INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 13:52 UTC

Gentlemen RaaS Operates Modular EDR-Killing Toolkit Targeting 48 Security Vendors with FortiGate Credential Exploitation

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0520
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	CrowdStrike Falcon, SentinelOne, Microsoft Defender, Palo Alto Cortex XDR, Sophos, Trend Micro, ESET, Bitdefender, McAfee/Trellix, Kaspersky, Fortinet FortiGate (VPN/SSL-VPN configurations exposed via FortiBleed; specific FortiOS versions not confirmed in available source material)
Published	2026-06-18T18:31:52
Discovery Source	Rss

Executive Summary

The Gentlemen ransomware-as-a-service group has built and is actively deploying GentleKiller, a modular toolkit designed to disable endpoint detection and response tools across 48 security vendors before executing ransomware or exfiltrating data. The group is targeting organizations with Fortinet FortiGate infrastructure, exploiting credentials exposed through the FortiBleed event, to gain initial access before neutralizing defenses. Organizations running FortiGate VPN alongside any major EDR platform face a two-stage attack path: credential-based entry followed by security tool removal, leaving them blind before encryption begins.

Technical Analysis

Gentlemen RaaS operates GentleKiller, a modular EDR-killing toolset reported to terminate over 400 processes associated with 48 security vendors, including CrowdStrike Falcon, SentinelOne, Microsoft Defender, Palo Alto Cortex XDR, Sophos, Trend Micro, ESET, Bitdefender, McAfee/Trellix, and Kaspersky. The toolkit targets defense evasion prior to payload execution, consistent with MITRE ATT&CK T1562.001 (Impair Defenses: Disable or Modify Tools). Initial access is linked to FortiGate VPN credential exploitation (T1133, T1078) intersecting with the FortiBleed credential exposure event; specific FortiOS versions affected by that exposure are not confirmed in available source material. Post-access activity involves process discovery (T1057),

command execution (T1059), and likely privilege escalation (T1068) to achieve the process termination required for EDR neutralization. The group cross-pollinates tools with at least three other ransomware operations, indicating tool-brokering within the RaaS ecosystem (T1588.002, T1195). Payload delivery results in data encryption (T1486) with exfiltration via proxy infrastructure (T1090.001) and application-layer C2 (T1071.001). Relevant CWEs: CWE-284 (Improper Access Control), CWE-506 (Embedded Malicious Code), CWE-269 (Improper Privilege Management). No CVE ID is associated with the GentleKiller toolkit itself. The FortiBleed credential exposure event is referenced as the source of initial access; specific CVE identifiers and affected FortiOS versions are not detailed in the available source material for this item. Source: BleepingComputer reporting (T3 news outlet). Vendor-specific advisories from affected security vendors (CrowdStrike, SentinelOne, Microsoft, Palo Alto Networks, Sophos, Trend Micro, ESET, Bitdefender, Trellix, Kaspersky) and Fortinet would strengthen attribution and technical detail if published. Confidence: Medium, reported by established security news outlet but lacks independent corroboration from affected vendors or primary threat intelligence sources.

Action Checklist

1. Step 1: Containment. Audit all FortiGate VPN and SSL-VPN accounts immediately. Rotate every credential that may have been exposed in the FortiBleed event. Disable or restrict external VPN access for accounts that cannot be verified clean. Apply NIST AC-2 (Account Management) procedures: review active accounts, suspend unrecognized sessions, and enforce AC-7 (Unsuccessful Logon Attempts) lockout thresholds.
2. Step 2: Detection. Query EDR and SIEM logs for mass process termination events targeting security tool executables, particularly sequences killing 5 or more security-vendor processes in under 60 seconds. Hunt for T1562.001 indicators: unexpected stops of EDR agent services, tampered driver signatures (T1553.002), and process hollowing patterns. Review FortiGate VPN authentication logs for logins from unusual geographies, off-hours access, or accounts that have not logged in recently. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication. Rotate all FortiGate VPN credentials organization-wide; do not limit rotation to accounts with confirmed suspicious activity. Re-enable and verify integrity of all EDR agents across endpoints, confirm agents are running and tamper-protection is active. Remove any unauthorized accounts or sessions identified in Step 2. Apply CIS 5.3 (Disable Dormant Accounts) and CIS 6.2 (Establish an Access Revoking Process) for any accounts flagged in the audit.
4. Step 4: Recovery. Verify EDR agent health and telemetry continuity on all endpoints before declaring recovery. Confirm FortiGate VPN authentication logs show no anomalous sessions post-rotation. Run a targeted threat hunt for T1486 (Data Encrypted for Impact) indicators and check backup integrity before resuming normal operations. Monitor for T1090.001 (proxy) and T1071.001 (application-layer C2) patterns in outbound traffic. Apply NIST AU-9 (Protection of Audit Information) to ensure log integrity was not tampered during any EDR-kill window.
5. Step 5: Post-Incident. Evaluate whether tamper protection was enabled on all EDR platforms before this event; GentleKiller's effectiveness depends partly on agents running without hardened tamper protection. Implement NIST AC-6 (Least Privilege) to limit which accounts and processes can interact with security agent services. Apply CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.4 (Require MFA for Remote Network Access) to all VPN entry points. Review tool-sharing risk in your supply chain context given the group's cross-RaaS tool brokering (T1195, T1588.002). Enforce NIST IA-2 (Authentication) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) as

standing policies for all remote access paths.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance counsel if any endpoint shows evidence of ransomware file encryption activity (T1486 indicators), if backup repositories are found inaccessible or modified, or if PII/PHI data stores were accessible from any VPN session associated with a FortiBleed-exposed credential — all of which trigger breach notification obligations under HIPAA, GDPR, or applicable state law.
Recovery Notes	Do not declare recovery until EDR telemetry is confirmed operational and generating events on 100% of in-scope endpoints — a single silent endpoint may indicate a GentleKiller-disabled agent masking active ransomware staging. Monitor FortiGate VPN authentication logs and outbound network traffic for a minimum of 14 days post-rotation, as Gentlemen RaaS affiliates have demonstrated patience in re-using previously established footholds or returning after initial eviction. Validate all backup restore points against pre-incident file hashes before resuming data-dependent production workloads, as the group's pre-ransomware exfiltration phase may have included backup interference.
Forensic Artifacts	FortiGate SSL-VPN authentication logs (log type=event, subtype=vpn) covering the full FortiBleed exposure window — these will show the specific accounts, source IPs, and session durations used by Gentlemen RaaS affiliates to gain initial access via the 74,000 exposed credentials | Windows Sysmon Event ID 5 (Process Terminate) and Event ID 6 (Driver Load) logs on all endpoints, capturing the GentleKiller mass-termination sequence targeting EDR vendor executables and any BYOVD driver artifacts loaded immediately prior to the security tool kill chain | Live memory acquisition (WinPmem/DumpIt output) from endpoints where EDR agents went silent — GentleKiller's process hollowing and in-memory execution techniques leave artifacts in process memory that are destroyed on reboot or process termination | Windows Registry export of 'HKLM\SYSTEM\CurrentControlSet\Services' and 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' from all affected hosts, capturing GentleKiller persistence mechanisms and any modified service ImagePath values pointing to malicious binaries | File system artifacts in %TEMP%, %APPDATA%, and C:\ProgramData with creation timestamps falling within the compromise window — GentleKiller's modular architecture stages components to disk before execution, and these directories are the primary drop locations for the toolkit's per-vendor kill modules

Per-Action IR Details

Step 1: Containment — Audit all FortiGate VPN and SSL-VPN accounts immediately. Rotate every credential that may have been exposed in the FortiBleed event. Disable or restrict external VPN access for accounts that cannot be verified clean. Apply NIST AC-2 (Account Management) procedures: review active accounts, suspend unrecognized sessions, and enforce AC-7 (Unsuccessful Logon Attempts) lockout thresholds.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate and limit damage from the identified threat vector before eradication begins

Controls: NIST AC-2 (Account Management), NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-12 (Session Termination), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export FortiGate VPN session and account data via CLI: 'get vpn ssl monitor' and 'get user local' to enumerate active SSL-VPN sessions and local accounts. Cross-reference against a known-good account list maintained in a spreadsheet or flat file. Terminate unrecognized sessions with 'diagnose vpn ssl del-tunnel' by index. A 2-person team can split account audit (person 1) and active session termination (person 2) in parallel. No SIEM required — raw FortiGate CLI output is sufficient.

Evidence: BEFORE revoking any sessions or rotating credentials, capture: (1) Full FortiGate SSL-VPN session table via 'diagnose vpn ssl monitor' — records active tunnel IDs, source IPs, user accounts, and session durations for all active connections; (2) FortiGate traffic logs and authentication logs from /var/log/log.dat or syslog forwarding target, filtering on VPN authentication events (log type=event, subtype=vpn) to identify accounts used during the FortiBleed exposure window; (3) FortiGate ARP table and routing table snapshot ('get router info routing-table all', 'diagnose ip arp list') to map any lateral movement from VPN-sourced IPs before session teardown.

Step 2: Detection — Query EDR and SIEM logs for mass process termination events targeting security tool executables, particularly sequences killing 5 or more security-vendor processes in under 60 seconds. Hunt for T1562.001 indicators: unexpected stops of EDR agent services, tampered driver signatures (T1553.002), and process hollowing patterns. Review FortiGate VPN authentication logs for logins from unusual geographies, off-hours access, or accounts that have not logged in recently. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate multi-source indicators to confirm GentleKiller deployment and determine scope of EDR neutralization across the environment

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM/EDR: Deploy Sysmon with a config that captures Event ID 1 (Process Create) and Event ID 5 (Process Terminate); filter for termination of known security vendor executables (CSFalconService.exe, SentinelAgent.exe, MsMpEng.exe, cyserver.exe, SAVAdminService.exe, etc.) within short time windows using PowerShell: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Id -eq 5} | Select-Object TimeCreated, Message | Export-Csv sysmon_term.csv'. For driver tampering, run 'sigcheck -vt -c drivers.csv C:\Windows\System32\drivers' (Sysinternals sigcheck) to flag unsigned or revoked-cert drivers loaded by GentleKiller modules. For FortiGate auth review, parse syslog output with grep: 'grep -i "ssl-vpn" /var/log/fortigate.log | awk "{print $1,$2,$5,$9}"' to surface anomalous logins.

Evidence: BEFORE any containment actions alter live state, capture: (1) Windows Security Event Log Event ID 7036 (Service Control Manager — service stopped) and Event ID 7045 (new service installed) on all endpoints, which GentleKiller triggers when terminating EDR agent services; (2) Sysmon Event ID 6 (Driver Load) entries showing any drivers loaded immediately prior to the security tool termination sequence — GentleKiller's BYOVD or driver-manipulation modules will appear here with anomalous timestamps or missing/invalid signatures; (3) Live memory acquisition (WinPmem or DumpIt) from any endpoint where security tools have gone silent, capturing GentleKiller's in-memory hollowing artifacts before process termination destroys them; (4) Active network connections snapshot ('Get-NetTCPConnection | Export-Csv netconn.csv') to identify C2 channels or lateral movement paths established during the EDR-blind window created by GentleKiller.

Step 3: Eradication — Rotate all FortiGate VPN credentials organization-wide; do not limit rotation to accounts with confirmed suspicious activity. Re-enable and verify integrity of all EDR agents across endpoints — confirm agents are running and tamper-protection is active. Remove any unauthorized accounts or sessions identified in Step 2. Apply CIS 5.3 (Disable Dormant Accounts) and CIS 6.2 (Establish an Access Revoking Process) for any accounts flagged in the audit.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all artifacts of compromise including FortiBleed-exposed credentials and GentleKiller persistence mechanisms before restoring normal operations

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking

Process)

Compensating: For credential rotation without an IdP automation tool: generate new random passwords for all FortiGate local VPN accounts using a password manager or PowerShell 'New-Guid' for uniqueness, update via FortiGate CLI 'config user local; edit ; set passwd ; end' for each account. For EDR integrity verification without a central management console: run a PowerShell script across endpoints using PSRemoting — 'Invoke-Command -ComputerName (Get-Content endpoints.txt) -ScriptBlock {Get-Service -Name "CSFalconService","SentinelAgent","WinDefend" | Select-Object Name,Status}' — and flag any stopped or missing services for manual reinstallation. Verify driver integrity post-reinstall with sigcheck.

Evidence: BEFORE rotating credentials and removing accounts, ensure the following volatile evidence is already captured from Step 2. Additionally, before re-enabling EDR agents, collect: (1) File system artifacts in GentleKiller's likely staging directories — %TEMP%, %APPDATA%, C:\ProgramData — looking for dropped executables, batch scripts, or DLLs with randomized names and recent creation timestamps matching the compromise window; (2) Registry persistence keys 'HKLM\SYSTEM\CurrentControlSet\Services' for any newly registered services or modified existing service ImagePath values pointing to GentleKiller components; (3) Windows Event Log Event ID 4720 (account created) and 4726 (account deleted) to document all unauthorized account activity before those accounts are removed, preserving forensic chain of custody.

Step 4: Recovery — Verify EDR agent health and telemetry continuity on all endpoints before declaring recovery. Confirm FortiGate VPN authentication logs show no anomalous sessions post-rotation. Run a targeted threat hunt for T1486 (Data Encrypted for Impact) indicators and check backup integrity before resuming normal operations. Monitor for T1090.001 (proxy) and T1071.001 (application-layer C2) patterns in outbound traffic. Apply NIST AU-9 (Protection of Audit Information) to ensure log integrity was not tampered during any EDR-kill window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to verified clean state and confirm defensive telemetry is operational before resuming production, with heightened monitoring for Gentlemen RaaS re-entry or ransomware stage execution

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs)

Compensating: For EDR health verification without a central console: run the PSRemoting script from Step 3 again post-reinstall and compare output against a baseline service list. For ransomware indicator hunting without EDR: use YARA rules targeting known ransomware file-header patterns and extension changelists against file shares — 'yara -r ransom_rules.yar /mnt/fileshare'. Check backup integrity by performing a test restore of a non-critical file from the most recent backup snapshot and verifying hash matches pre-compromise hashes where available. For outbound C2 detection: capture 30 minutes of outbound traffic on the network perimeter with Wireshark filtering on non-standard ports and high-entropy DNS queries ('tshark -i eth0 -f "port not 80 and port not 443" -w outbound_suspect.pcap').

Evidence: Before declaring recovery complete, capture and retain: (1) FortiGate VPN authentication logs post-rotation (minimum 72 hours) filtered for any authentication success events — any successful login post-rotation using a previously FortiBleed-exposed account pattern warrants immediate re-containment; (2) File system change journal (USN Journal — 'fsutil usn readjournal C: csv > usn_journal.csv') on file servers and critical hosts to identify any file encryption activity that may have occurred during the EDR-blind window, evidenced by mass rename events with unfamiliar extensions; (3) Backup catalog integrity hashes compared against pre-incident baseline to confirm Gentlemen RaaS did not pre-stage backup deletion or encryption prior to main ransomware detonation.

Step 5: Post-Incident — Evaluate whether tamper protection was enabled on all EDR platforms before this event; GentleKiller's effectiveness depends partly on agents running without hardened tamper protection. Implement NIST AC-6 (Least Privilege) to limit which accounts and processes can interact with security agent services. Apply CIS 6.3 and CIS 6.4 (Require MFA for Externally-Exposed Applications and Remote Network Access) to all VPN entry points. Review tool-sharing risk in your supply chain context given the group's cross-RaaS tool brokering (T1195, T1588.002). Enforce D3-MFA (Multi-factor Authentication) on all remote access paths and D3-CRO (Credential Rotation) as a standing policy.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned specific to GentleKiller's EDR-kill capability and FortiBleed credential exposure, and implement structural controls to prevent Gentlemen RaaS re-entry

Controls: NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without enterprise MDM to enforce tamper protection centrally: document and manually verify tamper-protection status on each EDR platform via its local agent UI or CLI equivalent (e.g., CrowdStrike: 'falconctl -g --tamper-protection'; SentinelOne: agent console tamper-protection flag). For MFA on FortiGate VPN without a commercial IdP: configure FortiGate's built-in TOTP two-factor authentication using FortiToken Mobile (free tier available) or integrate with a self-hosted FreeRADIUS server paired with Google Authenticator. For least-privilege enforcement on EDR service accounts: use 'sc sdset ' on Windows to restrict which accounts can stop or modify the EDR service, preventing GentleKiller from using standard user context to terminate agents.

Evidence: For the post-incident review, compile and preserve as long-term forensic record: (1) The complete timeline of EDR service stop events (Windows Event ID 7036) correlated against FortiGate VPN authentication timestamps to reconstruct the precise sequence from FortiBleed credential use to GentleKiller deployment; (2) Any GentleKiller binary samples or script artifacts recovered from endpoint staging directories — submit to an internal YARA rule library and share hashes via your threat intel sharing community (ISACs) to support cross-organizational detection; (3) FortiGate configuration backup (pre- and post-incident) to document what access policies were in place at time of exploitation and confirm hardening changes are captured in change management records.

Detection Guidance

Primary detection focus: EDR process termination at scale and FortiGate VPN anomalies. In your SIEM, alert on sequences where 5 or more security vendor processes (match against your installed EDR/AV executable names) are stopped or killed within a 60-second window on a single host; this pattern is a strong GentleKiller behavioral indicator aligned with T1562.001. Query Windows Security Event Log for Event ID 7036 (service stopped) or 7045 (new service installed) against a watchlist of EDR agent service names. For FortiGate: review VPN authentication logs for accounts active during the FortiBleed exposure window that have logged in from new IP ranges, new countries, or during off-hours; cross-reference against your account inventory per CIS 5.1. Hunt for T1068 privilege escalation indicators: unexpected token impersonation, LSASS access, or driver loading events preceding EDR service stops. Check for T1553.002 indicators: unsigned or revoked driver loads, which are a common EDR-kill mechanism. For network-layer detection, flag outbound connections to Tor exit nodes or known proxy infrastructure (T1090.001). Apply NIST SI-4 equivalent monitoring (if mapped in your environment) for real-time alerting on security tool tampering. Behavioral detection patterns are the primary method until vendor-published IOCs become available. Check CrowdStrike, SentinelOne, Microsoft, Palo Alto Networks, and other affected vendors' threat intelligence feeds for published indicators of compromise (IOCs) related to GentleKiller or Gentlemen RaaS.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/gentlemen-ransomware-uses-multiple-edr-killers-to-disable-defenses/`	Primary source reporting on GentleKiller toolkit and Gentlemen RaaS operations — review for any IOCs published in the full article	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1562.001** — Disable or Modify Tools
- **T1071.001** — Web Protocols
- **T1588.002** — Tool
- **T1486** — Data Encrypted for Impact
- **T1133** — External Remote Services
- **T1059** — Command and Scripting Interpreter
- **T1057** — Process Discovery
- **T1068** — Exploitation for Privilege Escalation
- **T1555** — Credentials from Password Stores
- **T1090.001** — Internal Proxy
- **T1078** — Valid Accounts
- **T1195** — Supply Chain Compromise
- **T1553.002** — Code Signing

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SI-2** — Flaw Remediation
- **AC-2** — Account Management
- **SA-9** — External System Services

- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1562.001	Disable or Modify Tools	Defense-Evasion
T1071.001	Web Protocols	Command-And-Control
T1588.002	Tool	Resource-Development
T1486	Data Encrypted for Impact	Impact
T1133	External Remote Services	Persistence
T1059	Command and Scripting Interpreter	Execution
T1057	Process Discovery	Discovery
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1555	Credentials from Password Stores	Credential-Access
T1090.001	Internal Proxy	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1195	Supply Chain Compromise	Initial-Access
T1553.002	Code Signing	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/gentlemen-ransomware...	T3
Endpoint security market trends and key players - Facebook	https://www.facebook.com/groups/hacking101/posts/2538557046544198/	T3
Best Endpoint Protection Platforms (Transitioning to ... - Gartner	https://www.gartner.com/reviews/market/endpoint-protection-platforms	T2
Top 7 Endpoint Protection Solutions for 2026 - SentinelOne	https://www.sentinelone.com/cybersecurity-101/endpoint-security/end...	T3
Top Endpoint Protection Vendors - Cloudtango	https://www.cloudtango.net/cybersec/endpoint-protection/	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-19 13:52 UTC by TJS Security Command Center