INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-11 06:47 UTC

Ryuk Ransomware Operator Pleads Guilty: What the Conviction Means for Ransomware Accountability

THREAT ACTOR | LOW | CVSS 2.5

SCC Item ID	SCC-TAC-2026-0038
Type	Threat Actor
Severity	LOW
CVSS Base Score	2.5
Affected Products	U.S. companies targeted in Ryuk ransomware campaigns (2018-2021); specific victims not disclosed in available source material
Published	2026-07-10T13:46:10
Discovery Source	Rss

Executive Summary

A 34-year-old Armenian national pleaded guilty in U.S. federal court to charges related to hacking U.S. companies and deploying Ryuk ransomware, according to BleepingComputer. Ryuk was among the most destructive ransomware families of the 2018-2021 period, targeting hospitals, government entities, and enterprises via TrickBot and BazarLoader infections. This conviction is reported as a rare successful prosecution of a ransomware affiliate; its direct operational impact on current ransomware risk is limited, as Ryuk is largely dormant and its lineage is considered to have evolved into Conti.

Technical Analysis

Ryuk ransomware operated primarily from 2018 to 2021, typically delivered through TrickBot or BazarLoader initial access infections. Operators employed spearphishing (T1566, T1566.001) for initial access, used valid accounts (T1078) and SMB/lateral movement techniques (T1021, T1021.002) to traverse networks, executed commands via Windows Command Shell (T1059.003), and communicated over standard application-layer protocols (T1071.001). Prior to encryption (T1486), operators disabled backup and recovery mechanisms (T1490) and stopped services (T1489). Process injection (T1055) and obfuscation techniques (T1027) were used to evade defenses. No CVE or CWE identifiers are associated with this item; Ryuk exploited misconfigurations and credential access rather than specific software vulnerabilities. Ryuk's operational lineage is considered to have evolved into Conti. No active Ryuk infrastructure or new campaigns are indicated by the source material.

Action Checklist

1. Step 1: Containment. Although no active Ryuk campaign is indicated, if historical Ryuk IOCs appear in your environment, isolate affected endpoints immediately and block known TrickBot/BazarLoader C2 infrastructure at the perimeter. Consult FBI and CISA historical Ryuk advisories for IOC lists.
2. Step 2: Detection. Review endpoint and network logs for MITRE techniques associated with Ryuk: Windows Command Shell execution (T1059.003), SMB lateral movement (T1021.002), process injection events (T1055), and volume shadow copy deletion (T1490). Cross-reference against NIST AU-6 (Audit Record Review) to ensure logs are being actively reviewed for these indicators. CIS 8.2 (Collect Audit Logs) should be validated to confirm logging coverage across enterprise assets.
3. Step 3: Eradication. Ryuk is not an active threat requiring emergency remediation. If historical indicators are found, remove TrickBot/BazarLoader persistence mechanisms, rotate compromised credentials per D3-CRO (Credential Rotation), and enforce least privilege per NIST AC-6 (Least Privilege) to limit lateral movement paths.
4. Step 4: Recovery. Validate that multi-factor authentication is enforced on all remote access and administrative accounts per CIS 6.4 and CIS 6.5. Confirm backup integrity and test restoration procedures. Monitor for anomalous account activity (D3-LAM, Local Account Monitoring) post-remediation.
5. Step 5: Post-Incident. Use this conviction as a tabletop trigger. Review ransomware response playbooks against the Ryuk/Conti TTP chain. Assess gaps in phishing controls (NIST AC-17 for remote access restrictions), MFA coverage (D3-MFA), and user account permissions (D3-UAP). Document lessons learned against NIST IR controls.

IR / Forensic Enrichment

Triage Priority	DEFERRED
Escalation Criteria	Escalate to immediate priority if any TrickBot, BazarLoader, or Ryuk IOCs match active network traffic, endpoint telemetry, or file system artifacts — particularly if volume shadow copy deletion events (Windows Security Event ID 524 or Sysmon process creation for vssadmin.exe) are observed, as this indicates active pre-encryption staging; additionally, if affected systems include healthcare, critical infrastructure, or systems processing PHI/PII, engage legal counsel for HIPAA breach notification assessment.
Recovery Notes	Restore from the earliest backup predating confirmed TrickBot infection — not merely the Ryuk encryption event — because TrickBot operators establish persistent access days to weeks before deploying Ryuk, meaning more recent backups may contain active TrickBot implants or harvested credentials embedded in cached data. After restoration, enforce a mandatory credential rotation for all accounts with network logon capability before bringing systems back online, and monitor Windows Security Event ID 4624 (Type 3 network logons) and Event ID 4648 (explicit credential use) continuously for a minimum of 30 days, as Ryuk affiliates frequently return to previously compromised environments using cached credentials not discovered during initial eradication. Validate that all backup repositories are isolated from production SMB-accessible paths to prevent recurrence of Ryuk's documented backup destruction behavior.

Forensic Artifacts	TrickBot module directory in %APPDATA%\\ containing downloaded modules (e.g., systeminfo32.dll for credential harvesting, mailsearcher32.dll for email exfiltration) — TrickBot stores configuration and stolen credentials in subdirectories named after its functional modules | Windows Prefetch files (C:\Windows\Prefetch\) for WBADMIN.EXE, VSSADMIN.EXE, BCDEDIT.EXE, and the Ryuk binary dropper — prefetch records execution timestamp and file path, establishing the exact moment Ryuk's pre-encryption backup destruction sequence began | NTDS.dit and SYSTEM registry hive on domain controllers — TrickBot's shareDll module specifically targets Active Directory credential stores; presence of unauthorized access timestamps on NTDS.dit confirms domain-wide credential compromise preceding Ryuk deployment | Network flow logs (NetFlow/IPFIX) or Windows Firewall logs showing SMB (port 445) lateral movement from the initial TrickBot-infected host to additional workstations and servers — Ryuk uses harvested domain admin credentials to authenticate via SMB/WMI for ransomware staging across the network | Encrypted file extension survey across file shares and endpoints — Ryuk appends the .RYK extension to encrypted files and drops a ransom note named RyukReadMe.txt in each encrypted directory, providing a breadcrumb trail of the encryption sweep sequence and scope of data impact

Per-Action IR Details

Step 1: Containment — No active Ryuk campaign is indicated. If historical Ryuk IOCs appear in your environment, isolate affected endpoints immediately and block known TrickBot/BazarLoader C2 infrastructure at the perimeter. Consult FBI and CISA historical Ryuk advisories for IOC lists.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For teams without enterprise firewalls or NDR: use Windows Defender Firewall with Advanced Security (`netsh advfirewall`) to block known TrickBot/BazarLoader C2 IP ranges published in CISA Alert AA20-302A. On Linux perimeter hosts, apply `iptables -A OUTPUT -d -j DROP`. Run `netstat -ano` or `Get-NetTCPConnection` on suspected hosts and compare established connections against CISA Ryuk IOC lists before isolating.

Evidence: Before isolating any endpoint where Ryuk/TrickBot/BazarLoader activity is suspected, capture: (1) full RAM image using WinPmem or DumpIt to preserve TrickBot in-memory injection artifacts and Ryuk's process hollowing state; (2) live network connections via `Get-NetTCPConnection | Export-Csv` or `netstat -ano > netstat_capture.txt` to document active C2 beaconing to TrickBot infrastructure (typically HTTPS on 447/449 or custom ports); (3) running process list via `tasklist /v /fo csv > processes.csv` to capture BazarLoader loader processes before host isolation destroys live state.

Step 2: Detection — Review endpoint and network logs for MITRE techniques associated with Ryuk: Windows Command Shell execution (T1059.003), SMB lateral movement (T1021.002), process injection events (T1055), and volume shadow copy deletion (T1490). Cross-reference against NIST AU-6 (Audit Record Review, Analysis, and Reporting) requirements. CIS 8.2 (Collect Audit Logs) should be validated to confirm logging coverage across enterprise assets.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, deploy Sysmon with SwiftOnSecurity's config (minimum: Events 1, 3, 7, 8, 10, 11, 13) and query with PowerShell: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -match 'cmd.exe|wmic|vssadmin'}`. Use Sigma rule 'win_susp_vssadmin_delete_shadows' converted to PowerShell for volume shadow deletion detection. Query

Windows Security Log for Event ID 4688 (Process Creation) filtering on `vssadmin.exe delete shadows`, `wbadmin delete`, and `bcdedit /set recoveryenabled no` — all commands confirmed in Ryuk post-exploitation.

Evidence: Log sources and specific queries for Ryuk detection: (1) Windows Security Event Log — Event ID 4688 for `cmd.exe`, `powershell.exe`, `wmic.exe` spawned by `svchost.exe` or Office processes (TrickBot initial execution pattern); (2) Sysmon Event ID 3 for outbound SMB connections (port 445) from non-server workstations indicating Ryuk's SMB lateral movement; (3) Sysmon Event ID 8 (CreateRemoteThread) targeting `lsass.exe` from unexpected parent processes (TrickBot credential harvesting); (4) Windows System Event Log for Event ID 7045 (new service installed) — Ryuk registers a service named `MSWinSvc` or randomized variants; (5) VSS provider logs and Event ID 524 in System log confirming shadow copy deletion before encryption begins.

Step 3: Eradication — Ryuk is not an active threat requiring emergency remediation. If historical indicators are found, remove TrickBot/BazarLoader persistence mechanisms, rotate compromised credentials per D3-CRO (Credential Rotation), and enforce least privilege per NIST AC-6 (Least Privilege) to limit lateral movement paths.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without EDR for persistence hunting, use Autoruns (Sysinternals) to enumerate TrickBot's known persistence locations: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, scheduled tasks named with random strings in `C:\Users\\AppData\Roaming\`, and DLL side-loading in `%APPDATA%`. For BazarLoader, check for malicious DLLs registered via `HKLM\SYSTEM\CurrentControlSet\Services`. Run `reg query HKLM\SYSTEM\CurrentControlSet\Services /s | findstr /i ImagePath` and compare against known-good baselines. Rotate all domain admin credentials and service account passwords discovered in memory via TrickBot's credential harvesting module.

Evidence: Before removing TrickBot/BazarLoader persistence or rotating credentials, capture: (1) registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` to document persistence keys; (2) scheduled task XML exports via `schtasks /query /fo XML /v > schtasks_all.xml`; (3) full directory listing of `%APPDATA%`, `%TEMP%`, and `C:\ProgramData\` for TrickBot module files (typically named `.exe` or `_configs` directories); (4) copy of NTDS.dit and SYSTEM hive if domain controller compromise is suspected (TrickBot's `shareDll` module targets AD credential stores); (5) prefetch files from `C:\Windows\Prefetch\` for `WBADMIN.EXE`, `VSSADMIN.EXE`, and Ryuk dropper execution evidence.

Step 4: Recovery — Validate that multi-factor authentication is enforced on all remote access and administrative accounts per CIS 6.4 and CIS 6.5. Confirm backup integrity and test restoration procedures. Monitor for anomalous account activity (D3-LAM, Local Account Monitoring) post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 3.4 (Enforce Data Retention), NIST AC-17 (Remote Access)

Compensating: Without enterprise MFA solutions, enable Windows Hello for Business or enforce certificate-based authentication for RDP (Ryuk's primary lateral entry point after TrickBot establishes foothold). Validate backup integrity by restoring a test file from offline/air-gapped backup copies — Ryuk specifically targets network-accessible backup shares via SMB, so confirm backups are offline or immutable. Use `wevtutil qe Security /q:"*[System[(EventID=4624)] and EventData[Data[@Name='LogonType']='3']]"` to baseline and monitor for anomalous network logons post-recovery.

Evidence: Before restoring systems from backup, verify backup integrity has not been compromised by Ryuk's network share enumeration: (1) review backup server access logs for unauthorized SMB connections in the 72-hour window preceding the Ryuk encryption event (Ryuk operators routinely pre-stage backup destruction); (2) confirm backup files are not encrypted by checking file headers and attempting a test restore of a known-good file; (3) review Windows Security Event ID 4648 (explicit credential use) on backup servers to detect TrickBot-harvested credentials

used to access backup infrastructure; (4) document the last-known-good backup timestamp against the earliest confirmed TrickBot infection date to establish a safe restore point.

Step 5: Post-Incident — Use this conviction as a tabletop trigger. Review ransomware response playbooks against the Ryuk/Conti TTP chain. Assess gaps in phishing controls (NIST AC-17 for remote access restrictions), MFA coverage (D3-MFA), and user account permissions (D3-UAP). Document lessons learned against NIST IR controls.

NIST Phase: Post Incident

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

Controls: NIST AC-17 (Remote Access), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a 2-person tabletop using the publicly documented Ryuk/Conti TTP chain: TrickBot phishing lure → BazarLoader staging → Cobalt Strike beacon → Ryuk deployment (typically 1–3 days dwell time). Map each phase against your current detection coverage using free Atomic Red Team tests (T1059.003, T1021.002, T1490) to validate Sysmon and Windows Event Log detection gaps. Document findings in a lessons-learned report structured around NIST 800-61r3 §4.1 (Meeting with Stakeholders) and submit to leadership within 30 days of the tabletop.

Evidence: For lessons-learned documentation, gather and preserve: (1) aggregated TrickBot/BazarLoader IOCs from CISA Alert AA20-302A and FBI Flash CU-000142-MW for comparison against historical DNS, proxy, and firewall logs to determine if infrastructure was previously contacted; (2) audit of RDP and VPN authentication logs for the 90-day pre-tabletop window to identify accounts lacking MFA that would have been viable TrickBot lateral movement targets; (3) inventory of accounts with Domain Admin or backup operator privileges to quantify blast radius under a Ryuk scenario; (4) current Sysmon and Windows Event Log coverage gap analysis mapped against the Ryuk/Conti TTP chain to document detection blind spots before the next tabletop cycle.

Detection Guidance

Ryuk is not actively campaigning. For retrospective hunting or resilience validation, search endpoint telemetry for: deletion of volume shadow copies via vssadmin or wmic (T1490); SMB authentication events across non-standard host pairs (T1021.002); process injection anomalies into lsass.exe or svchost.exe (T1055); and obfuscated script execution from user directories (T1027). Network defenders should look for beaconing patterns consistent with TrickBot/BazarLoader C2 over HTTP/S (T1071.001). NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) should be in place to support this analysis. D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) are applicable countermeasures for ongoing detection posture. IOCs specific to this case are not available in the source material.

Framework Mappings

MITRE-ATTACK

- **T1059.003** — Windows Command Shell
- **T1071.001** — Web Protocols
- **T1566.001** — Spearphishing Attachment
- **T1490** — Inhibit System Recovery
- **T1021** — Remote Services
- **T1486** — Data Encrypted for Impact

- **T1489** — Service Stop
- **T1055** — Process Injection
- **T1021.002** — SMB/Windows Admin Shares
- **T1027** — Obfuscated Files or Information
- **T1078** — Valid Accounts
- **T1566** — Phishing

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)
- **CM-6** — Configuration Settings
- **AC-6** — Least Privilege
- **AC-2** — Account Management
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **IR-4** — Incident Handling

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059.003	Windows Command Shell	Execution
T1071.001	Web Protocols	Command-And-Control

Technique ID	Technique Name	Tactic
T1566.001	Spearphishing Attachment	Initial-Access
T1490	Inhibit System Recovery	Impact
T1021	Remote Services	Lateral-Movement
T1486	Data Encrypted for Impact	Impact
T1489	Service Stop	Impact
T1055	Process Injection	Defense-Evasion
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1027	Obfuscated Files or Information	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/ryuk-ransomware-memb...	T2
Vulnerability In Apache Commons Text Library	https://northwave-cybersecurity.com/threat-response/vulnerability-i...	T3
Security Notice: Apache commons-text vulnerability (CVE-2022 ...	https://support.xmatters.com/hc/en-us/articles/13843436346139-Secur...	T3
CVE-2022-42889 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2022-42889	T1
Apache Commons Text Vulnerability Security | Layer7 API ...	https://community.broadcom.com/discussion/apache-commons-text-vulne...	T3

Generated 2026-07-11 06:47 UTC by TJS Security Command Center