INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 18:59 UTC

GentleKiller Framework: The Gentlemen RaaS Deploys Centralized EDR Destruction Targeting 400 Processes Across 48 Security Products

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0522
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Security Products: CrowdStrike Falcon, Kaspersky, FACEIT Anti-Cheat, Valorant Anti-Cheat, Javelin, WatchDog, BeyondTrust Remote Support; Browsers: Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Opera, Vivaldi; UEFI/Secure Boot (8 vendors): Acer, AMD, ASUS, ECS, Getac, GIGABYTE, Toshiba, Uniwill, 48 total security products, 400 targeted processes
Published	2026-06-19T14:33:07
Discovery Source	Rss

Executive Summary

The Gentlemen ransomware-as-a-service group has deployed GentleKiller, a framework that disables endpoint detection and response tools at the kernel level before launching ransomware encryption. The framework targets 400 processes across 48 security products, including CrowdStrike Falcon, Kaspersky, and BeyondTrust Remote Support, and has been linked to 504 confirmed victims since March 2025 across Southeast Asia, South America, and Western Europe. Related UEFI/Secure Boot vulnerabilities affecting eight major hardware vendors expand the pre-OS attack surface, meaning organizations face a layered threat capable of neutralizing endpoint protection before security tooling even initializes.

Technical Analysis

GentleKiller employs Bring Your Own Vulnerable Driver (BYOVD) techniques, loading signed but vulnerable kernel drivers to achieve ring-0 execution and terminate protected security processes. The framework targets approximately 400 processes across 48 products including CrowdStrike Falcon, Kaspersky, FACEIT Anti-Cheat, Valorant Anti-Cheat, Javelin, WatchDog, BeyondTrust Remote Support, and major browsers (Chrome, Edge, Firefox, Brave, Opera, Vivaldi). BYOVD execution maps to MITRE T1068 (Exploitation for Privilege Escalation) and T1562.001 (Impair Defenses: Disable or Modify Tools). Ransomware deployment follows via T1486 (Data

Encrypted for Impact). Related CERT/CC-disclosed Secure Boot bypass vulnerabilities affect UEFI applications from Acer, AMD, ASUS, ECS, Getac, GIGABYTE, Toshiba, and Uniwill (T1542.003, T1553.002), enabling pre-OS persistence before security tooling initializes. Additional techniques include T1072 (Software Deployment Tools), T1195 (Supply Chain Compromise), T1555.003 (Credentials from Web Browsers), T1036.005 (Masquerading: Match Legitimate Name or Location), T1588.002 (Obtain Capabilities: Tool), T1078 (Valid Accounts), T1547.001 (Registry Run Keys / Startup Folder), T1588.006 (Obtain Capabilities: Vulnerabilities), and T1211 (Exploitation for Defense Evasion). CWE mapping: CWE-494 (Download of Code Without Integrity Check, vulnerable driver loading), CWE-269 (Improper Privilege Management, kernel-level escalation), CWE-693 (Protection Mechanism Failure, EDR bypass). No CVE identifier is associated with the GentleKiller campaign itself. UEFI/Secure Boot CVEs are tracked separately under CERT/CC disclosure. No vendor-issued patch specific to GentleKiller framework exists; mitigation relies on driver blocklisting, UEFI firmware updates, and detection engineering.

Action Checklist

1. Step 1: Containment. Immediately audit kernel driver load events across all endpoints; block known vulnerable driver hashes associated with BYOVD campaigns using your EDR's driver blocklist or the Microsoft Vulnerable Driver Blocklist policy (https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules). Isolate any host showing unexpected kernel driver loads or mass process termination events coinciding with security tool process deaths. For systems with affected UEFI vendors (Acer, AMD, ASUS, ECS, Getac, GIGABYTE, Toshiba, Uniwill), restrict physical and remote administrative access until firmware updates are applied.
2. Step 2: Detection. Query endpoint telemetry for T1562.001 indicators: sudden termination of security product processes (CrowdStrike, Kaspersky, BeyondTrust agent) not initiated by authorized administrators. Monitor Windows Event Log for kernel driver load events (Sysmon Event ID 6, or equivalent driver load telemetry). Flag any driver load where the signing certificate is valid but the driver appears on known BYOVD lists (https://www.loldrivers.io/). Search for T1068 patterns: processes spawning with SYSTEM-level privileges from unusual parent processes. Review UEFI Secure Boot status via firmware management tools, flag any system where Secure Boot is disabled or reports policy override. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for review cadence requirements.
3. Step 3: Eradication. Deploy updated UEFI firmware from all eight affected vendors (Acer, AMD, ASUS, ECS, Getac, GIGABYTE, Toshiba, Uniwill) per each vendor's security advisory addressing the CERT/CC-disclosed Secure Boot bypass. Enable and enforce the Microsoft Vulnerable Driver Blocklist (WDAC policy: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview) to prevent future BYOVD driver loads. Rotate credentials for any accounts active on compromised or suspect hosts per NIST AC-2 (Account Management). Remove any unauthorized drivers or scheduled tasks added via T1547.001. If ransomware payload executed, do not pay (per FBI and CISA guidance: https://www.cisa.gov/ransomware); restore from verified offline backups.
4. Step 4: Recovery. After firmware updates, validate Secure Boot re-enrollment and confirm policy enforcement via firmware audit logs. Verify all targeted security products (CrowdStrike Falcon, Kaspersky, BeyondTrust, etc.) are running and their self-protection mechanisms are active. Re-baseline kernel driver inventory per CIS 2.1 (Address Unauthorized Software), document all approved drivers and flag deviations. Monitor for T1078 (Valid Accounts) abuse in the 30 days post-remediation, as the group uses credential theft (T1555.003) that may yield persistent access independent of the BYOVD chain.

5. Step 5: Post-Incident. Review whether driver allowlisting (WDAC or equivalent) was enforced prior to this campaign; if not, implement it as a standing control. Assess whether UEFI firmware update cadence was included in your vulnerability management program per CIS 7.3 (Perform Automated Operating System Patch Management); UEFI firmware is frequently omitted. Evaluate EDR self-protection capabilities against kernel-level termination and request vendor documentation on anti-tamper mechanisms. Map control gaps to NIST SI-4 (System Monitoring and Information System Monitoring) and document residual risk. Conduct a tabletop exercise against the T1562.001 + BYOVD kill chain to validate detection and response playbooks.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal counsel if any host confirms ransomware encryption activity, if Secure Boot is disabled on systems processing PII or regulated data (triggering breach notification assessment under GDPR, HIPAA, or applicable state law), or if the IR team lacks capability to perform kernel-level memory forensics or UEFI firmware analysis — engage a specialist DFIR retainer.
Recovery Notes	Before returning any host to production, confirm three conditions in sequence: (1) UEFI firmware updated and Secure Boot re-enrolled with vendor-provided DBX update, validated via `Confirm-SecureBootUEFI`; (2) all targeted security products (CrowdStrike Falcon, Kaspersky, BeyondTrust) are running with self-protection active and confirmed via service state query; (3) WDAC vulnerable driver blocklist policy is enforced in block mode, not audit mode. Maintain elevated monitoring for 30 days post-recovery specifically for credential-based re-entry (Windows Security Event IDs 4624, 4648, 4720) given the Gentlemen group's concurrent browser credential theft targeting Chrome, Edge, Firefox, Brave, Opera, and Vivaldi credential stores on compromised hosts, which may provide persistent access independent of the BYOVD chain.
Forensic Artifacts	Kernel driver load records — Windows System Event ID 7045 (new driver/service installed) and Sysmon Event ID 6 (Driver Loaded) logs capturing the BYOVD driver name, file path, signing certificate thumbprint, and load timestamp; these are the primary forensic trace of GentleKiller's kernel-level EDR kill mechanism | Security product process termination records — Windows Security Event ID 4689 (Process Terminated) filtered on falcon-sensor.exe, csagent.exe, avp.exe, kavtray.exe, and BeyondTrust Remote Support agent process names; timestamps correlated against driver load events prove the GentleKiller kill-chain sequence | Browser credential store SQLite files — Chrome, Edge, Brave, Opera, and Vivaldi `Login Data` files (located at `%LOCALAPPDATA%\\User Data\Default\Login Data`) and Firefox `logins.json` (at `%APPDATA%\Mozilla\Firefox\Profiles\*.default\logins.json`) — the Gentlemen group targets these for credential harvesting concurrent with EDR destruction | UEFI/Secure Boot policy state — firmware audit logs and output of `Confirm-SecureBootUEFI`, `Get-SecureBootPolicy`, and `msinfo32` Secure Boot State field captured pre-remediation; DBX (forbidden signature database) contents exportable via PowerShell `Get-SecureBootUEFI -Name dbx` document whether the CERT/CC-disclosed Secure Boot bypass was leveraged to load GentleKiller's unsigned or revoked driver | Registry driver persistence keys — export of `HKLM\SYSTEM\CurrentControlSet\Services` showing any driver registered as a kernel-mode service with a start type of 1 (system) or 0 (boot) that does not match the approved driver baseline; GentleKiller's BYOVD driver will appear here if it established persistence beyond a single-session load

Per-Action IR Details

Step 1: Containment — Immediately audit kernel driver load events across all endpoints; block known vulnerable driver hashes associated with BYOVD campaigns using your EDR's driver blocklist or the Microsoft Vulnerable Driver Blocklist policy. Isolate any host showing unexpected kernel driver loads or mass process termination events coinciding with security tool process deaths. For systems with affected UEFI vendors (Acer, AMD, ASUS, ECS, Getac, GIGABYTE, Toshiba, Uniwill), restrict physical and remote administrative access until firmware updates are applied.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and prevent threat propagation before eradication actions are taken

Controls: NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Without enterprise EDR, use PowerShell to enumerate loaded kernel drivers on each host: `Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7045}` (new service/driver installs) and cross-reference against Microsoft's known vulnerable driver blocklist CSV (available at microsoft.com/security). For hosts with affected UEFI vendors, disable remote management interfaces (RDP, WinRM, iLO/BMC) via local firewall rules: `netsh advfirewall firewall add rule name='Block RDP' dir=in action=block protocol=TCP localport=3389`. Use Sysmon Event ID 6 (Driver Loaded) on any host where Sysmon is deployed to identify unsigned or known-bad driver loads immediately.

Evidence: BEFORE isolating any host, capture the following volatile state: (1) Full RAM image using WinPmem or DumpIt — GentleKiller operates at kernel level and in-memory driver artifacts will be destroyed on shutdown or isolation. (2) Enumerate all loaded kernel drivers: `driverquery /v /fo csv > drivers_snapshot.csv` and `Get-WinEvent -LogName System -Id 7045 | Export-Csv driver_installs.csv`. (3) Active network connections: `netstat -ano > netstat_snapshot.txt` — GentleKiller's C2 beacon or ransomware staging traffic may be live. (4) Running process tree: `tasklist /v /fo csv > process_snapshot.csv` — capture before any process termination to document which security tool processes (falcon-sensor.exe, kavtray.exe, BeyondTrust agents) are already dead. (5) Sysmon Event ID 6 logs from `Microsoft-Windows-Sysmon/Operational` channel before log rotation or tampering destroys them.

Step 2: Detection — Query endpoint telemetry for T1562.001 indicators: sudden termination of security product processes (CrowdStrike, Kaspersky, BeyondTrust agent) not initiated by authorized administrators. Monitor Windows Event Log for kernel driver load events (Event ID 6 in Sysmon, or equivalent driver load telemetry). Flag any driver load where the signing certificate is valid but the driver appears on known BYOVD lists. Search for T1068 patterns: processes spawning with SYSTEM-level privileges from unusual parent processes. Review UEFI Secure Boot status via firmware management tools — flag any system where Secure Boot is disabled or reports policy override. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for review cadence requirements.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across log sources to confirm incident scope and characterize the GentleKiller BYOVD kill chain

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, run the following on each suspect host: (1) Sysmon Event ID 6 query for driver loads with invalid or allowlisted-but-vulnerable signatures: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 6} | Select-Object TimeCreated, Message | Export-Csv sysmon_drivers.csv`. (2) Check for sudden security process deaths in Windows Security Event Log: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4689 -and $_.Message -match 'falcon|kaspersky|beyondtrust'} | Export-Csv process_terminations.csv`. (3) Query Secure Boot status: `Confirm-SecureBootUEFI` (returns True/False) — run across all hosts via PSRemoting if available. (4) Deploy the free Sigma rule for BYOVD patterns (available in the SigmaHQ GitHub repo under `windows/driver`) converted to

PowerShell or Winlogbeat queries.

Evidence: Volatile evidence to capture concurrent with (not after) detection queries: (1) Windows System Event Log — Event ID 7045 (new kernel-mode driver installed) and Event ID 7036 (service state changes) covering the window when CrowdStrike Falcon sensor (CSFalconService), Kaspersky (AVP.EXE), or BeyondTrust agent processes went offline. (2) Sysmon Event ID 1 (Process Create) logs showing parent-child chains where an unexpected process spawned with SYSTEM privileges — GentleKiller's privilege escalation via BYOVD will produce anomalous parent process relationships. (3) UEFI/firmware event logs accessible via `Get-WinEvent -LogName 'Microsoft-Windows-Kernel-Boot'` — flag Secure Boot policy changes or DBX (forbidden signature database) modifications. (4) Windows Security Event ID 4688 (Process Creation) filtered on process names matching GentleKiller's 400-process target list, particularly falcon-sensor.exe, avp.exe, and BeyondTrust Remote Support agent executables.

Step 3: Eradication — Deploy updated UEFI firmware from all eight affected vendors (Acer, AMD, ASUS, ECS, Getac, GIGABYTE, Toshiba, Uniwill) per each vendor's security advisory addressing the CERT/CC-disclosed Secure Boot bypass. Enable and enforce the Microsoft Vulnerable Driver Blocklist (WDAC policy) via PowerShell to prevent future BYOVD driver loads. Rotate credentials for any accounts active on compromised or suspect hosts per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation). Remove any unauthorized drivers or scheduled tasks added via T1547.001. If ransomware payload executed, do not pay — restore from verified offline backups.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all threat components (malicious drivers, persistence mechanisms, compromised firmware policy) and close the BYOVD and Secure Boot bypass vectors before recovery begins

Controls: NIST AC-2 (Account Management), NIST CM-7 (Least Functionality — implied via WDAC allowlisting; note: CM-7 is cited from knowledge base general family context), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: For teams without automated patch management: (1) Download UEFI firmware updates directly from each affected vendor's security advisory page (verify SHA-256 hash of firmware image before flashing). (2) Apply WDAC vulnerable driver blocklist manually via: `Set-CIPolicy` or by importing Microsoft's pre-built WDAC base policy XML from the Windows Security GitHub repo. (3) Credential rotation without a PAM tool: use `net user /domain` for domain accounts or local `net user` for workstations — prioritize accounts that had interactive sessions on isolated hosts per Windows Security Event ID 4624 logon records. (4) Enumerate and remove unauthorized scheduled tasks: `Get-ScheduledTask | Where-Object {$_.TaskPath -notlike '\Microsoft\*'} | Export-Csv suspicious_tasks.csv` — manually review and delete any added by GentleKiller's persistence mechanism.

Evidence: BEFORE rotating credentials, patching firmware, or removing drivers, capture: (1) Full memory image (WinPmem/DumpIt) — kernel-resident GentleKiller driver code and decrypted configuration may only exist in RAM. (2) Export all currently loaded drivers with hashes: `Get-WinEvent -LogName System -Id 7045 | Format-List` plus `sigcheck -vt -nobanner C:\Windows\System32\drivers\*.sys` (Sysinternals sigcheck) to capture signing metadata of suspect drivers before removal. (3) Registry export of driver persistence keys: `reg export HKLM\SYSTEM\CurrentControlSet\Services drivers_registry.reg` — GentleKiller may register BYOVD drivers as services. (4) Scheduled task XML export: `schtasks /query /fo xml /v > all_tasks.xml`. (5) List of accounts with active sessions at time of compromise from Windows Security Event ID 4624 and 4634 — required to scope credential rotation to all exposed accounts, not just admin accounts.

Step 4: Recovery — After firmware updates, validate Secure Boot re-enrollment and confirm policy enforcement via firmware audit logs. Verify all targeted security products (CrowdStrike Falcon, Kaspersky, BeyondTrust, etc.) are running and their self-protection mechanisms are active. Re-baseline kernel driver inventory per CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — document all approved drivers and flag deviations. Monitor for T1078 (Valid Accounts) abuse in the 30 days post-remediation, as the group uses credential theft (T1555.003) that may yield persistent access independent of the BYOVD chain.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to verified-clean state, confirm security control integrity, and establish enhanced monitoring for Gentlemen group re-entry via stolen credentials

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without enterprise firmware management tooling: (1) Validate Secure Boot status post-firmware update on each affected host: `Confirm-SecureBootUEFI` — must return True; document results per host. (2) Confirm CrowdStrike Falcon sensor is running and tamper-protected: check `sc query csagent` and `sc query csfalconservice` — both must show RUNNING state. For Kaspersky, check `sc query AVP`. For BeyondTrust, verify the Remote Support agent service is active via `sc query`. (3) Build a kernel driver allowlist baseline using: `driverquery /v /fo csv > approved_drivers_baseline.csv` — store offline and diff against future snapshots weekly using a simple PowerShell comparison script. (4) Monitor for credential abuse post-remediation by alerting on Windows Security Event ID 4625 (failed logon) spikes and Event ID 4648 (logon using explicit credentials) from unexpected source hosts.

Evidence: During recovery validation, capture and retain: (1) Firmware audit log export confirming Secure Boot DBX update and policy re-enrollment timestamp — retain as compliance evidence. (2) Service state snapshots for all 48 targeted security products confirming restoration: `Get-Service | Where-Object {$_.Name -match 'csagent|csfalcon|AVP|bomgar'} | Export-Csv security_services_restored.csv`. (3) Approved driver baseline CSV (see compensating above) — this becomes the forensic reference for future anomaly detection against GentleKiller re-deployment. (4) Windows Security Event logs for the 30-day post-remediation monitoring window, specifically Event IDs 4624, 4625, 4648, and 4720 (account creation) — the Gentlemen group's credential theft via browser credential stores (Chrome, Edge, Firefox, Brave, Opera, Vivaldi Login Data SQLite files) may enable re-entry independent of the BYOVD chain.

Step 5: Post-Incident — Review whether driver allowlisting (WDAC or equivalent) was enforced prior to this campaign; if not, implement it as a standing control. Assess whether UEFI firmware update cadence was included in your vulnerability management program per CIS 7.3 (Perform Automated Operating System Patch Management) — UEFI firmware is frequently omitted. Evaluate EDR self-protection capabilities against kernel-level termination and request vendor documentation on anti-tamper mechanisms. Map control gaps to NIST SI-4 (no mapped control — SI-4 is outside the provided knowledge base reference) and document residual risk. Conduct a tabletop exercise against the T1562.001 + BYOVD kill chain to validate detection and response playbooks.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned review, control gap analysis, and detection/playbook improvement driven by the GentleKiller campaign's exploitation of missing driver allowlisting and UEFI firmware management gaps

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Without a formal GRC platform for gap tracking: (1) Document the WDAC allowlisting gap in a plain-text risk register with remediation owner and target date — use Microsoft's WDAC Wizard (free, GUI-based) to build an initial allowlist policy scoped to approved kernel drivers. (2) Add UEFI firmware to your patch tracking spreadsheet as a distinct asset category — create a quarterly manual check process: download firmware versions from each of the eight affected vendor advisory pages and compare against installed versions via `Get-WmiObject -Class Win32_BIOS`. (3) Request anti-tamper documentation from CrowdStrike, Kaspersky, and BeyondTrust vendor portals — specifically ask whether kernel-level process termination by a BYOVD driver can bypass their self-protection. (4) Run the tabletop using the CERT/CC Secure Boot bypass scenario as the threat model, with Sysmon Event ID 6 and Windows Event ID 7045 as the primary detection tripwires.

Evidence: Post-incident documentation to retain as institutional memory and audit evidence: (1) Lessons-learned report capturing which of the 48 targeted security products were confirmed killed by GentleKiller on affected hosts — this scopes vendor anti-tamper improvement requests. (2) WDAC policy baseline XML and enforcement audit log

showing pre- vs. post-incident driver allowlist state — demonstrates control implementation timeline. (3) UEFI firmware version inventory (pre- and post-patch) for all eight affected vendor systems — serves as evidence of remediation completeness for any regulatory inquiry. (4) Tabletop exercise after-action report mapping gaps in detection of Sysmon Event ID 6 (driver load) and Event ID 4689 (process termination) for CrowdStrike Falcon, Kaspersky, and BeyondTrust processes — feeds directly into Sysmon configuration tuning and Sigma rule updates. (5) Browser credential store audit — enumerate presence of Chrome `Login Data`, Edge `Login Data`, Firefox `logins.json`, Brave `Login Data`, Opera `Login Data`, and Vivaldi `Login Data` SQLite files on compromised hosts to assess scope of credential exposure from T1555.003 activity.

Detection Guidance

Primary detection focus is on kernel driver load events and security process termination sequences. In Sysmon, monitor Event ID 6 (Driver Loaded) for drivers not on your approved baseline, cross-reference against published BYOVD vulnerable driver hash lists (Microsoft, https://www.loldrivers.io/). Alert on any event sequence where multiple security product processes (CrowdStrike, Kaspersky, BeyondTrust agent, browser security components) terminate within a short window without an authorized change ticket. In Windows Security Event Log, monitor Event ID 7045 (new service installed) and 4697 (service installed in system) for unexpected kernel-mode services. For UEFI/Secure Boot bypass indicators, query firmware management tooling for Secure Boot state changes or policy overrides, log these as high-priority events per NIST AU-2 (Event Logging) and NIST AU-12 (Audit Record Generation). Behavioral indicators for T1555.003 (browser credential theft): unexpected access to browser profile directories (AppData\Local\Google\Chrome\User Data, equivalent paths for Edge, Firefox, Brave, Opera, Vivaldi) by non-browser processes. For T1547.001 persistence: audit Run/RunOnce registry keys and startup folders for entries added outside change management windows. Network-level: monitor for unexpected outbound connections from hosts immediately following security tool termination events, this pattern indicates the pre-encryption staging phase.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`not available in source material`	No IOC values were provided in the source data; do not fabricate	LOW

Framework Mappings

MITRE-ATTACK

- **T1562.001** — Disable or Modify Tools
- **T1068** — Exploitation for Privilege Escalation
- **T1486** — Data Encrypted for Impact
- **T1072** — Software Deployment Tools
- **T1195** — Supply Chain Compromise
- **T1555.003** — Credentials from Web Browsers
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1542.003** — Bootkit

- **T1553.002** — Code Signing
- **T1588.002** — Tool
- **T1078** — Valid Accounts
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1588.006** — Vulnerabilities
- **T1211** — Exploitation for Defense Evasion

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-3** — Configuration Change Control
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

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

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1562.001	Disable or Modify Tools	Defense-Evasion
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1486	Data Encrypted for Impact	Impact
T1072	Software Deployment Tools	Execution
T1195	Supply Chain Compromise	Initial-Access
T1555.003	Credentials from Web Browsers	Credential-Access
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1542.003	Bootkit	Persistence
T1553.002	Code Signing	Defense-Evasion
T1588.002	Tool	Resource-Development
T1078	Valid Accounts	Defense-Evasion
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1588.006	Vulnerabilities	Resource-Development
T1211	Exploitation for Defense Evasion	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/the-gentlemen-raas-uses-gentlekil...	T3

Source	URL	Tier
FACEIT Anti-cheat - Secure boot requirement update! - Reddit	https://www.reddit.com/r/BattleBitRemastered/comments/1454ave/facei...	T3
Get easy to manage and affordable antivirus - CrowdStrike	https://www.crowdstrike.com/en-us/nab/	T3
Platforms - BeyondTrust	https://www.beyondtrust.com/products/remote-support/features/platforms	T3
Falcon Secure Access: Secure Every User on Every Device - YouTube	https://www.youtube.com/watch?v=_CH7SbhxUAY	T3

Generated 2026-06-19 18:59 UTC by TJS Security Command Center