-company-digital-certi. Remove any Zhong Stealer payloads identified during detection. Revoke and reissue any internal code-signing certificates if obtained through DigiCert's affected customer support channel during the April 2026 window.
4. Step 4: Recovery. After applying the corrected Defender signatures, validate that DigiCert root certificates are present and trusted in the AuthRoot store on affected endpoints. Re-test certificate-dependent applications (TLS connections, signed software execution, authenticode validation). Monitor Defender telemetry for recurrence of the Cerdigent.A!dha false positive. Confirm no Zhong Stealer persistence mechanisms remain via full endpoint scan with updated signatures.
5. Step 5: Post-Incident. Conduct a control gap review against NIST SP 800-161 (supply chain risk management) for certificate authority dependencies. Set up certificate transparency log monitoring to detect unauthorized issuance against your domains. Establish alerting on bulk certificate revocation events from CAs in your trust chain. Review your CA vendor selection criteria to include incident response and breach notification commitments. Document this incident as a case study for the risk of trust-chain overreach in automated defensive tooling.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership, legal counsel, and executive stakeholders if any of the following conditions are confirmed: (1) a Zhong Stealer payload executed successfully on an endpoint with access to PII, PHI, financial data, or privileged credentials — triggering applicable breach notification obligations under HIPAA, state privacy statutes, or PCI DSS Requirement 12.10.4; (2) the DigiCert-breached customer support channel was used to obtain or manage your organization's own EV code-signing certificates during the April 2026 window, indicating direct supply chain compromise of your signing infrastructure; or (3) the Defender AuthRoot removal caused a CRL or OCSP validation failure that allowed revoked certificates (including the 60 compromised EV certificates) to be treated as trusted during the outage window, potentially enabling Zhong Stealer payloads to execute undetected.
Recovery Notes	Recovery validation must confirm two independent failure modes are resolved: the Zhong Stealer active infection and the Defender-induced AuthRoot trust store corruption — do not close the incident until both are verified clean on all affected endpoints, as partial recovery (e.g., Defender signatures updated but compromised EV-signed binaries still present) leaves the environment exposed. Monitor Defender telemetry and CAPI2 logs continuously for a minimum of 14 days post-recovery, as APT-linked campaigns such as Zhong Stealer typically include secondary persistence mechanisms (scheduled tasks, DLL side-loading, or registry-based autoruns) that may not be detected in an initial full scan. Before returning affected endpoints to full production trust, re-validate all internally deployed software packages signed by Lenovo, Kingston, Shuttle Inc, or Palit Microsystems certificates against the current DigiCert revocation list, since the trust store disruption may have masked legitimate revocation checks during the outage window.
Forensic Artifacts	Windows AuthRoot certificate store registry export — HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates — capturing pre- and post-incident states to identify which DigiCert root thumbprints were removed by the Defender signature regression and whether any unauthorized certificates were introduced during the incident window | CAPI2 Operational Event Log (Applications and Services Logs\Microsoft\Windows\CAPI2\Operational) — Event IDs 11 (CertVerifyRevocation) and 30 (X509Objects) — recording certificate chain validation attempts and failures specific to DigiCert-anchored chains during the April 30 Defender signature regression and any Zhong Stealer execution attempts | Windows Defender Quarantine folder contents at C:\ProgramData\Microsoft\Windows Defender\Quarantine\ — containing VDM-encoded copies of payloads detected as Trojan:Win32/Cerdigent.A!dha, recoverable via MpCmdRun.exe for static analysis to confirm whether detections were Zhong Stealer payloads or legitimate DigiCert-signed binaries misclassified by the faulty signature update | Prefetch files under C:\Windows\Prefetch\ for executables signed by the 60 compromised EV certificates — recording first and last execution timestamps, loaded DLL paths, and parent process context even if the Zhong Stealer payload was subsequently deleted or quarantined, establishing a definitive execution timeline | Sysmon Event ID 10 (ProcessAccess) targeting LSASS and Event ID 3 (NetworkConnect) from executables in user-writable directories (C:\Users, C:\ProgramData, C:\Temp) — capturing Zhong Stealer credential harvesting activity against Windows Credential Manager and browser stores, and outbound C2 connection metadata including destination IP, port, and initiating process image path

Per-Action IR Details

Step 1: Containment — Audit your software inventory for executables signed by any of the 60 revoked DigiCert EV certificates. Cross-reference against DigiCert's published revocation list. Temporarily block execution of newly signed binaries from affected certificate holders (Lenovo, Kingston, Shuttle Inc, Palit Microsystems) until signatures are re-validated against current trust chains.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-7 (Least Functionality — restrict unauthorized software execution), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Use Sysinternals Sigcheck to enumerate all signed executables and dump their certificate thumbprints: `sigcheck -tv -c -a C:\` redirected to CSV, then filter output against DigiCert's published list of 60 revoked thumbprints. On endpoints, deploy an AppLocker or Windows Defender Application Control (WDAC) policy scoped to Publisher conditions that blocks the specific Subject CN values for Lenovo, Kingston, Shuttle Inc, and Palit Microsystems certificates issued between January and April 2026. No SIEM required — a PowerShell script using `Get-AuthenticodeSignature` recursively across Program Files and user-writable directories (C:\Users, C:\ProgramData, C:\Temp) can be run by one analyst across the fleet via PSRemoting.

Evidence: Before blocking, snapshot the full Authenticode signature chain for every flagged executable using `sigcheck -a -v ` and preserve the output — this captures the signer thumbprint, certificate serial number, timestamp authority, and chain validity status, which will be needed to confirm whether Zhong Stealer payloads were signed under one of the 60 compromised EV certificates. Also export the current Windows AuthRoot and Intermediate CA store state via `certutil -store AuthRoot > authroot_baseline.txt` and `certutil -store CA > intca_baseline.txt` before any remediation actions alter the trust store, preserving the pre-remediation chain-of-custody state for forensic comparison.

Step 2: Detection — Check Windows Event Log and Defender quarantine logs for detections of Trojan:Win32/Cerdigent.A!dha. Query endpoint telemetry for certificate revocation events affecting DigiCert roots in the Windows AuthRoot store. Monitor for Zhong Stealer IOCs: look for unusual outbound connections, credential-store access patterns, and unsigned or recently signed executables executing from user-writable directories.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For Cerdigent.A!dha detections: query Windows Event Log — Application and Services Logs\Microsoft\Windows\Windows Defender\Operational — for Event ID 1116 (malware detected) and 1117 (malware action taken), filtering on ThreatName containing 'Cerdigent'. For AuthRoot store tampering caused by the Defender signature regression: query Security Event Log for Event ID 4657 (registry value modified) on key `HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates` to identify when DigiCert root thumbprints were removed. For Zhong Stealer credential-store access: deploy Sysmon with EventID 10 (ProcessAccess) rules targeting LSASS as TargetImage, and EventID 11 (FileCreate) for writes to `%APPDATA%\Microsoft\Credentials` and browser credential storage paths. Use this Sigma rule pattern: process creation (EventID 4688 or Sysmon EventID 1) where ParentImage is a Lenovo/Kingston/Palit/Shuttle binary signed with a certificate issued April 2026 spawning cmd.exe, powershell.exe, or regsvr32.exe.

Evidence: Collect the following before any quarantine or remediation actions alter available evidence: (1) Windows Defender quarantine folder contents at `C:\ProgramData\Microsoft\Windows Defender\Quarantine\` — Zhong Stealer payloads removed by Defender will be stored here in VDM-encoded format recoverable with MpCmdRun.exe; (2) Prefetch files under `C:\Windows\Prefetch\` for any executable names corresponding to known Zhong Stealer dropper filenames, which record execution timestamps and loaded DLL paths even after file deletion; (3) Sysmon Event ID 3 (NetworkConnect) logs capturing outbound connections from user-writable directory executables, preserving destination IPs and ports associated with Zhong Stealer C2 infrastructure; (4) CAPI2 Event Log (Applications and Services Logs\Microsoft\Windows\CAPI2\Operational) Event ID 11 (CertVerifyRevocation) and Event ID 30 (X509Objects) to reconstruct which DigiCert root certificates were evaluated, revoked, or removed during the April 30 Defender signature regression window.

Step 3: Eradication — Apply the corrected Microsoft Defender signature update to restore legitimate DigiCert root certificates to the Windows AuthRoot trust store. Verify with Microsoft's published guidance at the

confirmed T1 source: https://learn.microsoft.com/en-us/answers/questions/5610417/windows-defender-flagged-our-company-digital-certi. Remove any Zhong Stealer payloads identified during detection. Revoke and reissue any internal code-signing certificates if obtained through DigiCert's affected customer support channel during the April 2026 window.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: To apply the corrected Defender signature update without WSUS or SCCM: run `MpCmdRun.exe -SignatureUpdate` on each affected endpoint, then verify the engine and signature version via `MpCmdRun.exe -CheckSignatureUpdate` or `Get-MpComputerStatus | Select AntivirusSignatureVersion, AntivirusSignatureLastUpdated`. For Zhong Stealer payload removal: run `MpCmdRun.exe -Scan -ScanType 2` (full scan) with updated signatures before deletion to generate a detection record, then use `MpCmdRun.exe -RemoveDefinitions -DynamicSignatures` only if a specific dynamic signature is confirmed as the false-positive source per Microsoft guidance. For certificate reissuance verification: use `certutil -verify -urlfetch ` to confirm the replacement certificate chains to a non-revoked DigiCert root and passes OCSP/CRL checks. Document each remediation action with before/after `certutil -store AuthRoot` output to satisfy NIST AU-3 (Content of Audit Records) requirements without a SIEM.

Evidence: Before executing eradication, preserve: (1) a memory image of any endpoint where Zhong Stealer execution is confirmed — use WinPmem (free, open source) to capture a raw memory dump, which may contain decrypted credential material, injected code, or C2 configuration that is lost after reboot or payload removal; (2) a full copy of the Defender quarantine folder (`C:\ProgramData\Microsoft\Windows Defender\Quarantine\`) as an encrypted archive before signatures are updated, since the corrected signatures may re-classify quarantined files and alter their metadata; (3) the specific Defender signature version that caused the AuthRoot removal, recorded from `Get-MpComputerStatus | Select AntivirusSignatureVersion` on an affected endpoint before the update is applied, to establish the exact regression window for change management documentation and potential regulatory reporting.

Step 4: Recovery — After applying the corrected Defender signatures, validate that DigiCert root certificates are present and trusted in the AuthRoot store on affected endpoints. Re-test certificate-dependent applications (TLS connections, signed software execution, authenticode validation). Monitor Defender telemetry for recurrence of the Cerdigent.A!dha false positive. Confirm no Zhong Stealer persistence mechanisms remain via full endpoint scan with updated signatures.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Validate DigiCert root restoration without an enterprise MDM: run `certutil -store AuthRoot | findstr /i 'DigiCert'` on a sample of endpoints and compare thumbprints against DigiCert's published root list. For Authenticode validation recovery testing: use `sigcheck -tv` (Sysinternals) which will surface any certificates still failing chain validation due to residual AuthRoot store corruption. For persistence mechanism hunting specific to Zhong Stealer: query the Run and RunOnce registry keys (`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`) and scheduled tasks (`schtasks /query /fo LIST /v | findstr /i 'lenovo\|kingston\|palit\|shuttle'`) for any entries referencing the affected certificate holder names or paths in user-writable directories. Use Autoruns (Sysinternals) with VirusTotal integration enabled to flag any persistence entries pointing to recently signed or unsigned binaries.

Evidence: For post-recovery validation, retain: (1) a diff of the AuthRoot certificate store between the pre-remediation baseline (`authroot_baseline.txt` captured in Step 1) and the post-recovery state, confirming all legitimate DigiCert

roots are restored and no unauthorized certificates were added during the incident window; (2) Defender Event Log entries (Event ID 1150 and 1151 — antimalware platform health) confirming signature update success and the absence of further Cerdigent.A!dha detections post-update, establishing a clean-state timestamp for the recovery record; (3) CAPI2 Operational log Event ID 10 (X509Objects — successful certificate chain build) for DigiCert-anchored chains post-recovery, confirming that TLS and Authenticode operations dependent on the restored roots are functioning correctly.

Step 5: Post-Incident — Conduct a control gap review against NIST SP 800-161 (supply chain risk management) for certificate authority dependencies. Implement certificate transparency log monitoring to detect unauthorized issuance against your domains. Establish alerting on bulk certificate revocation events from CAs in your trust chain. Review your CA vendor selection criteria to include incident response and breach notification commitments. Document this incident as a case study for the risk of trust-chain overreach in automated defensive tooling.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), NIST SA-9 (External System Services — third-party CA dependency management), NIST SR-3 (Supply Chain Controls and Processes), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For certificate transparency (CT) log monitoring without a commercial platform: configure a free crt.sh monitoring account or use the `certspotter` open-source tool (Certspotter by SSLMate) to alert on any new certificate issuances for your organization's domains — this would have surfaced unauthorized EV certificate issuance from the DigiCert breach. For bulk revocation alerting: write a daily cron job or scheduled task using `certutil -URL ` to retrieve and diff CRL sequence numbers from DigiCert's CRL Distribution Points, alerting on delta counts exceeding a threshold (e.g., >10 new revocations in a single CRL update). For the NIST SP 800-161 gap review: map the DigiCert incident against SR-3 (Supply Chain Controls and Processes) and SR-6 (Supplier Assessments and Reviews) specifically — document whether your CA vendor contracts include breach notification SLAs, and whether your trust store management policy requires validation of CA security posture at renewal. Note: the step references NIST SP 800-161; the current authoritative designation for NIST supply chain risk management guidance is NIST SP 800-161 Rev. 1 (May 2022) — ensure the gap review references the revision.

Evidence: Preserve for post-incident review and potential regulatory reporting: (1) a complete timeline of the Defender signature regression — correlating the April 30 Defender signature version deployment timestamp (from Windows Update logs at `C:\Windows\SoftwareDistribution\ReportingEvents.log`) against the first AuthRoot removal Event ID 4657 observed, establishing the blast radius window; (2) a list of all certificate-dependent business processes disrupted by the AuthRoot removal (TLS failures, Authenticode blocks, application crashes), sourced from CAPI2 logs and application event logs (Event ID application errors referencing certificate validation failures), to support a business impact assessment; (3) DigiCert's breach notification communications and revocation advisory, preserved with receipt timestamps, to document whether the CA met contractual and regulatory breach notification obligations — relevant if your organization operates under FedRAMP, PCI DSS, or state breach notification statutes that include vendor incident notification requirements.

Detection Guidance

For the Defender false positive: query endpoint logs for Defender detections of 'Trojan:Win32/Cerdigent.A!dha' between April 30, 2026 and the date corrected signatures were deployed. Check Windows Event ID 1116 (malware detected) and 1117 (remediation action taken) in Microsoft-Windows-Windows Defender/Operational log. Identify endpoints where DigiCert root certificates were removed from the AuthRoot store by correlating certificate store change events. For Zhong Stealer: look for executables with EV code-signing signatures from the 60 revoked DigiCert certificates (cross-reference revocation list). Monitor for infostealer behavioral patterns:

access to browser credential stores, keychain or credential manager reads, staging of data in temp directories, and outbound connections to unfamiliar endpoints over non-standard ports. Attribution to the Zhong Stealer infostealer is based on threat intelligence reporting; no file hashes or C2 addresses have been published in primary sources. Hunting should focus on behavioral indicators (credential access, staging, signed binary execution) rather than hash-based detection. MITRE techniques to hunt: T1059 (script execution from signed binaries), T1078 (valid accounts accessed post-compromise), T1105 (ingress tool transfer), T1195.001/.002 (supply chain compromise indicators in software update channels). Treat the absence of published IOCs as a gap, not a clearance of exposure.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`not available`	No confirmed Zhong Stealer payload hashes are present in current source data. Absence should be treated as a detection gap, not a clearance.	LOW
DOMAIN	`not available`	No confirmed C2 domains for Zhong Stealer are present in current source data.	LOW

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1078** — Valid Accounts
- **T1562.001** — Disable or Modify Tools
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1553.002** — Code Signing
- **T1588.003** — Code Signing Certificates
- **T1195.002** — Compromise Software Supply Chain
- **T1105** — Ingress Tool Transfer
- **T1566.001** — Spearphishing Attachment

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)

- **IA-5** — Authenticator Management
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **AC-3** — Access Enforcement
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **2.5** — Allowlist Authorized Software
- **3.10** — Encrypt Sensitive Data in Transit
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1078	Valid Accounts	Defense-Evasion
T1562.001	Disable or Modify Tools	Defense-Evasion
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access

Technique ID	Technique Name	Tactic
T1553.002	Code Signing	Defense-Evasion
T1588.003	Code Signing Certificates	Resource-Development
T1195.002	Compromise Software Supply Chain	Initial-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1566.001	Spearphishing Attachment	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/microsoft-defender-w...	T3
Two DigiCert root certificates flagged as malware ■ Some ...	https://x.com/BleepinComputer/status/2051003642870980717	T3
■■ Microsoft Defender Mistakenly Flags DigiCert Root ...	https://x.com/The_Cyber_News/status/2050984065038422426/photo/1	T3
Defender Flags DigiCert Root Certificates	https://cybersecuritynews.com/defender-flags-digicert-root-certific...	T3
Windows Defender flagged our company digital certificate ...	https://learn.microsoft.com/en-us/answers/questions/5610417/windows...	T1

Generated 2026-05-04 06:06 UTC by TJS Security Command Center