INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 06:46 UTC

The Gentlemen RaaS: C2 Exposure Reveals 1,570+ Corporate Victims Across a Disciplined, Multi-Platform Ransomware Operation

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0198
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Windows, Linux, NAS, BSD, VMware ESXi, Hyper-V, Windows Defender, SMB, Group Policy (Active Directory)
Published	2026-04-21T14:18:00
Discovery Source	Rss

Executive Summary

Check Point researchers accessed a SystemBC command-and-control server tied to The Gentlemen ransomware-as-a-service operation, revealing more than 1,570 compromised corporate networks, the vast majority never publicly disclosed. The group has operated since July 2025, targeting Windows, Linux, VMware ESXi, Hyper-V, NAS, and BSD environments across heterogeneous enterprise infrastructure. The gap between 320 publicly claimed victims and 1,570+ C2-confirmed victims indicates that most compromised organizations are in an active dwell phase, exposing them to data theft, pre-ransomware staging, and selective extortion - threats that remain hidden until deployment or extortion demand.

Technical Analysis

The Gentlemen operates as a mature RaaS with multi-platform encryptors targeting Windows, Linux, NAS, BSD, VMware ESXi, and Hyper-V environments. SystemBC serves as the primary C2 and proxy channel, providing encrypted SOCKS5 tunneling to mask attacker traffic, relevant to CWE-319 (cleartext transmission) and CWE-327 (broken/risky cryptographic algorithms). The operation abuses Windows Defender (T1562.001) to disable defenses, uses SMB for lateral movement (T1021.002), and achieves persistence through Group Policy modification (T1484.001). Additional MITRE techniques observed include process injection (T1055), lateral tool transfer (T1570), C2 over HTTP/S (T1071.001), service stop (T1489), inhibit system recovery (T1490), valid account abuse (T1078), PowerShell execution (T1059.001), data encryption for impact (T1486), and exploit of public-facing applications (T1190). CWE-693 (protection mechanism failure) reflects the Defender bypass

tradecraft. No specific CVE is attributed in the primary research; ESXi and Hyper-V exploitation aligns with known hypervisor attack patterns. The 1,570-to-320 victim ratio is a critical intelligence signal indicating active pre-extortion dwell across a large portion of the botnet. Sources: Check Point Research (T3), The Hacker News (T3), Microsoft Security Blog (T1).

Action Checklist

1. Step 1: Containment, Immediately audit SystemBC indicators across your environment; block known SystemBC C2 communication patterns at the perimeter firewall and proxy. Isolate any host exhibiting outbound SOCKS5 tunneling to unrecognized external IPs. Prioritize ESXi, Hyper-V, and NAS hosts given The Gentlemen's confirmed targeting scope.
2. Step 2: Detection, Hunt for SystemBC artifacts: search EDR telemetry for svchost anomalies spawning network connections, unexpected SOCKS5 proxy traffic, and PowerShell execution chains (Event ID 4104). Check Windows Event Logs for Group Policy modification events (Event ID 5136) and Windows Defender tampering (Event ID 5001, 5004, 5007). If EDR is deployed, consult vendor-specific behavioral detection rules for Defender tampering (e.g., CrowdStrike's Falcon Intelligence for Defender API abuse patterns). Review SMB lateral movement indicators via Event ID 4624 (logon type 3) combined with new service creation (Event ID 7045) on remote hosts.
3. Step 3: Eradication, Remove SystemBC implants identified during detection; re-enable and verify integrity of Windows Defender real-time protection. Audit and revert unauthorized Group Policy Objects. Reset credentials for any valid accounts showing anomalous logon patterns (T1078). Patch internet-facing systems, with priority on ESXi and Hyper-V hosts exposed externally.
4. Step 4: Recovery, After eradication, validate that Defender policies are restored and no unauthorized GPOs remain. Monitor SMB traffic baselines for 14 days post-remediation. Confirm ESXi and Hyper-V snapshot/backup integrity before restoring workloads; ransomware operators targeting these platforms often delete snapshots (T1490) prior to encryption.
5. Step 5: Post-Incident, Conduct a gap assessment against CIS Benchmark controls for Windows Server and VMware ESXi hardening. Implement network segmentation to limit SMB reachability between workstation and server VLANs. Deploy deception assets (honeypots) tuned to SMB lateral movement patterns to improve early detection of future intrusions consistent with this tradecraft.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and breach notification counsel immediately if any of the following conditions are confirmed: evidence of data exfiltration prior to encryption (The Gentlemen C2 telemetry indicates staging before encryption), compromise of ESXi or Hyper-V hypervisors hosting systems that process PII, PHI, or PCI-DSS-scoped data (triggering mandatory breach notification timelines under GDPR Article 33, HIPAA §164.412, or state notification laws), active ransomware encryption detected on production systems, or the responding team lacks the capability to conduct live memory forensics on SystemBC-infected hosts.

Recovery Notes	Before restoring any virtualized workloads on ESXi or Hyper-V, verify backup integrity by restoring to an isolated VLAN and validating system hashes against pre-incident baselines — The Gentlemen specifically targets hypervisor snapshot chains for deletion (T1490), meaning backups predating the July 2025 campaign start date are the only reliable restore points. Monitor SMB traffic (TCP 445), new Windows service creation (Event ID 7045), and outbound SOCKS5 connections continuously for a minimum of 14 days post-eradication, as SystemBC implants have been observed re-establishing C2 channels from secondary persistence mechanisms not caught in initial triage. Re-run the CIS Benchmark assessment 30 days post-recovery to validate that hardening changes persisted and no drift toward pre-incident configuration has occurred via unauthorized GPO modification.
Forensic Artifacts	SystemBC implant in-memory configuration: Captured via full memory acquisition (WinPmem/Magnet RAM Capture) from suspected hosts — contains plaintext or lightly obfuscated C2 IP:port pairs, RC4 or AES encryption keys, and proxy configuration specific to The Gentlemen's C2 infrastructure; this artifact is destroyed on reboot. | Windows Defender Operational Event Log (Microsoft-Windows-Windows Defender/Operational.evtx): Event IDs 5001, 5004, and 5007 directly evidence Defender real-time protection disablement and configuration tampering that The Gentlemen operators perform prior to deploying ransomware payloads across Windows hosts. | Active Directory DS Replication and GPO modification logs (Windows Security Event ID 5136, objectClass=groupPolicyContainer): Documents unauthorized Group Policy Objects created or modified under T1484.001 to distribute ransomware binaries or disable security controls across domain-joined systems at scale. | ESXi datastore metadata and vmkernel logs (/vmfs/volumes/ directory timestamps, /var/log/hostd.log, /var/log/shell.log): Timestamps of deleted .vmdk snapshot delta files and descriptor files evidence T1490 snapshot deletion by The Gentlemen operators immediately preceding ESXi encryption; hostd.log records the API calls used to enumerate and delete VM snapshots. | Network proxy and firewall logs showing SOCKS5 tunnel establishment: Specifically, TCP sessions to external IPs on port 1080 or operator-configured high ports originating from svchost.exe-masquerading processes — these logs document the SystemBC C2 beaconing channel, lateral movement staging, and the dwell time between initial compromise and ransomware deployment across the 1,570+ victim network pattern confirmed by Check Point research.

Per-Action IR Details

Step 1: Containment — Immediately audit SystemBC indicators across your environment; block known SystemBC C2 communication patterns at the perimeter firewall and proxy. Isolate any host exhibiting outbound SOCKS5 tunneling to unrecognized external IPs. Prioritize ESXi, Hyper-V, and NAS hosts given The Gentlemen's confirmed targeting scope.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SI-4 (System Monitoring), CIS 13.4 (Perform Traffic Filtering Between Network Segments), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: On pfSense or iptables-managed perimeters, block outbound TCP 1080 (SOCKS5 default) and flag any non-standard high-port SOCKS5 negotiation: `iptables -A OUTPUT -p tcp --dport 1080 -j DROP && iptables -A OUTPUT -p tcp --dport 4000:9999 -m state --state NEW -j LOG --log-prefix 'SOCKS5-SUSPECT'`. For ESXi hosts, use `esxcli network firewall ruleset set --enabled=false --ruleset-id=sshServer` to disable unnecessary remote access immediately. Run Wireshark or tcpdump on perimeter tap with filter `tcp port 1080 or (tcp[13]=2 and tcp[12]=0x50)` to catch active SOCKS5 handshakes in flight. For NAS isolation, disable SMB shares and remote admin interfaces at the switch port level if host-level access is unavailable.

Evidence: Before isolating any host, capture full memory with WinPmem or Magnet RAM Capture on Windows endpoints — SystemBC runs as a reflectively-loaded implant and its configuration (C2 IP:port pairs, encryption keys) exists only in process memory. On ESXi, run `vm-support -s` to capture a diagnostic bundle including vmkernel logs and active network connections before pulling the NIC. Preserve firewall and proxy logs showing outbound SOCKS5 negotiation sequences and destination IPs/ports for C2 attribution. Document all active TCP sessions from suspected hosts using `netstat -anob` (Windows) or `ss -tnp` (Linux) before network isolation destroys that live state.

Step 2: Detection — Hunt for SystemBC artifacts: search EDR telemetry for svchost anomalies spawning network connections, unexpected SOCKS5 proxy traffic, and PowerShell execution chains (Event ID 4104). Check Windows Event Logs for Group Policy modification events (Event ID 5136) and Windows Defender tampering (Event ID 5001, 5004, 5007). Review SMB lateral movement indicators via Event ID 4624 (logon type 3) combined with new service creation (Event ID 7045) on remote hosts.

NIST Phase: Detection Analysis

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

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

Compensating: Deploy Sysmon with SwiftOnSecurity config (minimum) and add custom rules for: Event ID 3 (NetworkConnect) where ParentImage contains 'svchost.exe' AND DestinationPort is 1080 or matches known SystemBC high-port ranges; Event ID 1 (ProcessCreate) where ParentCommandLine contains 'powershell' spawning unknown binaries. For GPO tampering without SIEM, run this PowerShell on domain controllers hourly via Task Scheduler: `Get-ADObject -Filter {ObjectClass -eq 'groupPolicyContainer'} -Properties whenChanged | Where-Object {$_.whenChanged -gt (Get-Date).AddHours(-1)} | Select-Object Name, whenChanged | Export-Csv C:\GPO_Changes.csv -Append`. Use Sigma rule detection for SystemBC (search GitHub: SigmaHQ rule 'sysmon_susp_svchost_no_cli') converted to Windows Event Log queries with sigmac. Query Security.evtx directly using `wevtutil qe Security /q:"*[System[EventID=5136]]" /f:text` for AD object modification events.

Evidence: Collect Windows Security Event Log entries for Event ID 5136 (DS Object Modified) filtered on objectClass=groupPolicyContainer to identify unauthorized GPO changes consistent with The Gentlemen's use of GPO to deploy ransomware payloads and disable Defender. Capture Windows Defender operational log at `%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4Operational.evtx` for Event IDs 5001 (real-time protection disabled), 5004 (monitoring configuration changed), and 5007 (configuration changed) — these directly evidence Defender tampering preceding encryption. Preserve Sysmon Event ID 3 logs showing svchost.exe network connections to external IPs, which fingerprint SystemBC's use of svchost as a masquerade host. For ESXi, collect `/var/log/hostd.log` and `/var/log/shell.log` for unauthorized API calls or shell sessions preceding snapshot deletion activity consistent with T1490.

Step 3: Eradication — Remove SystemBC implants identified during detection; re-enable and verify integrity of Windows Defender real-time protection. Audit and revert unauthorized Group Policy Objects. Reset credentials for any valid accounts showing anomalous logon patterns (T1078). Patch internet-facing systems, with priority on ESXi and Hyper-V hosts exposed externally.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

Compensating: For SystemBC implant removal without EDR, use Autoruns (Sysinternals) to identify persistence mechanisms — SystemBC commonly persists via scheduled tasks or service registration; export baseline with `autorunsc.exe -a * -c > autoruns_baseline.csv` and diff against known-good. Verify Defender integrity with: `sc query WinDefend` and `Set-MpPreference -DisableRealtimeMonitoring $false; Get-MpComputerStatus | Select-Object RealTimeProtectionEnabled,AMServiceEnabled`. For GPO audit and revert, run `Get-GPOReport -All -ReportType

XML -Path C:\GPO_Audit.xml` then compare against last known-good backup in `SYSVOL\{domain}\Policies`. Force AD credential resets for all accounts with Event ID 4624 logon type 3 activity during the compromise window using: `Get-ADUser -Filter * | Where-Object {$_.LastLogonDate -gt $compromiseDate} | Set-ADAccountPassword -Reset`. For ESXi patching without vCenter, download VMware ESXi patches directly from my.vmware.com and apply via: `esxcli software vib update -d /vmfs/volumes/datastore/patch.zip`.

Evidence: Before removing SystemBC implants, capture the full file path, hash (SHA-256), and parent process of each implant artifact — use `Get-FileHash -Algorithm SHA256` on all identified binaries and cross-reference against VirusTotal or MalwareBazaar offline feeds. Preserve the registry hive snapshot (`reg save HKLM\SYSTEM system.hiv`) to document any service keys or Run entries used for SystemBC persistence before deletion. Export the full GPO diff showing unauthorized objects — use `Get-GPOReport` output before and after revert — as this constitutes evidence of T1484.001 (Group Policy Modification). Document all accounts reset with timestamps and source logon events for potential regulatory breach notification records.

Step 4: Recovery — After eradication, validate that Defender policies are restored and no unauthorized GPOs remain. Monitor SMB traffic baselines for 14 days post-remediation. Confirm ESXi and Hyper-V snapshot/backup integrity before restoring workloads; ransomware operators targeting these platforms often delete snapshots (T1490) prior to encryption.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 11.1 (Establish and Maintain a Data Recovery Process), CIS 8.2 (Collect Audit Logs)

Compensating: Validate ESXi snapshot integrity using `vim-cmd vmsvc/snapshot.getall ` for each VM and cross-check snapshot creation timestamps against the estimated compromise window — snapshots created or deleted during the intrusion period are suspect. Verify Hyper-V checkpoint integrity with `Get-VMSnapshot -VMName * | Select-Object VMName, Name, CreationTime | Export-Csv C:\HyperV_Snapshots.csv`. For SMB baseline monitoring without SIEM, deploy a lightweight osquery scheduled query: `SELECT pid, remote_address, remote_port, local_port FROM process_open_sockets WHERE remote_port=445` running every 5 minutes, logging to a central syslog target. Validate Defender policy restoration using Group Policy Results: `gpresult /H C:\GPResult.html /F` and inspect the security policy section for any remaining unauthorized configurations.

Evidence: Before restoring any ESXi or Hyper-V workload, preserve the datastore file listing with timestamps (`ls -la /vmfs/volumes/` on ESXi) to document evidence of T1490 snapshot deletion — missing .vmdk delta files or -snapshot descriptor files with anomalous modification times directly evidence pre-encryption staging. Capture the final SMB session table from domain controllers (`net session` and Windows Security Event ID 4624 logon type 3 logs) to establish a clean post-eradication baseline for the 14-day monitoring window. Archive the restored GPO XML exports as the verified clean-state reference for future deviation detection.

Step 5: Post-Incident — Conduct a gap assessment against CIS Benchmark controls for Windows Server and VMware ESXi hardening. Implement network segmentation to limit SMB reachability between workstation and server VLANs. Deploy deception assets (honeypots) tuned to SMB lateral movement patterns to improve early detection of future intrusions consistent with this tradecraft.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SC-7 (Boundary Protection), NIST SI-4 (System Monitoring), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 13.4 (Perform Traffic Filtering Between Network Segments)

Compensating: Run CIS-CAT Lite (free from CIS) against Windows Server and ESXi benchmarks to produce a scored gap report without enterprise tooling. For SMB segmentation on a budget, implement Windows Firewall GPO rules blocking TCP 445 inbound to workstation OUs from server subnets: `New-NetFirewallRule -DisplayName 'Block-SMB-Lateral' -Direction Inbound -Protocol TCP -LocalPort 445 -RemoteAddress -Action Block`. Deploy

OpenCanary (free, Python-based) as an SMB honeypot: configure `smb.enabled: true` in opencanary.conf and alert on any connection to the deception share — The Gentlemen's lateral movement via SMB service creation (Event ID 7045) will trigger this before reaching production hosts. Update Sigma detection rules in your SIEM or Windows Event Forwarding pipeline to include the specific SystemBC SOCKS5 behavioral pattern documented in the Check Point research for long-term threat hunting.

Evidence: Compile the complete incident timeline documenting SystemBC C2 dwell time (first beaconing event to detection), all accounts used under T1078, all GPO objects modified under T1484.001, and all hosts with confirmed Defender tampering events — this timeline is required for regulatory breach notification assessment and lessons-learned documentation per NIST 800-61r3 §4. Preserve the Check Point-referenced C2 IOC list (SystemBC C2 IPs/domains) as a permanent threat intelligence artifact in your IOC repository for ongoing detection tuning. Document all gaps identified in the CIS Benchmark assessment as formal risk acceptance or remediation tickets to satisfy NIST RA-3 (Risk Assessment) requirements.

Detection Guidance

Primary detection focus: SystemBC C2 beaconing and SOCKS5 proxy traffic. Query proxy and firewall logs for outbound connections using SOCKS5 protocol to non-inventory external IPs, particularly at irregular intervals suggesting automated beaconing. In EDR, hunt for svchost.exe or rundll32.exe instances with anomalous parent processes initiating encrypted outbound sessions. Windows Event ID 5136 (directory service object modified) combined with unexpected GPO changes is a high-fidelity indicator for T1484.001. Windows Defender tampering: monitor Event IDs 5001, 5004, and 5007 in the Microsoft-Windows-Windows Defender/Operational log. SMB lateral movement: correlate Event ID 4624 (type 3 network logons) from a single source to multiple destinations within short time windows, paired with Event ID 7045 (new service installed) on target hosts. Process injection (T1055): look for cross-process memory writes from non-system processes. PowerShell (T1059.001): alert on encoded command execution and AMSI bypass patterns. As of the publication date of this intelligence item, no comprehensive public IOC list has been released by Check Point Research; treat all SystemBC-attributed infrastructure as high-confidence adversary-controlled until formally published by the vendor.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not publicly confirmed as of configuration date]`	SystemBC C2 infrastructure attributed to The Gentlemen RaaS — specific IOCs not released in available source material; monitor Check Point Research and threat sharing platforms (ISACs, MISP) for updated indicators	LOW
IP	`[not publicly confirmed as of configuration date]`	SystemBC proxy/C2 IP infrastructure — specific values not disclosed in available source material; subscribe to Check Point ThreatCloud or equivalent feeds for confirmed indicators	LOW

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1583.004** — Server
- **T1041** — Exfiltration Over C2 Channel
- **T1055** — Process Injection
- **T1570** — Lateral Tool Transfer
- **T1071.001** — Web Protocols
- **T1057** — Process Discovery
- **T1489** — Service Stop
- **T1484.001** — Group Policy Modification
- **T1078** — Valid Accounts
- **T1059.001** — PowerShell
- **T1021.002** — SMB/Windows Admin Shares
- **T1490** — Inhibit System Recovery
- **T1543** — Create or Modify System Process
- **T1190** — Exploit Public-Facing Application
- **T1090.001** — Internal Proxy
- **T1562.001** — Disable or Modify Tools

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **SI-3** — Malicious Code Protection
- **CM-7** — Least Functionality
- **CM-6** — Configuration Settings
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SC-13** — Cryptographic Protection
- **SC-8** — Transmission Confidentiality and Integrity
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures

ISO-27001-2022

- **A.8.24** — Use of cryptography
- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1583.004	Server	Resource-Development
T1041	Exfiltration Over C2 Channel	Exfiltration
T1055	Process Injection	Defense-Evasion
T1570	Lateral Tool Transfer	Lateral-Movement
T1071.001	Web Protocols	Command-And-Control
T1057	Process Discovery	Discovery
T1489	Service Stop	Impact
T1484.001	Group Policy Modification	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1059.001	PowerShell	Execution
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1490	Inhibit System Recovery	Impact

Technique ID	Technique Name	Tactic
T1543	Create or Modify System Process	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1090.001	Internal Proxy	Command-And-Control
T1562.001	Disable or Modify Tools	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/systembc-c2-server-reveals-1570-v...	T3
DFIR Report – The Gentlemen & SystemBC: A Sneak Peek Behind ...	https://research.checkpoint.com/2026/dfir-report-the-gentlemen/	T3
CVE-2021-34450: Windows Hyper-V RCE Vulnerability - SentinelOne	https://www.sentinelone.com/vulnerability-database/cve-2021-34450/	T3
Ransomware operators exploit ESXi hypervisor vulnerability for ...	https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware...	T1
Threat Actors Exploiting New ESXi Vulnerability - Arete	https://areteir.com/resources/vmware-esxi-vulnerability-protection	T3

Generated 2026-04-22 06:46 UTC by TJS Security Command Center