INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-06 05:47 UTC

Germany Names REvil and GandCrab Operator: Daniil Shchukin Identified as 'UNKN' After Years of Anonymity

THREAT ACTOR | HIGH | CVSS 7.5

SCC Item ID	SCC-TAC-2026-0004
Type	Threat Actor
Severity	HIGH
CVSS Base Score	7.5
Affected Products	No specific products; enterprise victims across 130+ confirmed incidents globally spanning REvil and GandCrab RaaS campaigns
Published	2026-04-05T22:07:17
Discovery Source	Rss

Executive Summary

German federal police (BKA) have publicly identified Daniil Maksimovich Shchukin, alias 'UNKN,' as a principal operator of both GandCrab and REvil ransomware-as-a-service platforms, linking him to 130+ confirmed extortion incidents globally. REvil is responsible for the 2021 Kaseya VSA supply chain attack and the JBS Foods compromise, representing some of the most disruptive ransomware campaigns of the last decade. Given historical Russian non-extradition policy for cybercrime cases, immediate arrest is unlikely, but the attribution signals continued international pressure on RaaS infrastructure and may disrupt operational trust within the broader REvil affiliate network.

Technical Analysis

Daniil Maksimovich Shchukin (DOB unconfirmed publicly; reported age 31) operated as 'UNKN,' a core administrator and recruiter for GandCrab (active approx. 2018-2019) and its successor REvil/Sodinokibi. GandCrab pioneered the affiliate RaaS model at scale and is estimated by security researchers to have extorted hundreds of millions of dollars in ransom payments before operators declared retirement in 2019. REvil inherited infrastructure, code lineage, and affiliate relationships. REvil's most significant operations include the Kaseya VSA supply chain compromise (July 2021, CVE-2021-30116) affecting 1,500+ downstream organizations, and the JBS Foods attack (June 2021) resulting in an $11 million ransom payment. Relevant MITRE ATT&CK techniques across REvil campaigns include: T1195 (Supply Chain Compromise, Kaseya vector), T1566 (Phishing, initial access in enterprise campaigns), T1078 (Valid Accounts, credential abuse post-access), T1059

(Command and Scripting Interpreter, payload execution), T1570 (Lateral Tool Transfer), T1486 (Data Encrypted for Impact, ransomware payload), T1490 (Inhibit System Recovery, VSS deletion), T1489 (Service Stop, security tool termination), T1041/T1071 (exfiltration and C2 channels), T1567 (Exfiltration to cloud, double extortion), T1219 (Remote Access Tools, persistence), T1588.005 (Exploits acquired for affiliate use). CWE references: CWE-693 (Protection Mechanism Failure) and CWE-284 (Improper Access Control) reflect the control gaps consistently exploited across victim environments. Attribution methodology per BKA likely involved blockchain financial forensics, OPSEC failures over multi-year operational exposure, and coordination with Europol and partner agencies. No patch or vendor advisory applies; this is a threat actor attribution, not a vulnerability disclosure. REvil core infrastructure was disrupted in late 2021 following coordinated law enforcement action (U.S. DOJ, Europol), but affiliate tooling and TTPs remain in active use by successor groups.

Action Checklist

1. Step 1: Containment. Review your ransomware blast radius controls now. Confirm network segmentation isolates backup infrastructure from production. Verify that VSS (Volume Shadow Copy) deletion is blocked or alerted via endpoint controls. If you use any RMM or VSA-type tooling, confirm it is fully patched and access is restricted to known IP ranges with MFA enforced.
2. Step 2: Detection. Hunt for REvil/Sodinokibi indicators across endpoint and network telemetry using historical IOCs from the 2021 Kaseya campaign (primary detection basis). No new IOCs were published with this attribution. Query EDR for known REvil execution patterns: PowerShell with encoded commands, vssadmin.exe delete shadows, bcdedit.exe /set recoveryenabled no, and wbadmin delete catalog. Review SIEM for T1078 anomalies (valid accounts used at unusual hours or from unusual geolocations). Refer to the BKA wanted notice for any updated information.
3. Step 3: Eradication. No active patch action required for this attribution event. If historical REvil exposure is identified in your environment, consult CISA's official Kaseya VSA advisory for detailed remediation steps. Remove any identified persistence mechanisms: scheduled tasks, registry run keys, and remote access tools dropped by REvil payloads. Rotate all credentials for accounts active during any suspected compromise window.
4. Step 4: Recovery. Validate backup integrity and confirm backups are air-gapped or immutable. Test restoration procedures for critical systems. Monitor for re-infection indicators for 30 days post-remediation, particularly lateral movement patterns and any reappearance of known REvil file extensions or ransom note artifacts. Confirm security tooling (EDR, backup agents) is fully operational and not in a degraded state from prior tampering.
5. Step 5: Post-Incident. This attribution is a signal event, not a new attack. Use it to pressure-test your ransomware controls against documented REvil TTPs mapped above. Specific control gaps to assess: MFA coverage on remote access and admin accounts (T1078), supply chain vendor security review processes (T1195), immutable backup enforcement (T1490), and RMM tool access restriction policies. If your organization was a GandCrab or REvil victim and has not conducted a full post-incident review, this attribution may surface new forensic context worth revisiting with your IR team.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if any of the following are confirmed: (1) Kaseya VSA or similar RMM agent was installed and unpatched during July 2–5, 2021; (2) REvil ransom note artifacts or encrypted file extensions are discovered in the environment; (3) Evidence of data exfiltration (outbound bulk transfers, C2 beaconing) is identified during the detection hunt — triggering breach notification assessment under GDPR (72-hour), CCPA, or HIPAA given REvil's documented double-extortion exfiltration of sensitive data prior to encryption.
Recovery Notes	Before returning any system to production, verify that all VSA agent instances are removed or patched to version 9.5.7a or later (per Kaseya advisory KSA-2021-001), all credentials active during the suspected compromise window are rotated, and immutable backup integrity is confirmed via hash validation against pre-incident baselines. Monitor all recovered endpoints for 30 days using Sysmon Event IDs 1, 3, and 11 for re-appearance of REvil execution indicators (vssadmin.exe, bcdedit.exe, randomized-extension file creation events), as REvil affiliates have historically re-compromised organizations that did not fully eradicate the initial access vector. Given BKA's public attribution confirming REvil operational continuity, treat the RaaS platform as an active threat and do not reduce monitoring posture after the 30-day window without a documented risk acceptance decision.
Forensic Artifacts	Kaseya VSA IIS access logs (C:\inetpub\logs\LogFiles\) — contain POST requests to the specific URI paths (/dl.asp, /userFilterTableGetContents.asp) exploited in CVE-2021-30116 to deliver the malicious agent.crt payload to managed endpoints; timestamps establish initial access time precisely | Windows Prefetch files for VSSADMIN.EXE, BCDEDIT.EXE, and WBADMIN.EXE (C:\Windows\Prefetch\) — execution timestamps confirm when REvil's recovery inhibition routine ran relative to encryption onset, establishing the attack timeline and confirming pre-encryption staging | REvil ransom note files named '[random_hex]-readme.txt' and encrypted files with randomized 5-8 character extensions scattered across network shares — file system metadata (MFT entry timestamps, USN journal entries) reconstructs the encryption sweep sequence and identifies the originating host | Windows Security Event Log Event ID 4688 (Process Creation with command-line logging enabled) showing KaseyaAgentMon.exe or AgentMon.exe as parent process spawning PowerShell.exe with -enc arguments — this parent-child process relationship is the forensic signature of REvil delivery via the Kaseya VSA trusted execution context | Memory image from any host where REvil execution is suspected but encryption had not fully completed — REvil holds the symmetric AES file encryption keys in process memory until the master key is exfiltrated to C2; a timely memory capture may enable key recovery and decryption without paying ransom, and is also required to recover the embedded JSON config blob containing C2 addresses and affiliate ID

Per-Action IR Details

Step 1: Containment — Review your ransomware blast radius controls now. Confirm network segmentation isolates backup infrastructure from production. Verify that VSS (Volume Shadow Copy) deletion is blocked or alerted via endpoint controls. If you use any RMM or VSA-type tooling, confirm it is fully patched and access is restricted to known IP ranges with MFA enforced.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Choose a containment strategy based on the type of incident; criteria include potential damage, evidence preservation, and service availability.

Controls: NIST IR-4 (Incident Handling) — implement containment consistent with the incident response plan, NIST SC-7 (Boundary Protection) — monitor and control communications at external and internal network boundaries to isolate backup VLAN from production segments, NIST SI-7 (Software, Firmware, and Information Integrity) — employ integrity verification to detect unauthorized VSS deletion or tampering by REvil pre-encryption routines, CIS 4.4

(Implement and Manage a Firewall on Servers) — enforce host-based firewall rules preventing lateral movement from RMM-connected endpoints to backup infrastructure, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA on all VSA-type RMM portals; REvil's Kaseya VSA attack (July 2021) exploited authenticated management interfaces to push malicious updates

Compensating: For teams without enterprise NAC or micro-segmentation: (1) Use Windows Firewall with Advanced Security (wf.msc) to create an inbound rule on backup servers blocking all traffic except from your designated backup management subnet — deploy via GPO. (2) Run 'vssadmin list shadows' on critical hosts via PowerShell and establish a baseline; schedule a daily Task Scheduler job running 'vssadmin list shadows >> C:\logs\vss_audit.txt' and diff against baseline to detect deletions. (3) Deploy Sysmon with SwiftOnSecurity config — Event ID 1 will capture vssadmin.exe and bcdedit.exe process creation with full command-line arguments. (4) If running Kaseya VSA or similar RMM, verify the agent service account has no local admin rights beyond what is required and restrict the management port (default TCP 443/5721) at the perimeter firewall to a named admin IP allowlist.

Evidence: BEFORE isolating or reconfiguring any segment, capture: (1) Windows Security Event Log Event ID 4625/4624 on RMM servers showing authentication attempts and source IPs — REvil's Kaseya entry point involved exploitation of the VSA web interface from external IPs bypassing authentication (CVE-2021-30116). (2) Sysmon Event ID 3 (Network Connection) logs from VSA agent processes to detect C2 beacon patterns REvil used post-exploitation (historically Cloudflare CDN IPs and onion domains). (3) Current VSS snapshot inventory via 'vssadmin list shadows /for=C:' on all production hosts — document snapshot IDs and creation timestamps as pre-containment baseline to confirm whether REvil's pre-encryption wiper has already executed. (4) RMM server IIS access logs (typically C:\inetpub\logs\LogFiles\) for POST requests to /dl.asp, /userFilterTableGetContents.asp, and /cgi-bin/ paths exploited in the Kaseya VSA compromise.

Step 2: Detection — Hunt for REvil/Sodinokibi indicators across endpoint and network telemetry. Query EDR for known REvil execution patterns: PowerShell with encoded commands, vssadmin.exe delete shadows, bcdedit.exe /set recoveryenabled no, and wbadmin delete catalog. Review SIEM for T1078 anomalies (valid accounts used at unusual hours or from unusual geolocations). Cross-reference threat intel feeds against the BKA wanted notice (https://www.bka.de/DE/IhreSicherheit/Fahndungen/Personen/BekanntePersonen/CC_BW/DMS/Sachverhalt.html) for any published IOCs. Note: no new IOCs were released with this attribution; historical REvil IOCs from the 2021 Kaseya campaign remain the primary detection basis.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Use indicators of compromise, log analysis, and threat intelligence to identify the scope and nature of the incident.

Controls: NIST SI-4 (System Monitoring) — monitor systems to detect attacks and indicators of potential compromise including REvil-specific execution chains, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review and analyze system audit records for REvil staging behaviors including encoded PowerShell, shadow copy deletion, and backup catalog removal, NIST IR-5 (Incident Monitoring) — track and document all identified REvil/GandCrab indicators, correlating across endpoints touched by VSA agents during the Kaseya campaign window (July 2–5, 2021), NIST SI-5 (Security Alerts, Advisories, and Directives) — consume and operationalize the BKA attribution notice and CISA AA21-200A advisory IOCs as detection inputs, CIS 8.2 (Collect Audit Logs) — ensure logging is enabled on all endpoints that had VSA agents installed, covering the 2021 compromise window and current activity, MITRE ATT&CK T1078 (Valid Accounts) — hunt for REvil's use of legitimate domain credentials post-exploitation for lateral movement, MITRE ATT&CK T1490 (Inhibit System Recovery) — detect vssadmin.exe, bcdedit.exe, and wbadmin invocations characteristic of REvil pre-encryption staging, MITRE ATT&CK T1059.001 (PowerShell) — detect encoded PowerShell commands used by REvil dropper and MBR wiper components

Compensating: Without SIEM/EDR, execute this hunt manually: (1) PowerShell on each endpoint: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4688,4624,4625,4648)} | Export-Csv C:\hunt\auth_events.csv' — filter 4688 records for Image paths containing vssadmin.exe, bcdedit.exe, wbadmin.exe, or PowerShell.exe with CommandLine containing '-enc' or '-encoded'. (2) Deploy the free Sigma rule 'proc_creation_win_vssadmin_delete_shadows.yml' (SigmaHQ GitHub) converted to Windows Event Log XML queries and run via wevtutil.exe. (3) Use YARA rule from CISA AA21-200A IOC package against memory dumps and disk images of any VSA-connected host: 'yara -r revil_kaseya.yar C:\' (4) For T1078 hunting without SIEM: export Security log 4624 events to CSV and use PowerShell 'Group-Object' to identify accounts authenticating from >2 distinct source

IPs or outside business hours. (5) Check scheduled tasks on all endpoints: 'schtasks /query /fo LIST /v > C:\hunt\tasks.txt' and grep for tasks created in the July 2021 window or with actions referencing temp paths.

Evidence: Capture before any remediation: (1) Windows Security Event Log Event ID 4688 (Process Creation, with command-line auditing enabled) on all hosts — specifically filter for parent process being the Kaseya VSA agent service (KaseyaAgentMon.exe or AgentMon.exe) spawning cmd.exe or PowerShell.exe, which is the precise execution chain REvil used in the Kaseya supply chain attack. (2) Windows Security Event ID 4648 (Explicit Credential Use) showing the REvil affiliate's lateral movement using harvested credentials. (3) Prefetch files (C:\Windows\Prefetch\) for VSSADMIN.EXE-*.pf, BCDEDIT.EXE-*.pf, and WBADMIN.EXE-*.pf — timestamps confirm when recovery inhibition commands executed relative to encryption onset. (4) REvil drops a ransom note named '[random]-readme.txt' and appends a random 5-8 character extension to encrypted files — search recursively: 'Get-ChildItem -Recurse -Filter "*-readme.txt"'. (5) MFT ($MFT) artifacts and USN journal ($UsnJrnl:$J) from affected volumes to reconstruct the exact file encryption sequence and identify Patient Zero host.

Step 3: Eradication — No active patch action required for this attribution event. If historical REvil exposure is identified in your environment, follow the CISA advisory on the Kaseya VSA compromise (https://www.cisa.gov/news-events/alerts — search Kaseya VSA). Remove any identified persistence mechanisms: scheduled tasks, registry run keys, and remote access tools dropped by REvil payloads. Rotate all credentials for account active during any suspected compromise window.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: After containing the incident, eradicate the cause by deleting malware, disabling breached accounts, and identifying and mitigating all exploited vulnerabilities.

Controls: NIST IR-4 (Incident Handling) — eradication must address all identified persistence mechanisms before recovery begins, NIST SI-2 (Flaw Remediation) — for any Kaseya VSA instances still in inventory, apply patches addressing CVE-2021-30116, CVE-2021-30119, and CVE-2021-30120 per Kaseya advisory KSA-2021-001; confirm patch version 9.5.7a or later, NIST SI-3 (Malicious Code Protection) — scan all VSA-connected endpoints for REvil dropper artifacts: the malicious 'agent.crt' file delivered via VSA update mechanism and the legitimate-but-weaponized 'MsMpEng.exe' / 'mpsvc.dll' sideloading pair used to evade detection, NIST CM-7 (Least Functionality) — remove RMM agent software from any hosts that no longer require managed services; REvil leveraged the trusted VSA agent execution context to bypass application whitelisting, CIS 5.3 (Disable Dormant Accounts) — disable all service and admin accounts active on VSA infrastructure during the compromise window; REvil affiliates establish persistence via new local admin accounts (check for accounts created July 2–5, 2021 on impacted hosts)

Compensating: For teams without enterprise credential management or EDR-based remediation: (1) Persistence sweep via reg.exe: 'reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and 'reg query HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' on all impacted hosts — REvil drops persistence under randomized key names; compare against a known-good baseline. (2) Scheduled task audit: 'schtasks /query /fo CSV /v | ConvertFrom-Csv | Where-Object {$_."Task To Run" -match "temp|appdata|public"}' — REvil commonly stages payloads in %TEMP% and %PUBLIC%. (3) Credential rotation: use 'net user' to enumerate local accounts created during the suspected compromise window and disable unknowns; for AD, use 'Get-ADUser -Filter {WhenCreated -gt "07/01/2021"} | Select Name,WhenCreated,Enabled'. (4) For the specific DLL sideloading pair (MsMpEng.exe + mpsvc.dll): search 'Get-ChildItem -Recurse -Filter "mpsvc.dll" | Where-Object {$_.DirectoryName -notmatch "Windows Defender"}' — any hit outside the legitimate Defender path is an indicator.

Evidence: Preserve before eradicating persistence: (1) Full registry hive exports (HKLM\SYSTEM, HKLM\SOFTWARE, HKCU) from all impacted endpoints using 'reg export' — captures REvil's Run key persistence and any registry-based configuration the ransomware stores (REvil uses a base64-encoded JSON config embedded in HKLM\SOFTWARE\\[random_key]). (2) Copy all scheduled task XML definitions from C:\Windows\System32\Tasks\ before deletion — these serve as forensic evidence of attacker-created persistence. (3) Memory image (via WinPmem or Magnet RAM Capture) of any host where REvil execution is confirmed but encryption has not yet completed — REvil stores its symmetric file encryption keys in memory prior to exfiltrating the master key to the C2 server; a memory image taken before shutdown may allow key recovery. (4) Full disk image of Patient Zero VSA server before wipe using FTK Imager — preserve the malicious 'agent.crt' artifact and VSA database for legal hold given BKA's active prosecution interest in Shchukin.

Step 4: Recovery — Validate backup integrity and confirm backups are air-gapped or immutable. Test restoration procedures for critical systems. Monitor for re-infection indicators for 30 days post-remediation, particularly lateral movement patterns and any reappearance of known REvil file extensions or ransom note artifacts. Confirm security tooling (EDR, backup agents) is fully operational and not in a degraded state from prior tampering.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore systems to normal operation, confirm systems are functioning normally, and implement controls to prevent recurrence.

Controls: NIST CP-9 (System Backup) — verify backup copies are stored offline or in an immutable store; REvil specifically targets network-accessible backups including Veeam repositories and Windows Backup catalog (wbadmin delete catalog) before triggering encryption, NIST SI-7 (Software, Firmware, and Information Integrity) — verify integrity of restored systems against known-good baselines; REvil's DLL sideloading technique (mpsvc.dll) may persist in restored images if backup predates detection but postdates compromise, NIST IR-4 (Incident Handling) — recovery must include verification that all identified persistence mechanisms were eradicated before systems return to production, NIST AU-9 (Protection of Audit Information) — validate that audit logging infrastructure itself was not tampered with; REvil affiliates have cleared Windows Event Logs (Event ID 1102 — Audit Log Cleared) as an anti-forensics step prior to encryption, CIS 7.2 (Establish and Maintain a Remediation Process) — document all recovery actions with timestamps; required if this incident triggers breach notification obligations under GDPR, CCPA, or HIPAA given REvil's history of data exfiltration prior to encryption

Compensating: For teams restoring from backup without enterprise backup validation tooling: (1) Hash validation of restored system binaries: after restore, run 'Get-FileHash C:\Windows\System32*.exe -Algorithm SHA256 | Export-Csv hashes.csv' and compare against Microsoft's known-good hash values from the NVD or vendor. (2) Confirm backup agent integrity before trusting backup data: check the backup agent binary's digital signature via 'Get-AuthenticodeSignature'. (3) Post-recovery re-infection monitoring without EDR: deploy Sysmon with network logging (Event ID 3) and configure alerts for any outbound connection to Tor exit nodes or known REvil C2 IP ranges published in CISA AA21-200A. (4) Set a 30-day cron/Task Scheduler job running daily: 'Get-ChildItem -Recurse -Filter "*-readme.txt" | Export-Csv C:\monitor\ransomnote_scan.csv' and 'Get-ChildItem -Recurse | Where-Object {$_.Extension.Length -eq 8 -and $_.Extension -match "^\.[a-z0-9]{5,8}$"}' to catch re-encryption attempts by REvil's randomized extension pattern.

Evidence: Capture before and during recovery: (1) Windows Security Event ID 1102 (Audit Log Cleared) and 104 (System Log Cleared) — REvil affiliates routinely clear logs as final anti-forensics step; the presence or absence of these events across the timeline is itself a forensic finding. (2) Veeam or Windows Server Backup job history logs — document whether backup deletion via wbadmin or direct Veeam DB manipulation succeeded, partially succeeded, or failed; this determines recovery scope. (3) Network flow records (NetFlow/IPFIX) or firewall logs covering the 72-hour window before encryption onset — REvil exfiltrates data via HTTP POST to C2 prior to encryption (MITRE T1041); these flows establish data exfiltration scope for breach notification analysis. (4) Post-restore integrity check output — hash comparison results serve as documented evidence that recovered systems are clean, required for any regulatory notification or cyber insurance claim.

Step 5: Post-Incident — This attribution is a signal event, not a new attack. Use it to pressure-test your ransomware controls against documented REvil TTPs mapped above. Specific control gaps to assess: MFA coverage on remote access and admin accounts (T1078), supply chain vendor security review processes (T1195), immutable backup enforcement (T1490), and RMM tool access restriction policies. If your organization was a GandCrab or REvil victim and has not conducted a full post-incident review, this attribution may surface new forensic context worth revisiting with your IR team.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Hold a lessons-learned meeting, produce an incident report, retain evidence, and use findings to improve the IR program and preventive controls.

Controls: NIST IR-4 (Incident Handling) — lessons-learned output should update the ransomware IR playbook with REvil-specific TTP detections and containment triggers, NIST IR-8 (Incident Response Plan) — if REvil/GandCrab

victimization is confirmed, update the IR plan to reflect supply chain attack vectors (T1195) and RMM-delivered ransomware scenarios, NIST RA-3 (Risk Assessment) — reassess organizational risk in light of BKA attribution confirming REvil operational continuity under Shchukin/UNKN; the RaaS platform remains active despite law enforcement pressure, NIST SA-12 (Supply Chain Protection) — formalize vendor security review process for all RMM and managed service providers; the Kaseya VSA incident demonstrated that a single RMM platform can serve as a ransomware delivery vehicle to thousands of downstream MSP clients simultaneously, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate REvil-affiliated RaaS TTPs into the vulnerability management program's threat model, specifically targeting RMM software, VPN appliances (T1133), and AD exploitation paths (T1078.002), CIS 6.3 (Require MFA for Externally-Exposed Applications) — BKA attribution confirms UNKN-led REvil operations consistently exploited MFA gaps on externally-exposed admin panels; close this gap as priority one post-incident action, MITRE ATT&CK T1195.002 (Compromise Software Supply Chain) — document the supply chain attack vector in the lessons-learned report as a standing threat model input for future vendor risk assessments, MITRE ATT&CK T1490 (Inhibit System Recovery) — validate that immutable backup controls would have survived a REvil attack; test by attempting a backup deletion with a standard user account to confirm controls block the action

Compensating: For organizations without a formal GRC platform or threat modeling tool: (1) Use the free CISA Ransomware Readiness Assessment (RRA) tool (available at cisa.gov/resources-tools/services/ransomware-readiness-assessment) to self-assess against REvil-relevant controls — the RRA maps directly to the NIST CSF and covers backup integrity, MFA, and RMM security. (2) Run a tabletop exercise using the CISA/MS-ISAC Ransomware Guide scenario template, substituting the Kaseya VSA supply chain attack as the scenario seed — walk through how your organization would detect the VSA agent executing malicious updates. (3) Map your RMM vendor list against CISA's Known Exploited Vulnerabilities catalog (cisa.gov/known-exploited-vulnerabilities-catalog) to identify unpatched RMM CVEs; this is a free, manual, 2-person exercise. (4) Publish threat intel context from the BKA attribution internally using a structured format (STIX/TAXII is optional — even a formatted email with UNKN aliases, affiliated RaaS platforms, and historical IOC hashes from CISA AA21-200A serves as actionable staff awareness).

Evidence: Retain and archive for post-incident review: (1) All forensic images, memory captures, and log exports collected during the incident — NIST 800-61r3 §4 and legal counsel may require retention for insurance claims or regulatory reporting given REvil's confirmed data exfiltration capability (double extortion model). (2) Timeline reconstruction document linking UNKN/Shchukin's known GandCrab and REvil operational periods (2018–2021) against your organization's vulnerability exposure windows — if you ran unpatched Kaseya VSA during July 2021 or unpatched RDP/VPN during 2019–2021 GandCrab campaigns, document the exposure window for regulatory purposes. (3) Network flow records and DNS query logs covering any historical periods of suspected REvil dwell time — REvil affiliates typically maintained 5–10 days of dwell time for reconnaissance and data exfiltration before triggering encryption; these logs may reveal exfiltration scope previously unidentified. (4) Credential audit export showing which service and admin accounts were active during the compromise window — required for breach notification analysis if PII or PHI was accessible to those accounts.

Detection Guidance

No new IOCs were published alongside this attribution. Detection guidance is based on documented REvil/GandCrab TTPs. Key behavioral indicators: (1) vssadmin.exe or wmic.exe executing shadow copy deletion commands, alert on any instance in production environments; (2) bcdedit.exe with /set recoveryenabled no or /set bootstatuspolicy ignoreallfailures arguments; (3) PowerShell or cmd.exe spawned from unusual parent processes (Office apps, web servers, RMM agents); (4) Rapid file extension changes across multiple directories (REvil appends a random 8-character extension); (5) Ransom note files named in pattern [random]-readme.txt written to multiple directories simultaneously; (6) Outbound connections to Tor exit nodes or known double-extortion leak site infrastructure (historical example: happy-blog[.]su, confirmed offline as of 2021, provided for reference; validate current REvil affiliate leak domains against threat intelligence feeds before blocking). Log sources to prioritize: Windows Security Event Log (Event ID 4688 for process creation with command-line logging enabled), Sysmon (Event IDs 1, 3, 11), EDR process tree telemetry, and DNS/proxy logs

for C2 beacon patterns. For supply chain exposure (T1195/Kaseya vector), audit third-party RMM and VSA tool access logs for anomalous API calls or credential reuse. Refer to the MITRE ATT&CK Navigator and MITRE CTI GitHub repository for community-contributed REvil technique mappings to validate detection coverage.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`happy-blog[.]su`	Historical REvil double-extortion leak site. Defanged. Verify current resolution status before actioning; site may be inactive following 2021 law enforcement disruption.	LOW
URL	`https://www.bka.de/DE/IhreSicherheit/Fahndungen/Personen/BekanntePersonen/CC_BW/DMS/Sachverhalt.html`	BKA official wanted notice for Daniil Maksimovich Shchukin (UNKN). Primary attribution source. Check for published IOCs or updated case details.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1567** — Exfiltration Over Web Service
- **T1489** — Service Stop
- **T1071** — Application Layer Protocol
- **T1041** — Exfiltration Over C2 Channel
- **T1059** — Command and Scripting Interpreter
- **T1570** — Lateral Tool Transfer
- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts
- **T1219** — Remote Access Tools
- **T1490** — Inhibit System Recovery
- **T1588.005** — Exploits
- **T1195** — Supply Chain Compromise
- **T1566** — Phishing

NIST-800-53R5

- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection

- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1489	Service Stop	Impact
T1071	Application Layer Protocol	Command-And-Control
T1041	Exfiltration Over C2 Channel	Exfiltration
T1059	Command and Scripting Interpreter	Execution
T1570	Lateral Tool Transfer	Lateral-Movement
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion
T1219	Remote Access Tools	Command-And-Control
T1490	Inhibit System Recovery	Impact
T1588.005	Exploits	Resource-Development
T1195	Supply Chain Compromise	Initial-Access
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bka.de/DE/IhreSicherheit/Fahndungen/Personen/BekanntePe.. .	T3
Vulnerability Summary for the Week of August 18, 2025 | CISA	https://www.cisa.gov/news-events/bulletins/sb25-237	T1
Blumira Product Updates Timeline	https://www.blumira.com/product-updates	T3
[PDF] Department of Corrections Contract No. K11720	https://doc.wa.gov/sites/default/files/2025-02/K11720.pdf	T1
Microsoft Patches 130 Vulnerabilities, Including Critical Flaws in ...	https://thehackernews.com/2025/07/microsoft-patches-130-vulnerabili...	T3

Generated 2026-04-06 05:47 UTC by TJS Security Command Center