INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-07 06:06 UTC

BKA Names GandCrab and REvil Leadership: Attribution Milestone With Limited Operational Urgency

THREAT ACTOR | MEDIUM | CVSS 5.0

SCC Item ID	SCC-TAC-2026-0006
Type	Threat Actor
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	No specific products affected; historical victims include organizations using Kaseya VSA, Acer, and Texas local government entities (2019-2021 campaign window)
Published	2026-04-06T19:54:04
Discovery Source	Rss

Executive Summary

Germany's Federal Criminal Police Office (BKA) has publicly identified Daniil Maksimovich Shchukin and Anatoly Sergeevitsch Kravchuk as the operators behind the GandCrab and REvil ransomware-as-a-service operations, which were responsible for at least 130 extortion cases in Germany and estimated damages exceeding $40 million USD during their 2019-2021 active window. Both individuals are believed to reside in Russia, making near-term prosecution unlikely. This development carries no immediate operational risk for most organizations; it represents an attribution milestone with long-term value for international law enforcement coordination rather than an active threat requiring defensive action.

Technical Analysis

REvil (Sodinokibi) and its predecessor GandCrab operated as ransomware-as-a-service platforms, recruiting affiliates who conducted intrusions while the core group managed infrastructure, encryptors, and ransom negotiations. The most technically significant event attributed to this lineage is the July 2021 Kaseya VSA supply chain attack (CVE-2021-30116), in which REvil affiliates exploited an authentication bypass and arbitrary file upload vulnerability in on-premises Kaseya VSA servers to push a malicious update to downstream managed service provider (MSP) customers, affecting an estimated 800-1,500 businesses. MITRE ATT&CK techniques associated with this group's operations include: T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain), T1566 (Phishing), T1083 (File and Directory Discovery), T1041

(Exfiltration Over C2 Channel), T1489 (Service Stop), T1219 (Remote Access Software), T1490 (Inhibit System Recovery), T1486 (Data Encrypted for Impact), and T1657 (Financial Theft). No CVEs or active exploits are newly disclosed by this BKA attribution announcement. Both operations are assessed dormant since 2021. No patches, vendor advisories, or CWE classifications are associated with this specific intelligence item.

Action Checklist

1. Review posture, confirm that Kaseya VSA on-premises instances in your environment are patched against CVE-2021-30116 and are running a supported, up-to-date version; this vulnerability was the primary REvil supply chain vector and should have been remediated in 2021 per CISA guidance
2. Detection, query SIEM and EDR logs for historical REvil/GandCrab IOCs if threat hunting backlogs exist; search for known REvil file extensions (.sodinokibi, random-extension appended), ransom note filenames (e.g., [random]-readme.txt), and registry persistence keys associated with Sodinokibi; cross-reference against prior CISA and FBI REvil IOC releases
3. Eradication, no new active threat vector to remediate; if legacy REvil/GandCrab IOCs are found during retrospective hunting, isolate affected hosts, revoke potentially compromised credentials, and initiate standard incident response procedures
4. Recovery, validate backup integrity and offline backup availability for systems historically managed by MSPs using Kaseya VSA; confirm MSP vendor security posture if third-party managed services are in scope
5. Post-incident controls, use this attribution event as a prompt to review third-party and supply chain risk management controls, specifically software update validation for RMM and MSP tooling; map current detection coverage against T1195.002 and T1486 in your ATT&CK coverage assessment

IR / Forensic Enrichment

Triage Priority	DEFERRED
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if retrospective hunting (step 2) surfaces confirmed REvil/GandCrab IOCs — encrypted files, ransom notes, or Sodinokibi registry artifacts — in the environment, as this constitutes a historical breach potentially triggering state breach notification obligations for PII/PHI present on affected systems and may require cyber insurance notification within policy-mandated timeframes.
Recovery Notes	Recovery focus is retrospective validation, not active restoration: confirm all Kaseya VSA on-premises instances are patched to the post-CVE-2021-30116 version and verify no residual Sodinokibi persistence exists on endpoints previously managed by VSA agents deployed between July 2–5, 2021. Monitor restored systems for 30 days post-validation using Sysmon Event ID 13 (Registry Value Set) and Windows Security Event ID 4663 (Object Access) for any re-emergence of REvil's random-key registry persistence pattern, which has been observed in environments where eradication was incomplete. Retain all forensic artifacts — particularly the VSA SQL audit log and any memory captures — for a minimum of 12 months given the active law enforcement investigation context established by the BKA attribution announcement.

Forensic Artifacts	Kaseya VSA IIS access logs (`C:\inetpub\logs\LogFiles\`) containing anomalous POST requests to `/dl.asp` and `/userFilterTableRpt.asp` during July 2–5, 2021 — direct forensic evidence of CVE-2021-30116 exploitation used by REvil as the initial supply chain access vector | Kaseya VSA SQL Server audit database recording all agent procedure deployments — documents which managed endpoints received the malicious `agent.crt` dropper pushed by REvil via the compromised VSA update mechanism (MITRE T1072) | Windows VSS event log (Event ID 8193) and Sysmon Event ID 1 logs showing `vssadmin.exe delete shadows /all /quiet` execution — REvil's pre-encryption shadow copy destruction, present on every endpoint where encryption was initiated (MITRE T1490) | File system artifacts: files with random 5–10 character appended extensions and `[random]-readme.txt` ransom notes, alongside the Sodinokibi encrypted configuration blob in `HKCU\SOFTWARE\[random_alphanumeric]` registry key — unique to the REvil/Sodinokibi payload and distinguishable from GandCrab artifacts by the registry key structure | Memory forensics (WinPmem dump) of hosts where `MsMpEng.exe` or `explorer.exe` showed anomalous child processes — required to recover injected Sodinokibi shellcode and confirm whether the REvil affiliate used the `salsa20` encryption key material still present in process memory if the host was not fully rebooted post-infection (MITRE T1055)

Per-Action IR Details

Review posture — confirm that Kaseya VSA on-premises instances in your environment are patched against CVE-2021-30116 and are running a supported, up-to-date version; this vulnerability was the primary REvil supply chain vector and should have been remediated in 2021 per CISA guidance

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Maintaining IR Capability and Preventing Incidents

Controls: NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For teams without an enterprise vulnerability scanner: run `Invoke-WebRequest` or curl against the Kaseya VSA web interface header to retrieve the version string, then compare against Kaseya's end-of-life matrix. Alternatively, query installed software via PowerShell: `Get-WmiObject -Class Win32_Product | Where-Object { $_.Name -like '*Kaseya*' } | Select-Object Name, Version`. Cross-reference the returned version against CISA Advisory AA21-189A (July 2021) which lists the minimum safe version post-CVE-2021-30116 patch. If VSA is internet-facing, verify with Shodan CLI (`shodan host `) to confirm no public exposure remains.

Evidence: Before closing this review step, capture: (1) Kaseya VSA server application logs at `C:\Kaseya\Log\` and IIS logs at `C:\inetpub\logs\LogFiles\` for the July 2–5, 2021 window — REvil's initial access via CVE-2021-30116 produced anomalous POST requests to `/dl.asp` and `/userFilterTableRpt.asp` endpoints; (2) Windows Application Event Log on the VSA server for Event ID 1000/1001 (application crash/fault) which may indicate exploitation attempts against the authentication bypass; (3) Kaseya VSA audit logs for unauthorized agent procedure deployments, specifically procedures pushing `agent.crt` (the REvil dropper disguised as a certificate update).

Detection — query SIEM and EDR logs for historical REvil/GandCrab IOCs if threat hunting backlogs exist; search for known REvil file extensions (.sodinokibi, random-extension appended), ransom note filenames (e.g., [random]-readme.txt), and registry persistence keys associated with Sodinokibi; cross-reference against prior CISA and FBI REvil IOC releases

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Analyzing Indicators and Understanding Scope

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, execute retrospective hunting in three layers: (1) File system — run `Get-ChildItem -Path C:\ -Recurse -Include '*-readme.txt','*.sodinokibi' -ErrorAction SilentlyContinue` on managed endpoints; also scan for the REvil encrypted file marker by using a YARA rule targeting the Sodinokibi magic bytes and the hardcoded mutex `Global\206D87E0-0E60-DF25-DD8F-8E4E7D1E3BL0`; public YARA rules are available in the CISA/FBI joint advisory (AA21-131A). (2) Registry — query `HKLM\SOFTWARE\WOW6432Node\[random_key]` and `HKCU\SOFTWARE\[random_key]` for Sodinokibi's configuration blob stored as a base64-encoded value; use `reg query` or Autoruns (Sysinternals) filtered on non-Microsoft entries. (3) Process — deploy Sysmon with Event ID 1 (Process Create) and Event ID 13 (Registry Value Set) and search historical Sysmon logs for `MsMpEng.exe` or `certutil.exe` spawned by `AgentMon.exe` (Kaseya VSA agent process), which was the REvil lateral movement pattern post-VSA compromise.

Evidence: Preserve before hunting: (1) Sysmon Event ID 1 logs showing process lineage from `AgentMon.exe` or `KaseyaRemoteControlHost.exe` spawning PowerShell or cmd.exe — this is the execution chain REvil used post-VSA agent takeover (MITRE T1059.001); (2) Windows Security Event Log Event ID 4663 (Object Access) for file writes matching random 5–10 character extensions on file servers, indicating active encryption (MITRE T1486); (3) VSS shadow copy deletion events — Windows System Event Log or Sysmon Event ID 1 for `vssadmin.exe delete shadows /all /quiet` or `wmic.exe shadowcopy delete`, which REvil executed immediately prior to encryption; (4) Network flow logs or Wireshark captures for C2 beaconing to REvil's known Tor-based infrastructure — look for periodic HTTPS connections to `.onion` proxies or the hardcoded IPs published in FBI Flash CU-000147-MW.

Eradication — no new active threat vector to remediate; if legacy REvil/GandCrab IOCs are found during retrospective hunting, isolate affected hosts, revoke potentially compromised credentials, and initiate standard incident response procedures

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Eliminating Components of the Incident

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST SI-3 (Malicious Code Protection), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For a 2-person team without EDR: (1) Isolate by disabling the NIC via `netsh interface set interface 'Ethernet' admin=disable` or pulling the network cable — do not rely on firewall rules alone as REvil disables Windows Firewall via `netsh advfirewall set allprofiles state off`. (2) Credential revocation: force-reset all accounts whose Kerberos TGTs or NTLM hashes may have been harvested from the VSA server — REvil operators used Mimikatz (MITRE T1003.001) post-exploitation; run `Get-ADUser -Filter * | Disable-ADAccount` for non-essential accounts during the investigation window, then selectively re-enable. (3) Remove persistence: use Autoruns (Sysinternals) to identify and delete the Sodinokibi registry run key, typically written to `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` with a random alphanumeric name pointing to the encrypted payload DLL. (4) Verify eradication with ClamAV using the REvil-specific signatures from the CISA IOC list before returning hosts to production.

Evidence: Capture before any eradication action: (1) Full memory dump of the affected host using WinPmem or Magnet RAM Capture — Sodinokibi operates partly in-memory and injects into `MsMpEng.exe` or `explorer.exe` (MITRE T1055); this dump is required to recover the decryption key material and confirm full IOC scope; (2) Forensic image of the VSA server's `C:\Kaseya\` directory tree before any file removal — the attacker-modified `agent.crt` dropper and any webshells written to the VSA web root (`C:\Kaseya\WebPages\`) must be preserved as evidence; (3) Export of the Kaseya VSA audit database (SQL Server) showing all agent procedure executions in the attack window, which documents lateral spread to managed endpoints via the VSA RMM channel (MITRE T1072).

Recovery — validate backup integrity and offline backup availability for systems historically managed by MSPs using Kaseya VSA; confirm MSP vendor security posture if third-party managed services are in scope

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restoring Systems to Normal Operations

Controls: NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST IR-4 (Incident Handling), NIST SA-9 (External System Services), CIS 11.1 (Establish and Maintain a Data Recovery Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Without enterprise backup validation tooling: (1) Verify backup integrity manually by restoring a non-critical test system from the most recent pre-incident backup snapshot — REvil specifically targeted and encrypted network-accessible backup shares (MITRE T1490), so confirm backups are air-gapped or immutable before trusting them. (2) Query backup timestamps: if using Windows Server Backup, run `wbadmin get versions` to confirm the last clean backup predates July 2, 2021 (REvil Kaseya campaign start). (3) For MSP posture validation: require your MSP to provide written confirmation they have patched their VSA instance and rotated all agent-level credentials; reference CISA's MSP hardening guidance from Advisory AA22-131A as the baseline checklist. Document this confirmation per NIST SA-9 third-party oversight requirements.

Evidence: Before initiating recovery from backup: (1) Hash-verify backup media using `Get-FileHash` (SHA-256) against pre-incident baseline checksums to rule out backup tampering — REvil operators with extended dwell time have been documented accessing backup infrastructure prior to encryption; (2) Review VSS snapshot timestamps on backup servers for unexpected deletion events (Event ID 8193 in the VSS event log) indicating REvil's `vssadmin delete` command may have reached backup infrastructure; (3) Confirm MSP-managed endpoints have no residual Kaseya agent procedures queued — check the VSA agent procedure queue on all managed endpoints before reconnecting to production networks.

Post-incident controls — use this attribution event as a prompt to review third-party and supply chain risk management controls, specifically software update validation for RMM and MSP tooling; map current detection coverage against T1195.002 and T1486 in your ATT&CK coverage assessment

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned and Control Improvement

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SA-12 (Supply Chain Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For a 2-person team conducting ATT&CK coverage assessment without a SIEM: (1) Use the free ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) to layer your current Sysmon + Windows Event Log detection rules against T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain) and T1486 (Data Encrypted for Impact) — export the coverage heatmap as a gap report for leadership. (2) For T1195.002 detection, implement file integrity monitoring on RMM agent directories (`C:\Kaseya\`, `C:\Program Files\ConnectWise\`, etc.) using osquery's `file_events` table or Sysmon Event ID 11 (File Create) with path filters — this detects unauthorized updates pushed via compromised RMM channels. (3) For T1486, deploy the free Sigma rule `proc_creation_win_vssadmin_delete_shadows.yml` (available on the SigmaHQ GitHub repository) converted to Windows Event Log XML queries using sigma-cli, targeting Event ID 4688 with `CommandLine` containing `vssadmin` and `delete`.

Evidence: For the lessons-learned documentation required by NIST 800-61r3 §4: (1) Compile a timeline of all Kaseya VSA agent procedure executions from July 2–5, 2021 extracted from the VSA SQL audit log — this documents the blast radius of the supply chain compromise and is required for any cyber insurance claim or regulatory notification; (2) Export ATT&CK Navigator coverage gaps for T1195.002 and T1486 as baseline documentation showing detection posture at time of advisory, to measure improvement in the next review cycle; (3) Archive CISA Advisory AA21-189A and FBI Flash CU-000147-MW as the authoritative IOC reference for this threat actor campaign, tied to the BKA attribution announcement, to establish a documented threat intelligence record per NIST IR-6 (Incident Reporting) requirements.

Detection Guidance

No new IOCs or active indicators are released with this BKA attribution announcement. For retrospective threat hunting, reference the CISA advisory on the Kaseya VSA ransomware attack (https://www.cisa.gov/news-events/news/kaseya-ransomware-attack-guidance-affected-msps-and-their-customers) and the ODNI Kaseya VSA supply chain ransomware document for previously published IOC sets. Behavioral indicators associated with

REvil activity include: disabling of Volume Shadow Copy Service (vssadmin delete shadows commands, Windows Event ID 4688 with relevant command-line arguments), tampering with backup and recovery tools (T1490), staged exfiltration over encrypted C2 channels prior to encryption (T1041), and use of remote access tools not standard to the environment (T1219). SIEM detections should prioritize VSS deletion, bcdedit recovery mode modification, and lateral movement originating from RMM or MSP agent processes. Given operational dormancy since 2021, these detections are retrospective and low urgency unless a novel REvil successor campaign is identified.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`See CISA Kaseya VSA advisory for published IOC list`	CISA published IOCs specific to the July 2021 Kaseya VSA REvil attack; no new IOCs are released with this BKA attribution announcement	LOW
HASH	`See CISA Kaseya VSA advisory and ODNI document for published file hashes`	REvil encryptor and dropper hashes were published by CISA and FBI following the July 2021 incident; no new hashes are associated with this attribution event	LOW

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1083** — File and Directory Discovery
- **T1041** — Exfiltration Over C2 Channel
- **T1195.002** — Compromise Software Supply Chain
- **T1489** — Service Stop
- **T1219** — Remote Access Tools
- **T1490** — Inhibit System Recovery
- **T1486** — Data Encrypted for Impact
- **T1657** — Financial Theft

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality

- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-6** — Configuration Settings
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

NIST-CSF-2

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

HIPAA-SECURITY

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

ISO-27001-2022

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

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1083	File and Directory Discovery	Discovery
T1041	Exfiltration Over C2 Channel	Exfiltration
T1195.002	Compromise Software Supply Chain	Initial-Access
T1489	Service Stop	Impact
T1219	Remote Access Tools	Command-And-Control
T1490	Inhibit System Recovery	Impact
T1486	Data Encrypted for Impact	Impact
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/german-authorities-i...	T3
Kaseya Ransomware Attack: Guidance for Affected MSPs and their ...	https://www.cisa.gov/news-events/news/kaseya-ransomware-attack-guid...	T1
[PDF] Kaseya VSA Supply Chain Ransomware Attack - ODNI	https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/Kase...	T1
What Happened in the Kaseya VSA Incident? - Lawfare	https://www.lawfaremedia.org/article/what-happened-kaseya-vsa-incident	T3
Kaseya VSA ransomware attack - Grokipedia	https://grokipedia.com/page/Kaseya_VSA_ransomware_attack	T3

Generated 2026-04-07 06:06 UTC by TJS Security Command Center