INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-15 19:01 UTC

Rex Ransomware (.rex48) Identified with Double Extortion Tactics

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0321
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows systems (specific versions unconfirmed); broader platform scope under investigation
Published	2026-05-15
Discovery Source	Gemini

Executive Summary

A secondary analysis sourcing CYFIRMA researchers reports identification of a ransomware strain called Rex that appends a '.rex48' extension to encrypted files and employs double extortion, encrypting data while threatening public release if ransom is not paid within 72 hours. Windows systems are the reported target, though specific affected versions are unconfirmed and the campaign's full scope remains under investigation. The business risk is operational disruption from encrypted systems combined with reputational and regulatory exposure from threatened data publication. Critical caveat: CYFIRMA's original research report is not included in verified sources for this audit. Confidence in technical specifics is low pending independent verification of the primary source and confirmation of platform targeting beyond secondary references.

Technical Analysis

Rex ransomware (tracked by CYFIRMA) appends '.rex48' to encrypted files and presents victims with a 72-hour contact window before ransom escalation, a double extortion model combining data encryption with threatened public exposure. Reported target platform is Windows; specific versions are unconfirmed. No CVE is associated with this campaign. Mapped CWE: CWE-311 (Missing Encryption of Sensitive Data, referenced here in the context of unauthorized encryption by the attacker). MITRE ATT&CK coverage: T1486 (Data Encrypted for Impact), T1657 (Financial Theft), T1071 (Application Layer Protocol, likely for C2 communication). Lineage is unresolved: available sources reference a distinct 2016-era Linux.Rex.1 botnet (not ransomware) and a separate MedusaLocker variant labeled 'Rex ransomware.' Whether the CYFIRMA '.rex48' Windows strain is a new independent family, a MedusaLocker variant, or shares any lineage with prior 'Rex' families (which were

primarily botnets, not ransomware) is not confirmed. Prior 'Rex' references in available sources appear unrelated to the current Windows ransomware claim. No threat actor attribution is established. Source quality is low: primary reporting originates from a secondary Gemini-grounded source; CYFIRMA's original research report was not independently verified in this session and is not included in the audit sources. All technical specifics should be treated as LOW confidence until corroborated by primary source access.

Action Checklist

1. Step 1: Containment, Isolate any Windows systems exhibiting file extension changes to '.rex48' or displaying ransom notes. Disconnect affected hosts from the network immediately to prevent lateral spread. Do not power off; preserve volatile memory for forensic imaging. Note: Detection in Step 2 relies entirely on behavioral indicators and is not signature-based due to lack of sourced IOCs. False positive risk is elevated; require analyst review before isolation.
2. Step 2: Detection, Search endpoint logs and EDR telemetry for mass file rename events appending '.rex48', unexpected shadow copy deletion (vssadmin delete shadows), and outbound C2 traffic patterns consistent with T1071 (application-layer protocol abuse). Check for ransom note files dropped in user directories. No confirmed IOC hashes are available from independently verified primary sources at this time. All behavioral detections require analyst triage.
3. Step 3: Eradication, No vendor patch or specific remediation advisory is available for this campaign as of the configuration date. Remove identified malicious binaries using EDR tooling. Rebuild compromised hosts from known-clean images rather than attempting in-place cleaning. Verify backup integrity before restoration.
4. Step 4: Recovery, Restore from offline or immutable backups confirmed clean prior to the earliest suspected infection timestamp. Validate file integrity post-restoration. Monitor restored systems closely for 72 hours for re-infection indicators. Do not pay the ransom without consultation with law enforcement and legal counsel; payment does not guarantee data non-publication. Note: No actor attribution has been established for this campaign, so sanctions risk cannot currently be assessed. Legal review is required before any payment decision.
5. Step 5: Post-Incident, Review backup architecture for offline and immutable copies not accessible from production networks. Assess whether data exfiltration occurred before encryption to scope regulatory notification obligations. Map gaps against NIST CSF PR.DS (Data Security) and RS.CO (Response Communications) functions. Engage legal and compliance teams on notification timelines if exfiltration is confirmed.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to legal counsel and executive leadership immediately if forensic analysis of outbound proxy/firewall logs confirms pre-encryption data exfiltration occurred, as Rex's double extortion model creates concurrent regulatory breach notification obligations (GDPR 72-hour window, HIPAA 60-day window, or applicable state breach law) alongside active ransomware containment operations; also escalate if affected systems are confirmed to process PII, PHI, or financial data, or if initial attribution indicators overlap with OFAC-sanctioned ransomware actors, which would make ransom payment legally prohibited.

Recovery Notes	Restore only from backup media confirmed to have been offline and physically inaccessible to the production network at the time of the Rex infection, as the double extortion model implies the operators conducted network reconnaissance and may have accessed or destroyed network-reachable backups before deploying encryption. After restoration, enforce a minimum 72-hour heightened monitoring window using Sysmon with alerting on .rex48 FileCreate events, vssadmin delete shadows process execution (Sysmon Event ID 1), and anomalous outbound connections from user-space directories (%TEMP%, %APPDATA%), since Rex operators may retain persistence or re-access via credentials harvested during the initial intrusion. Do not treat ransom payment as a recovery path — Rex's double extortion model means payment addresses only decryption and not guaranteed suppression of exfiltrated data publication, and actor attribution must be screened against OFAC sanctions lists before any payment is contemplated.
Forensic Artifacts	$MFT (Master File Table) parsed with MFTECmd — provides exact creation timestamps for all .rex48 files and ransom note drops, establishing patient-zero directory, encryption progression order, and definitive infection start timestamp for backup recovery point selection | Windows Security Event Log Event ID 4688 (Process Creation) and Sysmon Event ID 1 — captures vssadmin.exe, bcdedit.exe, and wbadmin.exe executions with full CommandLine fields confirming Rex's shadow copy and backup catalog destruction, plus the originating Rex binary path and parent process chain | Sysmon Event ID 3 (Network Connection) and outbound proxy/firewall logs filtered for the 30-day pre-encryption window — identifies Rex C2 beaconing (MITRE T1071) and pre-encryption exfiltration sessions to actor-controlled infrastructure, required to determine double extortion scope and regulatory notification obligations | Windows VSS/Volume Shadow Copy service logs (Windows Application Event Log Event IDs 8193 and 12293) — confirms shadow copy deletion events correlated to the Rex infection timeline, establishing that in-place file recovery via VSS is unavailable and backup restoration is the only recovery path | Volatile memory image (WinPmem or Magnet RAM Capture) captured before system isolation — may contain Rex ransomware encryption key material, injected shellcode, or C2 configuration data in plaintext or partially decoded form, and is the only artifact that cannot be recovered after the system is powered down or isolated

Per-Action IR Details

Step 1: Containment — Isolate any Windows systems exhibiting file extension changes to '.rex48' or displaying ransom notes. Disconnect affected hosts from the network immediately to prevent lateral spread. Do not power off — preserve volatile memory for forensic imaging.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), 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 NAC or EDR-driven isolation, use Windows Firewall via PowerShell to block all inbound/outbound traffic on the affected host: `netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound`. Physically disconnect the network cable or disable the NIC via Device Manager if remote access is unavailable. For volatile memory capture before isolation, run WinPmem (`winpmem_mini_x64.exe output.raw`) or Magnet RAM Capture from a write-protected USB before touching any other artifact.

Evidence: Before isolating, capture: (1) full RAM image using WinPmem or Magnet RAM Capture to recover Rex ransomware encryption keys or injected process artifacts still resident in memory; (2) active network connections via `netstat -ano > netstat_snapshot.txt` to document live C2 channels; (3) running process list via `tasklist /v > processes.txt` and `wmic process get name,processid,parentprocessid,commandline > wmic_procs.txt` to identify the Rex executable or any injected host process; (4) list of recently modified files via `forfiles /p C:\ /s /m *.rex48 /c "cmd /c

echo @path @fdate @ftime" > rex48_files.txt` to establish encryption boundary and initial access timestamp.

Step 2: Detection — Search endpoint logs and EDR telemetry for mass file rename events appending '.rex48', unexpected shadow copy deletion (vssadmin delete shadows), and outbound C2 traffic patterns consistent with T1071 (application-layer protocol abuse). Check for ransom note files dropped in user directories. No confirmed IOC hashes are available from verified sources at this time.

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-2 (Event Logging), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM or EDR, use Sysmon (deploy with SwiftOnSecurity config) and query Windows Event Logs directly: (1) For mass file renames to .rex48 — Sysmon Event ID 11 (FileCreate) filtered on TargetFilename containing '.rex48': `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Message -match '\.rex48'}`. (2) For shadow copy deletion — Windows Security Event ID 4688 (Process Creation) or Sysmon Event ID 1 filtering CommandLine containing 'vssadmin' AND 'delete': `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'vssadmin.*delete'}`. (3) For ransom note drops — Sysmon Event ID 11 filtered on TargetFilename matching common Rex note naming patterns (e.g., 'README', 'HOW_TO_DECRYPT', 'RESTORE_FILES') across user profile directories (%USERPROFILE%, C:\Users*\Desktop). (4) For C2 (MITRE T1071) — Capture outbound traffic with Wireshark or `netsh trace start capture=yes` and filter for anomalous HTTP/HTTPS beaconing (regular intervals, unusual User-Agent strings, or connections to recently registered domains) from the ransomware process PID identified in Step 1.

Evidence: Collect before analysis actions alter log state: (1) Windows Security Event Log — Event ID 4688 (Process Creation) for vssadmin.exe, wbadmin.exe, bcdedit.exe (common ransomware defense evasion tools) and any unsigned executable launched from %TEMP%, %APPDATA%, or %ProgramData%; (2) Sysmon Event ID 1 (Process Create) for the Rex binary and any child processes, capturing full CommandLine and ParentCommandLine fields; (3) Sysmon Event ID 3 (Network Connection) for outbound connections originating from the ransomware process — note destination IPs, ports, and DNS query names; (4) Windows Application Event Log for VSS errors (Event ID 8193, 12293) confirming shadow copy deletion occurred; (5) File system timeline from $MFT (Master File Table) parsed with MFTECmd (`MFTECmd.exe -f $MFT --csv output_dir`) to establish exact order and timestamps of .rex48 file creation events and ransom note drops, which reveals encryption progression and potential patient-zero directory.

Step 3: Eradication — No vendor patch or specific remediation advisory is available for this campaign as of the configuration date. Remove identified malicious binaries using EDR tooling. Rebuild compromised hosts from known-clean images rather than attempting in-place cleaning. Verify backup integrity before restoration.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-2 (Baseline Configuration), NIST IR-4 (Incident Handling), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software)

Compensating: Without EDR, use the following manual procedure: (1) Boot the isolated system from a trusted WinPE USB or analyst workstation with the suspect drive mounted read-only (using a hardware write blocker). (2) Use ClamAV (`clamscan -r --remove=no --log=scan_results.txt C:\`) to identify and log malicious files without deletion — review before removing. (3) Build a YARA rule targeting the .rex48 extension dropper once a sample is acquired: `rule Rex_Ransomware { strings: $ext = ".rex48" $note = "HOW_TO_DECRYPT" condition: any of them }` and scan with `yara64.exe rex_rule.yar C:\ -r`. (4) Rebuild from a pre-incident golden image (bare-metal or VM snapshot) rather than attempting in-place removal — ransomware persistence mechanisms (scheduled tasks, registry Run keys) are difficult to enumerate completely without EDR telemetry.

Evidence: Before eradication actions destroy artifacts: (1) Collect the Rex ransomware binary — search Sysmon Event ID 1 CommandLine fields and $MFT timeline for the originating executable path, then copy to evidence storage with SHA-256 hash documented; (2) Export all identified persistence mechanisms — query

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, and scheduled tasks via `schtasks /query /fo LIST /v > scheduled_tasks.txt`; (3) Capture the ransom note file(s) verbatim from user directories — note exact filenames, paths, and embedded contact/payment URLs for threat intelligence pivoting; (4) Image the encrypted disk (using dcfldd or FTK Imager) before rebuilding, in case decryption keys become available from law enforcement action against the Rex operator infrastructure.

Step 4: Recovery — Restore from offline or immutable backups confirmed clean prior to the earliest suspected infection timestamp. Validate file integrity post-restoration. Monitor restored systems closely for 72 hours for re-infection indicators. Do not pay the ransom — payment does not guarantee data non-publication and may violate sanctions obligations depending on actor attribution.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Without an enterprise backup platform: (1) Verify backup media was offline and not network-accessible at time of infection — Rex double extortion operators likely performed network reconnaissance before deploying ransomware, meaning any network-reachable backup shares may have been exfiltrated and/or encrypted. (2) Confirm backup integrity by computing SHA-256 checksums of critical restored files and comparing against pre-incident hashes documented in your change management records. (3) Deploy Sysmon on restored systems immediately with alerting on: FileCreate events targeting .rex48 extensions, Process Creation events for vssadmin with 'delete' arguments, and outbound connections from newly spawned processes in %TEMP% or %APPDATA%. (4) Run `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' -MaxEvents 5000 | Export-Csv sysmon_72h_monitor.csv` at 24-hour intervals for the monitoring window to detect re-infection.

Evidence: Before restoring, document: (1) Exact timestamp of the earliest .rex48 file creation event (from $MFT timeline) to establish the definitive backup recovery point — any backup created after this timestamp is potentially tainted; (2) Verify no Rex-related processes or scheduled tasks persist on the restore environment itself before standing it up (review Sysmon Event ID 1 on the restore server if network-connected); (3) After restoration, run `certutil -hashfile SHA256` spot-checks on critical business files against known-good hashes to confirm decryption/restoration fidelity; (4) Document the ransom note's 72-hour deadline timestamp as the regulatory clock anchor — if exfiltration is confirmed, this establishes the latest possible breach notification trigger date for compliance purposes.

Step 5: Post-Incident — Review backup architecture for offline and immutable copies not accessible from production networks. Assess whether data exfiltration occurred before encryption to scope regulatory notification obligations. Map gaps against NIST CSF PR.DS (Data Security) and RS.CO (Response Communications) functions. Engage legal and compliance teams on notification timelines if exfiltration is confirmed.

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 IR-6 (Incident Reporting), NIST AU-11 (Audit Record Retention), NIST RA-3 (Risk Assessment), NIST SI-12 (Information Management and Retention), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.4 (Enforce Data Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a DLP or CASB solution to confirm exfiltration: (1) Review outbound firewall and proxy logs (or Windows Firewall log at `C:\Windows\System32\LogFiles\Firewall\pfirewall.log`) for large data transfers in the days preceding .rex48 encryption events — Rex double extortion operators typically exfiltrate before encrypting. (2) Correlate Sysmon Event ID 3 (Network Connection) records and DNS query logs (Windows DNS debug log or Wireshark captures) for connections to cloud storage endpoints (e.g., Mega.nz, paste sites, actor-controlled infrastructure) from the compromised host. (3) Use osquery (`SELECT * FROM process_open_sockets WHERE remote_port NOT IN (80, 443) AND state = 'ESTABLISHED';`) on surviving systems to identify any lingering unusual

outbound connections. (4) Document all findings in a structured incident report mapped to NIST 800-61r3 §4 lessons-learned format for use in tabletop exercise updates.

Evidence: Post-incident evidence to preserve for regulatory and legal purposes: (1) Full proxy/firewall log exports covering the 30-day window before first observed .rex48 file — filtered for large outbound transfers (>100MB sessions) or connections to file-sharing or anonymization infrastructure, which would confirm Rex's double extortion exfiltration phase; (2) Complete Sysmon log export (Event IDs 1, 3, 11) from all affected hosts, retained per NIST AU-11 (Audit Record Retention) requirements and applicable breach notification regulations; (3) A copy of the Rex ransom note with embedded payment/contact URLs preserved verbatim as evidence of extortion demand — relevant to law enforcement referral and sanctions screening against OFAC-designated ransomware groups; (4) Chain-of-custody documentation for all disk images and memory captures taken during Steps 1-4, establishing forensic integrity for any potential litigation or regulatory examination.

Detection Guidance

No confirmed IOC hashes, IPs, or domains are available from independently verified primary sources at this time. Detection should rely on behavioral indicators: (1) Mass file rename events appending '.rex48', query EDR or SIEM for high-volume rename operations within short time windows; (2) Shadow copy deletion, Windows Event Log or EDR alert on vssadmin.exe or wmic.exe invocations with 'delete shadows' arguments; (3) Ransom note creation, alert on creation of txt or html files with names matching common ransom note patterns (e.g., 'HOW_TO_DECRYPT', 'README') in multiple directories; (4) Outbound application-layer C2 (T1071), inspect for anomalous HTTP/HTTPS beaconing to newly registered or low-reputation domains from hosts showing other indicators. If the MedusaLocker lineage can be independently confirmed through secondary analysis, existing MedusaLocker YARA rules may provide experimental partial coverage; validate thoroughly before deployment and do not assume lineage without confirmation. All findings require human analyst review given the low source confidence on this campaign.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`.rex48 file extension on encrypted files`	File extension appended to encrypted files by Rex ransomware; behavioral indicator only, not a network IOC	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1071** — Application Layer Protocol
- **T1657** — Financial Theft
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

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.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071	Application Layer Protocol	Command-And-Control
T1657	Financial Theft	Impact
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Linux.Rex.1, a new Linux Trojan the creates a P2P Botnet	https://www.cyberdefensemagazine.com/linux-rex-1-a-new-linux-trojan...	T3
Rex Ransomware (MedusaLocker Variant) Decryption and Recovery	https://medusadecryptor.com/medusalocker/rex-ransomware/	T3
Nasty Rex Linux Trojan Packs DDoS Attacks, Ransomware, And ...	https://hothardware.com/news/nasty-rex-linux-trojan-packs-ddos-atta...	T3
Ransomware threatens Linux servers, especially web servers	https://www.carbonite.com/blog/2017/ransomware-threatens-linux-serv...	T3

Source	URL	Tier
Rex ransomware removal [.Rex48 file virus]. - YouTube	https://www.youtube.com/watch?v=zyY4NScXWqo	**T3**

Generated 2026-05-15 19:01 UTC by TJS Security Command Center