INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:37 UTC

Foster City Ransomware Attack Disrupts Municipal IT and Communication Systems

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0079
Type	Threat Campaign
Severity	HIGH
Affected Products	Foster City, California municipal IT infrastructure and communication systems
Published	2026-03-21

Executive Summary

Foster City, California suffered a ransomware attack that shut down municipal IT and communication systems, prompting city leadership to consider declaring a state of emergency. Multiple city services were disrupted, indicating broad impact across networked infrastructure. For organizations in the public sector or with shared services dependencies, this incident reinforces the operational and reputational risk ransomware poses to government continuity.

Technical Analysis

The Foster City incident is consistent with ransomware campaigns targeting local government entities. MITRE ATT&CK techniques observed in this class of attack include T1486 (Data Encrypted for Impact), T1490 (Inhibit System Recovery), and T1489 (Service Stop). Typical attack chains for municipal ransomware involve initial access via phishing (T1566) or exploitation of exposed remote services such as RDP or VPN endpoints, followed by lateral movement, privilege escalation, and deployment of encryption payloads. No CVE or CWE identifiers have been associated with this specific incident in available public reporting. Specific ransomware group attribution, confirmed initial access vector, and scope of any data exfiltration have not been publicly disclosed as of this analysis. Source quality is limited to Tier 3 regional and local news reporting; technical details should be treated as unconfirmed until official disclosure from Foster City or a credible threat intelligence source.

Action Checklist

1. Step 1 (Immediate): Audit and restrict internet-facing remote access services (RDP, VPN, Citrix); disable or enforce MFA on all external-facing endpoints if not already enforced.

2. Step 2 (Detection): Search endpoint and SIEM logs for indicators of T1486 activity, rapid file rename operations, volume shadow copy deletion commands (vssadmin, wbadmin), and services being stopped en masse.

3. Step 3 (Assessment): Inventory backup systems and verify backup integrity and offline or immutable status; confirm recovery time objectives are current and tested.

4. Step 4 (Communication): Brief leadership on ransomware exposure posture and review your organization's incident response plan for regulatory notification timelines applicable to your jurisdiction.

5. Step 5 (Long-term): Conduct or schedule a tabletop exercise simulating ransomware encryption of critical infrastructure; review network segmentation to limit lateral movement from a compromised endpoint to core systems.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or law enforcement (FBI IC3) immediately if any Step 2 indicators are confirmed in production logs, or if backup integrity assessment (Step 3) reveals encrypted/deleted backups. If your organization has no documented IR plan or backup testing, escalate to C-suite for emergency resource allocation within 24 hours.
Recovery Notes	Post-containment recovery: (1) Verify all backups are unencrypted and uncorrupted before restoring. (2) Restore systems in dependency order: domain controllers → file servers → end-user workstations. (3) Patch all systems immediately during restoration; do not restore to pre-compromise OS state. (4) Re-enable segmentation and MFA after restoration; do not restore to pre-incident permissive network. (5) Conduct forensic imaging of compromised systems before wiping; preserve evidence for 6 months pending law enforcement request.
Forensic Artifacts	Windows Event Log 4688 (Process Creation) and 4624/4625 (Logon events) — identify attacker entry point and command execution pattern | Windows Event Log 4697 (Service installed) and 7034/7035/7036 (Service stopped/started) — track persistence mechanisms and T1486 service termination activity | Volume Shadow Copy metadata and deletion attempts: `vssadmin list shadows` output, PowerShell transcript logs containing wbadmin/vssadmin commands | File system timeline (MFT on Windows, inode metadata on Linux) — track file encryption timestamp and rapid file rename operations characteristic of ransomware | Network traffic pcap from suspected compromise window, focusing on SMB/RDP/DNS queries to C2 infrastructure; firewall/proxy logs showing exfiltration or lateral movement

Per-Action IR Details

Step 1 (Immediate): Audit and restrict internet-facing remote access services (RDP, VPN, Citrix); disable or enforce MFA on all external-facing endpoints if not already enforced.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools and resources); §3.2.1 (containment strategy for initial access vectors)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-4 (Identifier Management), CIS 5.2 (Multi-factor Authentication)

Compensating: Without enterprise MFA: (1) Audit RDP/VPN listening ports with `netstat -ano | findstr :3389` (Windows) or `ss -tlnp | grep -E ':(3389|443)'` (Linux). (2) Enable Windows native NPS (Network Policy Server) RADIUS with TOTP via open-source NPS extensions or Yubico PAM for SSH. (3) Disable RDP entirely if not

operationally critical; use jump-host architecture with SSH key-only authentication. (4) Document current exposure in a spreadsheet: hostname, service, port, MFA status, last access log date.

Evidence: Before restricting access: (1) Collect Windows Event Log 4624 (logon) and 4625 (failed logon) for past 30 days to identify legitimate external access patterns. (2) Export firewall inbound rules and VPN/Citrix access logs to identify who is using these services. (3) Capture current RDP session list: `query session /server:[hostname]`. (4) Document baseline: screenshot of firewall policies, VPN client logs, Citrix session manager logs. This becomes your 'before' state for post-incident forensics.

Step 2 (Detection): Search endpoint and SIEM logs for indicators of T1486 activity — rapid file rename operations, volume shadow copy deletion commands (vssadmin, wbadmin), and services being stopped en masse.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Detection and Analysis: source identification and analysis); §3.2.2 (determine scope of compromise)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-2 (Audit Events), CIS 8.2 (Collect Detailed Audit Logs), CIS 8.5 (Implement YARA or Sigma rules for ransomware patterns)

Compensating: Without SIEM: (1) Search Windows Event Log 4688 (process creation) for parent/child process: `wmic logicaldisk get name | find /v ':' > drives.txt && for /f %d in (drives.txt) do dir %d:\*.exe 2>nul | find 'vssadmin' 'wbadmin' 'cipher'`. (2) Search Application event log for service stop events (Event ID 7034, 7035, 7036). (3) Parse PowerShell transcript logs (if enabled) at `C:\Users\[user]\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt` for vssadmin/wbadmin commands. (4) Use Autoruns (Sysinternals) to snapshot current services and compare against known-good baseline. (5) Manual log review: check `C:\Windows\System32\config\Security` (EVTX) for suspicious process chains.

Evidence: Capture BEFORE searching: (1) Full copy of `C:\Windows\System32\winevt\Logs\` (all .evtx files, especially Security, System, Application). (2) PowerShell transcript logs and PSReadLine history. (3) Process execution timeline: `wevtutil qe Security /q:*[System[(EventID=4688)]] /f:text > process_timeline.txt`. (4) Volume Shadow Copy metadata: `vssadmin list shadows > vss_baseline.txt` (run before deletion is detected). (5) File system timeline for encrypted file extensions (.locked, .crypt, etc.): `Get-ChildItem -Path C:\ -Recurse -Filter *.locked 2>$null | Export-Csv encrypted_files.csv`.

Step 3 (Assessment): Inventory backup systems and verify backup integrity and offline or immutable status; confirm recovery time objectives are current and tested.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment strategy: system backups and recovery capability); §2.1 (Preparation: backup and recovery procedures)

Controls: NIST 800-53 CP-9 (Information System Backup), NIST 800-53 CP-10 (Information System Recovery and Reconstitution), NIST 800-53 SC-7 (Boundary Protection — air-gapped backup storage), CIS 3.14 (Ensure Backups Are Stored Offline and Immutable)

Compensating: Without enterprise backup solution: (1) Manually inventory all backups: external USB drives, NAS appliances, tape storage. Create spreadsheet: backup name, location (online/offline/air-gapped), last verified date, RTO/RPO, storage format, encryption status. (2) Test recovery on non-production system: restore 1 file from each backup to confirm integrity (no corruption). (3) If using NAS/QNAP/Synology, verify snapshot immutability is enabled (`Snapshot Lock` feature in UI; check NFVO/WORM settings). (4) If using external drives: physically disconnect from network after daily backup; store in locked cabinet or offsite. Document chain of custody. (5) Verify RTO/RPO by restoring one critical system from backup and timing full restoration process.

Evidence: Capture BEFORE assessing: (1) Current backup configuration and job logs: extract from Veeam/Commvault/Bacula UI or examine cron jobs (`crontab -l`, `cat /etc/cron.d/*`). (2) Last successful backup timestamp and size: `Get-ChildItem -Path 'D:\Backups\' | Select-Object Name, LastWriteTime, Length`. (3) Network diagram showing backup storage connectivity (Is it on same network? Air-gapped? Immutable?). (4) Backup encryption keys and retention policy documentation. (5) RTO/RPO baseline from last disaster recovery test (or current SLA

agreements).

Step 4 (Communication): Brief leadership on ransomware exposure posture and review your organization's incident response plan for regulatory notification timelines applicable to your jurisdiction.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities: lessons learned, notification); §1 (overview of IR roles and responsibilities)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 IR-4 (Incident Handling), NIST 800-53 IR-6 (Incident Reporting), CIS 19.1 (Establish and Maintain an Incident Response Process)

Compensating: Without formal IR framework: (1) Create a one-page incident notification matrix: list all systems, owner, data classification, applicable regulations (HIPAA, PCI-DSS, state breach notification laws, municipal transparency laws). (2) Document notification timeline: law enforcement (FBI IC3 for ransomware), state AG (if required), customers (within 30-60 days per most state laws), insurance carrier, board/council, media. (3) Identify legal counsel and cyber insurance contacts; ensure their contact info is in printed form (not digital-only). (4) Draft a template incident communication: technical summary, actions taken, customer impact, guidance for users. (5) Brief leadership: ransomware exposure = network segmentation gaps, backup testing failures, MFA enforcement gaps. Use Foster City case as example.

Evidence: Capture BEFORE communicating: (1) Snapshot of current IR plan (version, date last reviewed, approval signatures). (2) Regulatory requirements applicable to your organization: compile into a checklist. (3) Prior incident response logs if any (anonymized lessons learned). (4) Documentation of who should be notified (stakeholder list, contact info, roles). (5) Chain of custody log if any forensic data is involved.

Step 5 (Long-term): Conduct or schedule a tabletop exercise simulating ransomware encryption of critical infrastructure; review network segmentation to limit lateral movement from a compromised endpoint to core systems.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4.1 (Lessons learned: recommendations for prevention); §2 (Preparation phase: IR exercises and team training)

Controls: NIST 800-53 CP-3 (Contingency Training), NIST 800-53 SC-7 (Boundary Protection and network segmentation), NIST 800-53 AC-4 (Information Flow Enforcement), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 12.1 (Segment Networks Based on Sensitivity)

Compensating: Without professional tabletop facilitator: (1) Use NIST SP 800-61 Appendix B (sample IR roles/responsibilities) as template. Schedule 2-hour tabletop: inject scenario 'Critical file server encrypted, backups offline, all RDP sessions blocked.' Play through decision tree: Who decides to declare incident? How is CEO notified? What's first action? (2) Network segmentation: map current network using `nmap -sn 192.168.0.0/16` and Wireshark traffic capture. Identify: (a) workstations able to reach domain controllers? (b) Users able to RDP into critical servers? (c) Printers, IoT on same VLAN as medical/financial systems? (3) Create VLANs: segment by function (user workstations, servers, backups, guest). Use firewall rules to restrict traffic: block workstations from initiating SMB to servers outside their department. (4) Document allowed trust relationships only; deny all else. (5) Retest after changes using same nmap/Wireshark process.

Evidence: Capture BEFORE redesigning network: (1) Current network diagram (logical and physical topology). (2) VLAN configuration and firewall rules export. (3) SMB/135-139/445 traffic capture showing who talks to whom: `Get-NetTCPConnection -State Established | Where-Object {$_.RemotePort -eq 445} | Export-Csv smb_connections.csv`. (4) Active Directory trust relationships and group policy scope. (5) Baseline of successful tabletop (or IR drill) outcome and recommendations. This becomes your 'before' state for measuring network segmentation improvements.

Detection Guidance

In the absence of confirmed IOCs from this incident, detection should focus on behavioral indicators consistent with T1486, T1489, and T1490. Key signals to monitor: (1) Volume shadow copy deletion, query Windows event logs for process creation events (Event ID 4688) or Sysmon Event ID 1 where command line contains 'vssadmin delete shadows', 'wbadmin delete catalog', or 'bcdedit /set recoveryenabled no'. (2) Mass file rename or extension change activity, EDR telemetry showing high-volume file modification events in short time windows, particularly across network shares. (3) Service termination, Event ID 7036 or 7040 in the System log showing security, backup, or database services stopping unexpectedly. (4) Lateral movement precursors, authentication anomalies such as logon type 3 events (network logon) from a single source to multiple hosts in short succession (Event ID 4624). No confirmed IOCs (hashes, IPs, domains, ransom note filenames) for this specific campaign have been publicly released. Monitor CISA advisories and MS-ISAC bulletins for any attribution updates.

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1490** — Inhibit System Recovery
- **T1489** — Service Stop

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **IR-4** — Incident Handling
- **AT-2** — Literacy Training and Awareness
- **SC-13** — Cryptographic Protection

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

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

CIS-V8

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

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1490	Inhibit System Recovery	Impact
T1489	Service Stop	Impact

Sources

Source	URL	Tier
	https://www.smdailyjournal.com/news/local/foster-city-hit-with-cybe...	T3
Foster City hit by ransomware attack, plans to declare state of ...	https://www.cbsnews.com/sanfrancisco/news/foster-city-cybersecurity...	T3
New details released after cyberattack paralyzes Bay Area city	https://www.sfgate.com/bayarea/article/bay-area-cyberattack-2208739...	T3
Cyberattack in Foster City shuts down many city services - YouTube	https://www.youtube.com/watch?v=4iJvGAMH8X8	T3
Foster City cyberattack: City to declare state of emergency - KRON4	https://www.kron4.com/news/technology-ai/peninsula-city-to-declare-...	T3

Generated 2026-03-29 18:37 UTC by TJS Security Command Center