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

AI-Powered Crime Tools Drive 389% Surge in Ransomware Victims, Reaching 7,831 in 2025

SECURITY ANALYSIS | HIGH

SCC Item ID	SCC-STY-2026-0107
Type	Security Analysis
Severity	HIGH
Affected Products	Global organizations across multiple sectors; no single product affected, enterprise networks broadly
Published	2026-05-02
Discovery Source	Gemini

Executive Summary

Ransomware victims surged to an estimated 7,831 globally in 2025, a reported 389% year-over-year increase, driven by AI-powered criminal tools that lower the technical bar for conducting sophisticated attacks at scale. Tools such as WormGPT and FraudGPT enable threat actors with limited expertise to craft convincing phishing campaigns and deploy ransomware, while critical vulnerabilities are now reportedly exploited within 24 to 48 hours of public disclosure. This shift signals a structural change in the threat landscape: volume, speed, and accessibility of attacks are increasing simultaneously, compressing the window organizations have to detect, patch, and respond.

Technical Analysis

The reported increase in ransomware victims reflects two converging trends documented in FortiGuard Labs research and corroborated by broader industry reporting. First, the commoditization of AI-assisted criminal tooling, specifically WormGPT and FraudGPT, removes the social engineering skill ceiling that previously limited ransomware affiliate recruitment. These tools generate convincing spear-phishing lures (MITRE T1566), automate credential harvesting campaigns, and assist in customizing malware payloads (T1587.001) and acquiring off-the-shelf malicious toolkits (T1588.001), enabling lower-skilled operators to execute campaigns that previously required experienced threat actors.

Second, time-to-exploit compression is accelerating the initial access phase. The reported 24-to-48-hour window between vulnerability disclosure and active exploitation (T1190) means that patch cycles calibrated to weekly or monthly cadences are structurally inadequate for critical-severity flaws in internet-facing systems. Once initial access is established, ransomware deployment via encryption (T1486) follows established playbooks that many organizations still lack mature detection coverage for.

The source data carries a medium confidence rating on specific statistics. The 389% increase and 7,831 victim count originate from a FortiGuard Labs report referenced through secondary discovery; the primary FortiGuard publication has not been independently verified in this session. The directional trend, however, is consistent with Microsoft's February 2025 sector targeting report (governments ranked top-three targeted globally) and the World Economic Forum Global Cybersecurity Outlook 2026, which identifies AI-enabled threat scaling as a primary systemic risk. Security teams should treat the specific figures as indicative rather than confirmed until verified against the primary FortiGuard source.

Defensive gaps most directly exploited in this threat pattern include: immature vulnerability prioritization processes that do not account for time-to-exploit velocity; insufficient email filtering and user awareness controls against AI-generated phishing; and incomplete EDR coverage that misses ransomware staging behavior before encryption executes. Sectors with historically high targeting rates, including government, healthcare, finance, and education, face amplified exposure given the volume increase.

Action Checklist

1. Step 1: Assess exposure, audit internet-facing assets for unpatched critical and high-severity vulnerabilities disclosed within the last 30 days; prioritize any with known public exploits given the reported 24-to-48-hour time-to-exploit window
2. Step 2: Review controls, verify email gateway filtering efficacy against AI-generated phishing content; confirm MFA enrollment across all privileged and remote-access accounts; validate EDR telemetry coverage for ransomware staging behaviors including volume shadow copy deletion and bulk file encryption activity
3. Step 3: Update threat model, add AI-assisted phishing (T1566), rapid vulnerability exploitation (T1190), and ransomware-as-a-service affiliate models using WormGPT/FraudGPT tooling to your threat register; update likelihood ratings for social engineering scenarios
4. Step 4: Communicate findings, brief leadership on the volume increase and time-to-exploit compression with specific relevance to your sector; frame the risk as a capacity and speed problem, not solely a technology gap
5. Step 5: Monitor developments, verify the specific FortiGuard Labs report statistics by consulting the primary FortiGuard Labs 2025 Ransomware Report; cross-reference with CISA's Known Exploited Vulnerabilities catalog and sector-specific advisories for rapid exploitation patterns consistent with the time-to-exploit compression described

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate to active incident response if: (1) perimeter log review reveals exploitation attempts against a KEV-listed vulnerability on an internet-facing asset within the 24-48 hour post-disclosure window; (2) Sysmon or Windows Security Event Log shows vssadmin.exe or wmic.exe invoking shadow copy deletion (Event ID 1, process ancestry from a web service or Office application); (3) MFA enrollment audit reveals privileged or remote-access accounts without MFA that have authenticated from external IPs in the last 72 hours; or (4) email gateway logs show a phishing campaign with click-through by a privileged user — any of these conditions shifts the engagement from preparation to active containment under NIST IR-4 (Incident Handling) with immediate notification to leadership per NIST IR-6 (Incident Reporting).
Recovery Notes	Following containment of any ransomware-related incident in this threat context, restore from offline or immutable backups only after completing a full IOC sweep for RaaS affiliate persistence mechanisms — specifically, scheduled tasks (query `schtasks /query /fo LIST /v` and review for tasks created in the 72 hours prior to encryption event), registry run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalent), and WMI subscriptions (`Get-WMIObject -Namespace root\subscription -Class __EventFilter`), as AI-assisted RaaS affiliates frequently establish secondary persistence before deploying the encryptor. Monitor restored systems for a minimum of 30 days post-recovery using Sysmon with process-creation and network-connection logging enabled, paying particular attention to any lateral movement attempts (Event ID 3, outbound connections from restored hosts to internal RFC1918 addresses on SMB port 445 or WMI port 135). Given the AI-assisted phishing entry vector, also re-issue credentials for any accounts whose phishing exposure cannot be ruled out and force MFA re-enrollment before restoring network access to recovered systems.
Forensic Artifacts	Windows Security Event Log — Event ID 4688 (Process Creation with command line) filtered for vssadmin.exe with 'delete shadows' argument and wmic.exe with 'shadowcopy delete' argument, indicating T1490 (Inhibit System Recovery) staging behavior consistent with RaaS affiliate pre-encryption preparation | Email gateway message trace logs and attachment sandbox verdicts for the 72 hours preceding any encryption event — specifically filter for messages with AI-generation indicators: near-zero grammar errors, sender domain registered within 30 days of delivery, and URLs using homograph or typosquatting domains, consistent with WormGPT/FraudGPT-generated lure campaigns | Perimeter firewall and web server access logs (Apache/Nginx access.log, IIS W3C logs) timestamped within 24-48 hours of any CISA KEV publication date affecting your internet-facing services — filter for HTTP 200 responses to URIs matching known exploitation patterns for recently disclosed vulnerabilities, establishing whether TTE-compressed exploitation preceded your patching cycle | Sysmon Event ID 1 (Process Creation) and Event ID 3 (Network Connection) logs filtered for ransomware staging behavior: cmd.exe or PowerShell spawned by a web service worker process (IIS w3wp.exe, Apache httpd.exe), followed by lateral movement connection attempts to internal hosts on SMB (445), RDP (3389), or WMI (135) — indicative of post-initial-access RaaS affiliate reconnaissance | Windows Volume Shadow Copy state (output of `vssadmin list shadows` run immediately upon detection) and file system change rate metrics from the File System event log (Microsoft-Windows-Kernel-General) — a sudden absence of VSS snapshots combined with high I/O rates on user data directories (Documents, Desktop, network shares) constitutes forensic confirmation of active encryption and drives immediate isolation decision under NIST 800-61r3 §3.3 containment

Per-Action IR Details

Step 1: Assess exposure — audit internet-facing assets for unpatched critical and high-severity vulnerabilities disclosed within the last 30 days; prioritize any with known public exploits given the reported

24-to-48-hour time-to-exploit window

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR Capability and Reducing Attack Surface

Controls: NIST SI-2 (Flaw Remediation), NIST RA-5 (Vulnerability Monitoring and Scanning), 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), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run a Shodan CLI query (`shodan search 'org:YOUR-ORG'`) to enumerate internet-facing assets, then cross-reference against CISA KEV catalog (`curl https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json`) using a Python script to flag any CVEs disclosed in the last 30 days with `dateAdded` within range. For internal scanning with no commercial scanner, deploy OpenVAS (Greenbone Community Edition) against your DMZ segment and filter results for CVSS ≥ 7.0 published after 30 days prior. Prioritize anything with a Metasploit module or public PoC on GitHub — search `site:github.com CVE-XXXX-XXXX exploit` for each critical finding.

Evidence: Before remediating, snapshot the current vulnerability state for the incident record: export your scanner results (OpenVAS XML or Shodan output) timestamped at audit time. Capture firewall rule exports and NAT tables showing which services are exposed. Pull network flow logs from your perimeter device (pfSense, Cisco ASA syslog, or cloud VPC flow logs) for the last 72 hours to identify whether any recently-disclosed CVE's affected port/service has already received unexpected inbound connection attempts from Shodan scanners or mass-exploitation bots — filter for SYN packets to the affected service port from IPs not in your allow-list.

Step 2: Review controls — verify email gateway filtering efficacy against AI-generated phishing content; confirm MFA enrollment across all privileged and remote-access accounts; validate EDR telemetry coverage for ransomware staging behaviors including volume shadow copy deletion and bulk file encryption activity

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Detection Capability Validation and Control Verification

Controls: NIST SI-3 (Malicious Code Protection), NIST SI-4 (System Monitoring), NIST IA-5 (Authenticator Management), NIST IR-3 (Incident Response Testing), 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 8.2 (Collect Audit Logs)

Compensating: For AI-generated phishing detection without a commercial email gateway: enable Microsoft Defender for Office 365 Plan 1 (included in M365 Business Basic) and configure the 'Standard' anti-phishing policy with impersonation protection enabled, or on-premises deploy Rspamd with the Neural module trained on recent WormGPT-style lure samples from OpenPhish. For MFA enrollment audit with no IdP dashboard, run: `Get-MsolUser -All | Where {$_.StrongAuthenticationRequirements.Count -eq 0} | Select UserPrincipalName` (Exchange Online) or query AD with `Get-ADUser -Filter * -Properties * | Where {$_.'msDS-MFALastUsed' -eq $null}`. For ransomware staging detection without EDR, deploy Sysmon with the SwiftOnSecurity config and write a PowerShell watcher: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where {$_.Id -eq 1 -and $_.Message -match 'vssadmin|wmic shadowcopy'}` to catch volume shadow copy deletion (T1490). For bulk encryption detection, monitor file system change rate with a scheduled task running `(Get-ChildItem C:\Users -Recurse | Measure-Object).Count` every 5 minutes and alert on delta >500 in a single interval.

Evidence: Before tuning controls, preserve baseline evidence of current state: export email gateway quarantine logs and spam filter decision logs for the last 14 days to identify any AI-crafted phishing that bypassed filtering (look for messages with high linguistic quality scores but mismatched sender domains or anomalous link patterns). Pull MFA enrollment reports from your IdP as a point-in-time snapshot. From Windows Security Event Log, collect Event ID 4625 (failed logon) and 4648 (explicit credential use) for all VPN and RDP endpoints over the past 30 days to establish a pre-control-review baseline of credential attack volume against remote access infrastructure.

Step 3: Update threat model — add AI-assisted phishing (T1566), rapid vulnerability exploitation (T1190), and ransomware-as-a-service affiliate models using WormGPT/FraudGPT tooling to your threat register; update likelihood ratings for social engineering scenarios

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Threat Modeling and IR Plan Currency

Controls: NIST IR-8 (Incident Response Plan), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without a commercial threat intelligence platform, perform this update using: (1) MITRE ATT&CK Navigator (free, web-based) — clone your current layer JSON and add T1566 (Phishing) sub-techniques T1566.001 and T1566.002 with a score increase reflecting AI-generation capability, T1190 (Exploit Public-Facing Application) with a 24-48hr exploitation note, and T1486 (Data Encrypted for Impact); (2) pull the CISA#StopRansomware advisories feed (https://www.cisa.gov/stopransomware) to identify which RaaS affiliates are currently active and map their TTPs into your Navigator layer; (3) document WormGPT/FraudGPT as a threat actor capability modifier in your risk register — treat any phishing scenario's likelihood score as elevated by one tier (e.g., 'Low' becomes 'Medium') until AI-phishing-resistant controls are validated.

Evidence: Before updating likelihood ratings, extract historical evidence to anchor the model revision: pull your email gateway's phishing detection logs for Q4 2024 through Q1 2025 and count AI-crafted phishing attempts (look for campaigns with low perplexity scores, grammatically flawless content, and domain spoofing) as your empirical baseline. Review your SIEM or Windows Event Log for any T1190-consistent patterns — Event ID 4625 spikes against internet-facing services correlated with CVE disclosure dates from the NVD feed. This evidence ties the threat model update to observed organizational exposure rather than industry statistics alone.

Step 4: Communicate findings — brief leadership on the volume increase and time-to-exploit compression with specific relevance to your sector; frame the risk as a capacity and speed problem, not solely a technology gap

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned and Organizational Communication

Controls: NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST IR-4 (Incident Handling), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a formal GRC platform, build the leadership brief using: (1) a one-page risk narrative citing the FortiGuard Labs 389% increase statistic alongside your organization's current mean-time-to-patch (MTTP) for critical vulnerabilities — if MTTP exceeds 48 hours, your organization is structurally exposed to the described TTE compression; (2) pull your sector's ransomware victim count from the CISA StopRansomware advisory page or FS-ISAC / H-ISAC / MS-ISAC sector-specific threat reports; (3) frame capacity gaps in concrete terms: 'We currently take X days to patch critical CVEs; threat actors are exploiting equivalent vulnerabilities within 24-48 hours — this is a Y-day exposure window per new critical CVE.' Use no acronyms, no ATT&CK IDs. Attach the MITRE ATT&CK Navigator screenshot showing T1566 and T1190 as your technical backup.

Evidence: The evidence package for the leadership brief should include: your organization's current vulnerability scan results showing count and age of unpatched critical/high CVEs on internet-facing assets; MFA enrollment gap report from Step 2; EDR telemetry coverage percentage across managed endpoints; and any observed phishing or exploitation attempts from the past 30 days pulled from email gateway and perimeter firewall logs. Presenting observed organizational evidence alongside the industry statistics directly ties the macro trend to your specific risk posture.

Step 5: Monitor developments — verify the specific FortiGuard Labs report statistics against the primary FortiGuard Labs publication; track CISA advisories and Known Exploited Vulnerabilities catalog for rapid exploitation patterns consistent with the TTE compression described

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Continuous Monitoring and Intelligence Integration

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without a commercial TI feed, establish a free monitoring stack: (1) subscribe to the CISA KEV RSS feed and set up a daily cron job that diffs new entries against your asset inventory (`curl

https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json | jq '[.vulnerabilities[] | select(.dateAdded >= "YYYY-MM-DD")]'`); (2) monitor FortiGuard Labs threat research directly at https://www.fortiguard.com/threat-signal-report and set a browser alert or use RSS-to-email for new publications; (3) subscribe to CISA's free email alerts at cisa.gov/subscribe-updates-cisa and the MS-ISAC Cyber Alert feed; (4) for WormGPT/FraudGPT-specific developments, monitor the Recorded Future or Flashpoint free community feeds, or track relevant threat actor Telegram channels via OSINT using legitimate monitoring tools — document any new capability announcements as threat model update triggers per Step 3.

Evidence: When a new CISA KEV entry is published, immediately check your perimeter logs for prior exploitation attempts against the affected service before patching: query firewall syslog or cloud VPC flow logs for inbound connections to the affected port/service from external IPs in the 24-72 hours following the CVE's NVD publication date (not the KEV addition date, as exploitation precedes KEV listing). If the affected service is web-facing, pull web server access logs (Apache access.log, IIS W3C logs, nginx access.log) and WAF logs for URI patterns consistent with the CVE's exploitation mechanism. This pre-patch forensic capture establishes whether you were targeted before remediation and triggers escalation to active incident handling if exploitation evidence is found.

Detection Guidance

Focus detection investment on three behavioral clusters tied to the TTPs described.

Phishing and initial access (T1566, T1190): Monitor email gateway logs for high-volume sending patterns, lookalike domain indicators, and messages that bypass traditional signature-based filters. AI-generated phishing frequently passes grammar and spelling heuristics; behavioral anomalies in link click timing and credential entry sequences are more reliable signals. Review authentication logs for credential stuffing patterns following phishing campaigns.

Ransomware staging and pre-encryption behavior (T1486): Hunt for volume shadow copy deletion (vssadmin delete shadows), disabling of backup services, and bulk file renaming or extension changes in endpoint telemetry. Alert on PowerShell or WMI commands consistent with lateral movement ahead of encryption events. Correlate EDR alerts with network segmentation violations between workstation and backup infrastructure segments.

Tooling acquisition and malware deployment (T1587.001, T1588.001): Monitor for process execution of known offensive tools and anomalous outbound connections to infrastructure associated with criminal marketplaces. Threat hunting hypotheses should include: newly provisioned external accounts accessing sensitive data repositories, followed by staging of compressed archives prior to encryption.

Log sources to prioritize: email gateway, authentication/identity provider, endpoint detection telemetry, network flow data for lateral movement, and backup system access logs. CISA's advisory AA24-317A (2023 Top Routinely Exploited Vulnerabilities) provides a reference baseline for initial access techniques to prioritize in detection rules.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`WormGPT`	AI-powered criminal tool leveraged via dark web marketplace access to generate convincing spear-phishing lures and assist in ransomware campaign execution without requiring social engineering expertise	MEDIUM
TOOL	`FraudGPT`	AI-powered criminal tool leveraged via dark web marketplace access to automate fraud, phishing, and malware customization operations as part of ransomware affiliate workflows	MEDIUM
TOOL	`Pending — refer to FortiGuard Labs 2025 ransomware report for published indicators`	The source report is expected to contain campaign-specific IOCs including C2 infrastructure, payload hashes, and affiliate tooling indicators; primary report URL was not independently verified in this session	LOW

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing
- **T1190** — Exploit Public-Facing Application
- **T1588.001** — Malware
- **T1587.001** — Malware

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-4** — Incident Handling

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1566	Phishing	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1588.001	Malware	Resource-Development
T1587.001	Malware	Resource-Development

Sources

Source	URL	Tier
6 Industries Most Vulnerable to Cyberattacks	https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks...	T1
Governments are in the top 3 most targeted sectors worldwide	https://news.microsoft.com/en-cee/2025/02/05/governments-are-in-the...	T1
Top Industries Most Vulnerable to Cyberattacks in 2026	https://www.eccu.edu/blog/top-industries-most-vulnerable-to-cyber-a...	T1
[PDF] Global Cybersecurity Outlook 2026 – World Economic Forum	https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2...	T3

Source	URL	Tier
2023 Top Routinely Exploited Vulnerabilities - CISA	https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a	**T1**

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