CONVERGE
TECHNOLOGY SOLUTIONS

THREAT INTEL REPORT 2025

Prepared by: Converge Cybersecurity Practice
convergetp.com/cybersecurity | 800.747.8585

MAY

Observations for May 2025

This month's threat activity shows a growing focus by attackers on security tools themselves, especially **Endpoint Detection and Response (EDR)** platforms. In one confirmed case, an attacker interrupted a SentinelOne software update to disable its protection and install **Babuk ransomware**. This method did not require advanced hacking skills–just timing and weak settings. It highlights how EDR, often the last defense on a system, is now being directly targeted to open the door for larger attacks.

This trend is not new, but it is gaining speed. Over the past year, attackers have used tools and techniques meant to turn off or get around EDR systems. These tools, along with mistakes in how EDR is set up or updated, are giving attackers more chances to strike. **EDR is no longer just a helpful tool–it is now a target**. If it fails, everything behind it is exposed.

In a separate event, attackers scanned thousands of websites for exposed Git files. These files can reveal passwords, code, and company details. When found, they are often used to steal data or plan future attacks. Many of these scans came from cloud servers, showing that attackers are using fast and cheap tools to search for common mistakes.

Finally, hiring teams were hit with **phishing emails** disguised as job applications. These emails tricked staff into downloading files that installed hidden software to steal information. Because hiring teams often deal with unknown senders, this method is hard to block without strong training and security tools in place. Together, these stories show that both systems and staff need better protection to keep up with changing threats.

Executive Overview

EDR AS A TARGET

Audience
- C-Suite Executives
- CISO
- IT Managers
- Risk Management Professionals
- Cybersecurity Professionals and Analysts
- Developers
- Project Managers
- Business Organizations

A newly disclosed technique known as Bring Your Own Installer (BYOI) allows attackers to bypass SentinelOne's Endpoint Detection and Response (EDR) protections by interrupting the agent upgrade process on misconfigured systems. This bypass results in a brief but exploitable window during which the endpoint is left completely unprotected. In a confirmed case, a threat actor used this method to disable SentinelOne protections and deploy Babuk ransomware.

This incident exemplifies a broader and accelerating trend: EDR is now a primary target of adversaries, and both technical misconfigurations and vendor-side issues are being leveraged to disable detection and response capabilities. Over the past two years, similar tactics have emerged through tools like EDRSilencer, EDRKiller, and the real-world CrowdStrike outage in 2024, where a failed agent update caused widespread protection gaps. These developments show that EDR must be treated not merely as a security product, but as critical infrastructure that demands rigorous configuration, centralized control, and constant validation.

SentinelOne has issued updated mitigation guidance, including the use of a new Online Authorization toggle that prevents unauthorized local agent upgrades. Organizations using SentinelOne—or any EDR product—should treat this as a high-priority misconfiguration risk and immediately assess their endpoint policy posture to avoid similar exploitation.

READ MORE: EDR AS A TARGET

GIT WEAKNESSES

Audience
- CISO
- Security Managers
- Cybersecurity Professionals
- DevSecOps Engineers
- Threat Intelligence Teams

On April 20-21, 2025, GreyNoise observed an unprecedented spike in global scans targeting Git configuration files, logging more than 4,800 unique IP addresses per day—surpassing all previous activity since September 2024. These scanning operations aim to discover exposed .git/config files and related directories which, if publicly accessible, could reveal sensitive codebase metadata, repository URLs, commit history, and credentials.

This spike, largely originating from cloud infrastructure in Singapore, the U.S., and Germany, indicates a coordinated and sustained reconnaissance campaign. With 95% of involved IPs flagged as malicious and previous breaches in 2024 exposing over 15,000 credentials and 10,000 repositories, this technique is a significant risk vector. The exploitation of known vulnerabilities, such as CVE-2021-23263, further increases the threat surface.

READ MORE: GIT WEAKNESSES

RETURN

Audience

- CISO
- Security Managers
- Cybersecurity Professionals
- Human Resources
- Recruitment Teams

RECRUITER VENOM

In Q2 2025, a financially motivated threat actor known as **Venom Spider** significantly escalated its operations by targeting Human Resources (HR) professionals with socially engineered phishing attacks. The group's campaign, observed by Arctic Wolf, deploys the modular **More_eggs** backdoor via ZIP files disguised as job application resumes. Delivered through personalized emails and hosted on fake candidate sites, the malware enables credential harvesting, persistent access, and data exfiltration.

This shift represents a notable evolution in targeting strategy, moving from e-commerce and online payments to a universal organizational weak point–recruitment workflows. The campaign leverages server-side polymorphism, CAPTCHA evasion, and "living-off-the-land" tactics, making detection by traditional security controls increasingly ineffective.

READ MORE: RECRUITERS VENOM

EDR AS A TARGET

OVERVIEW & IMPACT

Endpoint Detection and Response (EDR) tools represent the final and often only barrier between adversaries and critical systems once initial access has been achieved. However, as adversaries increasingly view EDR as the primary obstacle to malware deployment, lateral movement, and persistent, targeted efforts to bypass or disable these tools have accelerated.

The "Bring Your Own Installer" (BYOI) technique exposed in May 2025 against SentinelOne exemplifies a broader pattern: attackers are exploiting both tool-level misconfigurations and organizational implementation gaps to render EDR ineffective. This mirrors historical trends with open-source bypass tools like EDRSilencer and EDRKiller, and operational blunders such as the CrowdStrike outage in 2024, where a faulty agent update caused widespread endpoint failures across industries.

In this case, the SentinelOne bypass enabled adversaries to interrupt the upgrade process of the EDR agent, creating a protection gap during which Babuk ransomware was deployed. The attacker's method did not require exploitation of software vulnerabilities or rootkits–just timing, administrator access, and poor policy enforcement.

IMPACT

- **EDR Protection Gap:** 55-second downgrade window exploited to halt protection entirely.
- **Agent Unloading Without Tamper Code:** Anti-tamper protection bypassed without authorized uninstallation.
- **Babuk Ransomware Execution:** Ransomware executed in the unprotected window post-agent termination.
- **Agent Offline State:** SentinelOne console failed to reflect active protection gaps during exploitation.
- **Cross-Vendor Risk:** Research was coordinated across multiple EDR vendors; potential applicability extends beyond SentinelOne.
- **Historical Precedent:** Highlights that both threat actors and software vendors themselves (e.g., CrowdStrike, 2024) have contributed to EDR outages via poor testing, insufficient controls, or misconfigured update paths.

OBSERVATIONS

- Legitimate MSI installers were used to simulate agent upgrades, a method that can bypass basic detection thresholds.
- Terminating msiexec.exe halted the installation mid-upgrade, leaving no agent active.
- Event logs confirmed product version changes, service unloads, and installer exits consistent with agent manipulation.
- The SentinelOne endpoint went "offline" in the console but without raising sufficient alarms.
- Testing validated the attack across multiple versions of the agent unless the "Online Authorization" control was enabled.
- No tamper protection codes or EDR vulnerabilities were required–this was a purely procedural exploit.

GUIDANCE

STRATEGIC INTELLIGENCE

- **EDR Is the Final Line of Defense**
  - Once initial access is achieved, EDR is often the last mechanism standing between attackers and the endpoint. Its disruption—by configuration, vendor error, or active exploitation—represents total endpoint compromise.
  - **Past examples include:**
    - EDRSilencer and EDRKiller disabling EDR telemetry in stealthy campaigns.
    - CrowdStrike's 2024 update error, which caused mass agent failure across enterprise fleets.
    - MDR and EDR Integrationgaps.
- **Trend: EDR Is Now a Primary Target**
  - Adversaries are no longer bypassing or evading EDR—they are targeting it directly through kill chains.
  - **BYOI is part of a broader movement:** Living-off-the-Land Binary (LOLBins) abuse, legitimate software chaining, and policy-aware attacker behavior are enabling stealthy operations even in "protected" environments.
- **Enforce Configuration Hygiene**
  - EDR solutions are only as effective as their configurations.
  - Defaults are not secure. Relying on vendor defaults—such as allowing local upgrades—can render the platform ineffective under real-world attack conditions.

Operational Intelligence

- **Threat Vectors**
  - Administrative access and authorized installers abused to simulate legitimate agent updates.
  - Mid-upgrade termination creates an unprotected state with no active SentinelOne processes.
- **Monitoring & Detection Gaps**
  - No default alerting when agent upgrades are interrupted.
  - Agent appearing "offline" may be misinterpreted as a connectivity issue unless further investigated.
- **Response Actions**
  - Immediately enable "Online Authorization" in SentinelOne policy.
  - Disallow local MSI-based installations outside change-controlled windows.
  - Monitor for taskkill commands or msiexec.exe activity in conjunction with agent version changes.

Tactical Intelligence

- **Mitigation Strategies**
  - Enforce console-only agent upgrades with logging and change control validation.
  - Automate alerts for offline agents and correlate with local installation attempts.
  - Restrict access to installation binaries using endpoint application control or allowlisting.
  - Implement endpoint scripts that verify agent health post-upgrade and trigger alerts on failure.
- **Preventive Measures**
  - Validate all EDR deployment configurations quarterly or during red team exercises.
  - Perform adversary emulation to confirm that endpoint protection maintains integrity under common bypass scenarios.
  - Require MFA and justification for any local administrative access involving installer binaries.
  - Integrate agent presence checks into Zero Trust enforcement mechanisms.

THREAT HUNTING HYPOTHESES

EDR Downgrade Exploitation Window

Hypothesis: Threat actors are exploiting SentinelOne's local upgrade/downgrade process by terminating the installer mid-upgrade, leaving the endpoint unprotected.

Investigation Steps:

- Review SentinelOne event logs for rapid version transitions or "unload" events (Event ID 93) not followed by a successful agent restart.
- Correlate msiexec.exe executions with taskkill or administrative script activity.
- Identify endpoints that went offline in the console immediately after upgrade attempts and remained disconnected.

Unmonitored Endpoint Access Post-EDR Removal

Hypothesis: Attackers are deploying ransomware or remote access tools during gaps in EDR coverage created by intentional agent disruption.

Investigation Steps:

- Search file execution logs and scheduled task creations within 1-2 minutes of EDR agent termination.
- Look for known ransomware indicators (e.g., Babuk file artifacts, extension changes) on affected hosts.
- Cross-reference endpoint activity with SentinelOne offline periods for silent compromise indicators.

Widespread EDR Misconfiguration Across Environments

Hypothesis: Multiple endpoints across the organization remain vulnerable to local EDR downgrade bypass due to policy misconfiguration.

RETURN

Investigation Steps:

- Query SentinelOne policy settings to audit whether "Online Authorization" is disabled for any hosts.
- Scan system logs for recurring installer executions and incomplete upgrades across environment fleets.
- Verify administrative access activity patterns that align with SentinelOne installer use outside approved windows.

Ransomware Deployment via EDR Evade Toolchains

Hypothesis: Adversaries are combining the BYOI technique with other known EDR kill chains (e.g., EDRSilencer, BYOVD) for persistent EDR bypass and lateral movement.

Investigation Steps

- Search for signs of vulnerable or abused driver files known to be linked with EDR kill chains.
- Monitor for unusual usage of Windows Filtering Platform APIs or kernel-level driver loads.
- Identify overlap in systems affected by both downgrade techniques and driver-based evasion tools.

Sources

- **Aon:** Bring Your Own Installer – Bypassing SentinelOne
- **SentinelOne:** Protection Against Local Upgrade Technique
- **Fortified Health Security:** SentinelOne EDR Bypass Threat Bulletin
- **Security Affairs:** BYOI Bypass Technique Explained
- **Trend Micro: EDRSilencer:** Disrupting Endpoint Security Solutions
- **BleepingComputer:** EDRSilencer Red Team Tool Used in Attacks to Bypass Security
- **TechTarget:** Explaining the Largest IT Outage in History and What's Next

GIT WEAKNESSES

OVERVIEW & IMPACT

Attackers are leveraging large-scale, cloud-based IP infrastructure—primarily from providers such as Amazon, DigitalOcean, and Cloudflare – to perform broad internet scans for publicly exposed Git configuration files. These scans are not isolated events but part of a recurring global pattern, with the April 2025 event representing the most aggressive spike recorded to date.

When misconfigured, .git/ directories and associated config files can expose sensitive development metadata and credentials. These files are often left accessible due to oversights in web server configuration, especially in test or staging environments that are temporarily made public but never properly secured.

Once accessed, threat actors can:

- Infer the structure of development environments through exposed branch names and commit logs
- Identify source control systems in use (e.g., GitHub, GitLab) via remote origin URLs
- Harvest hardcoded secrets, tokens, and keys embedded in past commits
- Clone the full repository, gaining access to intellectual property, security mechanisms, and internal documentation

Such access not only undermines source code confidentiality but also increases the potential for downstream attacks—such as privilege escalation, lateral movement within CI/CD pipelines, or even software supply chain compromise.

IMPACT

- **Malicious Scanner Prevalence:** 95% of scanning IPs linked to known threat actors per GreyNoise intelligence.
- **Cross-Regional Exposure:** Reconnaissance traffic originated from and targeted Singapore, the U.S., and Germany.
- **Cloud-Based Recon at Scale:** Infrastructure points to automated scanning operations hosted on cloud platforms.
- **Credential & IP Theft Risk:** Similar exposures have led to theft of 15,000 credentials and 10,000 cloned private repos.
- **Exploit Amplification via CVE-2021-23263:** Vulnerability increases risk by exposing .git directories through misconfigured web servers.

OBSERVATIONS

- April 2025 activity involved ~4,800 unique IPs/day on peak dates
- Four observed spikes since September 2024, with April being the largest
- Scanning IPs are primarily associated with public cloud infrastructure
- Majority of scans are automated, using scripts and botnets
- Affected regions include APAC, North America, and Western Europe
- Scanned destinations often lack WAF or access control filtering for hidden directories

RETURN

GUIDANCE

Strategic Intelligence

- **Reframe Git Exposure as a Reconnaissance Risk**
  - Treat public-facing code repositories and developer infrastructure as potential early-stage targets in the kill chain.
  - Incorporate Git directory exposure checks into routine security posture assessments.
- **Harden Developer and CI/CD Governance**
  - Require enforcement of secrets management policies in version control systems.
  - Mandate access reviews for public repositories and enforce credential rotation policies.
- **Align With Cloud and DevSecOps Strategy**
  - Audit public cloud assets for web-exposed .git/ paths.
  - Integrate Git hygiene checks into CI/CD pipelines.

Operational Intelligence

- **Threat Vectors**
  - **Initial Access:** Crawlers identify .git/ config files to gain insight into repository structures and remote access URLs.
  - **Credential Leakage:** Commit histories and misconfigured Git hooks expose hardcoded secrets.
  - **Repository Cloning:** Attackers clone full repositories from exposed .git/ directories.
- **Detection & Monitoring Gaps**
  - Lack of WAF rules to block hidden path enumeration.
  - Inadequate logging of web path access attempts (e.g., .git/HEAD).
  - No automated scanning of exposed repos for secrets.
- **Security Enhancements for Organizations**
  - Deploy external Git exposure monitoring (e.g., GitGuardian, GitLeaks).
  - Block directory access with proper .htaccess, Nginx or secure proxy configuration.
  - Enforce private repository policies for all internal codebases.

Tactical Intelligence

- **Mitigation Strategies**
  - Disable directory indexing and deny access to .git paths at the server level.
  - Use file integrity monitoring to detect unauthorized access or changes in web root directories.
  - Rotate exposed secrets and tokens upon detection, even if access is not confirmed.
- **Preventive Measures**
  - Implement pre-commit hooks that scan for secrets before code is pushed.
  - Periodically run codebase scans using gitleaks, truffleHog, or similar tools.
  - Establish cross-functional response plans for accidental repository exposures.

RETURN

THREAT HUNTING HYPOTHESES

Reconnaissance Through Git Config Scanning

Hypothesis: Malicious actors are identifying exposed .git/config files to enumerate internal repositories and gain insight into developer workflows.

Investigation Steps:

- Query web access logs for patterns targeting .git/config or .git/HEAD.
- Correlate request sources with known GreyNoise Git Config Crawler IPs.
- Identify repeated scanning from cloud-hosted IP ranges.

CREDENTIAL EXPOSURE VIA GIT COMMIT HISTORY

Hypothesis: Leaked Git repositories contain hardcoded secrets or credentials that are being harvested post-exposure.

Investigation Steps:

- Use tools like gitleaks or truffleHog to scan commit histories of cloned repos.
- Match exposed secrets against credential vaults to confirm validity.
- Monitor for unauthorized access using known leaked keys.

Automated Repository Cloning via Misconfigured Git Dirs

Hypothesis: Threat actors are cloning entire repositories from accessible .git/ directories for code intelligence or supply chain insertion.

Investigation Steps:

- Monitor for outbound Git traffic anomalies from web-facing servers.
- Identify file downloads matching .pack, .idx, or objects/ structures.
- Analyze attacker-controlled mirrors or repositories for fingerprinted code matches.

Sources

- **GreyNoise:** Spike in Git Configuration Crawling
- **GBHackers:** 4,800 IPs Used to Target Git Config Files
- **Heise:** Git Config Files Targeted in Attacks
- **CVE-2021-23263:** MITRE CVE Details

RECRUITERS VENOM

OVERVIEW & IMPACT

The **Venom Spider** threat campaign demonstrates a strategic pivot toward exploiting HR departments as an initial access vector. HR teams are particularly vulnerable because their operational duties—evaluating unsolicited attachments and links from unknown sources—mirror phishing scenarios. This reality has allowed Venom Spider to blend seamlessly into the routine tasks of recruitment workflows.

Upon clicking a link in a seemingly legitimate job application email, recruiters are redirected to attacker-controlled websites. These sites mimic candidate resume portals and present a CAPTCHA page to bypass automated security scanning. The subsequent file download, posing as a resume, contains a ZIP archive embedded with a malicious LNK file and a decoy image. Execution of the shortcut triggers the **More_eggs** payload, which installs a modular backdoor and launches WordPad to mask the infection.

Impacts:

- **Broad Targeting Scope:** Any organization actively hiring is at risk.
- **Credential Theft:** The malware harvests usernames, passwords, and sensitive business data.
- **Infrastructure Abuse:** Uses legitimate Windows processes to maintain stealth.
- **Operational Risk:** Exploits high-volume HR activity (resume screening, job listings).

OBSERVATIONS

- **Initial Vector:** Spear-phishing emails with links to fraudulent resumes or personal job sites.
- **CAPTCHA Layer:** Fake CAPTCHA challenge used to deter automated scanners.
- **Payload Delivery:** Victim downloads a ZIP file containing a malicious .lnk file.
- **Distraction Mechanism:** WordPad is opened to distract while malware installs.
- **Backdoor Activation:** "More_eggs" executes, granting persistent shell access to the attacker.
- Server-side polymorphism generates unique payloads per victim.
- Use of existing subdomains and anonymized hosting to evade domain tracking.
- Living-off-the-land (LotL) strategies via ie4uinit.exe for stealth execution.

GUIDANCE

Strategic Intelligence

- **Threat Evolution:**
  - Venom Spider's pivot from e-commerce to HR systems reflects a strategic expansion to universally vulnerable roles.
  - Threat actors increasingly exploit business functions reliant on human interaction and trust-based workflows.
- **Business Implications:**
  - HR systems often interconnect with payroll, PII databases, and internal communications.
  - Data exfiltrated from HR departments may serve broader cybercriminal or espionage purposes.

RETURN

- **Recommendations:**
  - Evaluate HR workflows and implement zero-trust principles.
  - Treat HR and recruiting functions as critical attack surfaces requiring dedicated security controls.

Operational Intelligence

- **Detection Challenges:**
  - Use of legitimate tools like ie4uinit.exe hinders detection by traditional AV and EDR.
  - Server-side polymorphism bypasses signature-based filtering.
- **Security Weaknesses Exploited:**
  - High resume/application volume creates cognitive overload for HR teams.
  - Lack of file type inspection and behavioral sandboxing on HR endpoints.
- **Mitigation Strategies:**
  - Implement advanced phishing protection and behavioral analytics for HR-specific threats.
  - Deploy URL detonation services and sandbox testing on resume-related downloads.

Tactical Intelligence

- **Mitigation Strategies**
  - **Secure Resume Submission:** Require applicants to submit via secure portals with malware scanning.
  - **Filetype Restrictions:** Block .zip, .lnk, and other risky extensions in inbound HR communications.
  - **EDR Policy Tuning:** Flag and block use of ie4uinit.exe in non-standard contexts.
  - **User Training:** Conduct targeted phishing simulations and awareness training for HR personnel.
- **Security Measures**
  - Email Security Gateways with attachment inspection.
  - Strict endpoint policies for HR workstations.
  - Application whitelisting and restricted scripting capabilities.

THREAT HUNTING HYPOTHESES

Malware Delivery via Resume-Themed Phishing Emails

Hypothesis: Threat actors are delivering the More_eggs backdoor through spear-phishing emails that appear to be legitimate resume submissions targeting HR personnel.

Investigation Steps:

- Query email logs for messages containing ZIP file attachments from unknown external sources with subject lines referencing resumes or job applications.
- Inspect attachments for embedded .lnk files or dual-purpose ZIP contents with image decoys.
- Identify recurring domains or URLs that include CAPTCHA-like gatekeeping followed by file downloads.

Command-and-Control Communication via Polymorphic Infrastructure

Hypothesis: Spider uses server-side polymorphism and multi-level subdomains to evade threat detection and maintain resilient C2 channels.

Investigation Steps:

- Monitor DNS logs for repeated access to subdomain-rich structures on known or suspicious base domains.
- Detect unique download patterns where every request retrieves a differently hashed payload.
- Compare C2 traffic against IOC feeds and identify anomalous beaconing to newly registered or anonymized domains.

Credential Harvesting Through Living-Off-the-Land (LotL) Execution

Hypothesis: The More_eggs payload abuses native Windows binaries like ie4uinit.exe to execute scripts and collect credentials while evading endpoint detection.

Investigation Steps:

- Search process execution logs for instances of ie4uinit.exe invoked outside normal OS context
- Identify lateral movement or PowerShell activity tied to the initial binary's execution window
- Monitor memory dumps for credential stores accessed shortly after resume file execution

Sources

- **Arctic Wolf:** Venom Spider Uses Server-Side Polymorphism to Weave a Web Around Victims
- **CinchOps:** Venom Spider - The Malware Threat Targeting HR Professionals
- **SC Media:** Malware scammers target HR professionals with Venom Spider malware
- **UNU | HR Under Attack:** Sophisticated Malware Campaign Targets Recruiters

CONVERGE
TECHNOLOGY SOLUTIONS

Contact the Converge Threat Intel Group at cybersecurity@convergetp.com

convergetp.com/cybersecurity