INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-06 13:18 UTC

Germany Identifies 'UNKN' as Leader of REvil and GandCrab Ransomware Operations

THREAT ACTOR | CRITICAL

SCC Item ID	SCC-TAC-2026-0005
Type	Threat Actor
Severity	CRITICAL
Affected Products	Organizations targeted by REvil and GandCrab ransomware globally; at least 130 victims in Germany (2019-2021)
Published	2026-04-06
Discovery Source	Gemini

Executive Summary

German federal authorities (BKA) have publicly named Daniil Maksimovich Shchukin, alias 'UNKN,' as the alleged operational leader of the GandCrab and REvil ransomware-as-a-service operations, issuing a formal arrest warrant. REvil is linked to the 2021 Kaseya VSA and JBS Foods attacks; GandCrab is estimated to have extorted over $2 billion globally before shutting down in 2019. Shchukin remains at large in Russia, so no operational disruption to successor ransomware ecosystems should be assumed. Organizations should treat this as a threat-landscape update rather than a threat eliminated.

Technical Analysis

REvil (Sodinokibi) and GandCrab operated as ransomware-as-a-service platforms, meaning 'UNKN' led core development and administration while independent affiliates conducted intrusions. REvil officially suspended operations in July 2021 following law enforcement pressure, but successor operations (Blackmatter, Alphv/BlackCat) are believed to have absorbed affiliates and infrastructure, making this attribution event a public record of historical leadership rather than a disruption of active infrastructure. No CVE or CVSS scoring applies to this attribution action. Mapped MITRE ATT&CK techniques reflect REvil/GandCrab TTPs: initial access via phishing (T1566) and valid accounts (T1078); supply chain compromise (T1195, directly relevant to Kaseya VSA); command-and-control over encrypted channels (T1573) using standard application-layer protocols (T1071); data exfiltration (T1041); financial extortion (T1657); and impact via file encryption (T1486), service stop (T1489), and backup inhibition (T1490). REvil exploited CVE-2021-30116 (Kaseya VSA) in its most significant supply chain attack. Affiliates typically used RDP brute force, exposed VPN appliances, and phishing as entry vectors. The BKA action is a public attribution with an arrest warrant; no patch, takedown, or infrastructure seizure is associated with this announcement. Shchukin is believed to be in Russia, where

extradition is not available.

Action Checklist

1. Containment: No active infrastructure associated with this announcement has been identified for immediate blocking. Verify that any legacy REvil or GandCrab IOCs (from prior CISA/FBI advisories AA21-131A and AA21-265A) are present in your blocklists and EDR exclusion policies are not inadvertently whitelisting known REvil file paths.
2. Detection: Review SIEM and EDR telemetry for REvil/GandCrab TTPs: look for VSS deletion commands (vssadmin.exe delete shadows), PowerShell encoded commands, scheduled task creation by non-standard accounts, and lateral movement via SMB or RDP from unexpected internal hosts. Cross-reference endpoint logs against CISA advisory AA21-131A IOC list.
3. Eradication: No new patch or config change is required by this announcement. If REvil-related artifacts are found during detection review, follow CISA guidance AA21-265A for full eradication steps including credential rotation for all privileged accounts, RDP exposure audit, and review of managed service provider (MSP) access paths.
4. Recovery: If prior REvil/GandCrab exposure is confirmed during review, validate backup integrity and offline backup availability before any restoration. Confirm backups were not accessible from the compromised environment (T1490 inhibits recovery when backups are network-connected).
5. Post-Incident: This attribution event is a prompt to audit RaaS-relevant control gaps: MFA coverage on VPN and RDP, MSP/third-party access segmentation, VSS and backup access controls, and offline backup retention policy. Map current controls against NIST CSF Respond/Recover functions and CIS Benchmark v8 Controls 10 (Data Recovery) and 12 (Network Infrastructure Management).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if detection review confirms any REvil or GandCrab IOC match on production systems, particularly on systems processing PII or PHI, as this triggers breach notification obligations under GDPR (for EU data subjects, given the BKA investigation context), HIPAA, or applicable US state breach notification laws; also escalate if any MSP or third-party RMM agent (especially Kaseya VSA) is found active in the environment without a documented access control review.
Recovery Notes	Before restoring any system, confirm backup creation timestamps predate the earliest possible REvil/GandCrab dwell time by cross-referencing backup dates against the detection timeline established from Sysmon and Windows Security Event logs — REvil operators routinely maintained dwell times of 10–14 days before triggering encryption to maximize backup contamination. Post-restoration, deploy integrity monitoring (Windows Sysmon Event ID 11 for file creation) specifically watching for REvil's characteristic ransom note filename pattern '[0-9A-Z]{8}-readme.txt' and re-encryption of recently restored files for a minimum 30-day observation window. Maintain heightened monitoring on all MSP and RMM access paths for 90 days post-recovery, as REvil affiliates have demonstrated re-entry through the same MSP supply-chain vectors used in initial compromise.

Forensic Artifacts	Windows Security Event Log Event ID 4688 (Process Creation) entries with CommandLine values matching 'vssadmin.exe delete shadows /all /quiet', 'wmic shadowcopy delete', or 'bcdedit /set {default} recoveryenabled No' — these are REvil's standard pre-encryption VSS and recovery destruction commands (T1490) | Sysmon Event ID 1 (Process Create) logs showing cmd.exe or powershell.exe spawned from Kaseya VSA agent process 'AgentMon.exe' or working directory 'C:\kworking\' — the specific execution chain used in the July 2021 Kaseya VSA supply-chain attack attributed to REvil | Windows PowerShell Script Block Logging (Event ID 4104) entries containing Base64-encoded payloads — REvil's initial staging script deployed via Kaseya VSA used encoded PowerShell to disable Windows Defender and drop the encryptor binary, and the decoded content is recoverable from these logs even after the process exits | Encrypted file system artifacts: files renamed with victim-specific 8-character hex extension (REvil/Sodinokibi pattern) and ransom notes matching '[0-9A-Z]{8}-readme.txt' naming convention, distributed across all writable network shares accessible from the compromised host at time of encryption | Kaseya VSA server-side audit logs and agent procedure execution history at 'C:\kworking\agent.log' and within the VSA database's 'agentproc' tables documenting the malicious 'Kaseya VSA Agent Hot-fix' package (named 'agent.crt' in the Kaseya VSA attack) that delivered the REvil dropper to managed endpoints

Per-Action IR Details

Containment — No active infrastructure associated with this announcement has been identified for immediate blocking. Verify that any legacy REvil or GandCrab IOCs (from prior CISA/FBI advisories AA21-131A and AA21-265A) are present in your blocklists and EDR exclusion policies are not inadvertently whitelisting known REvil file paths.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST SI-4 (System Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Export the REvil/GandCrab IOC hashes from CISA AA21-131A and AA21-265A into a plain-text YARA rule set and run against all endpoints using: 'yara -r revil_gandcrab.yar C:\'. Cross-check firewall deny-list against known REvil C2 domains documented in AA21-131A using a simple PowerShell script: 'Get-Content iocs.txt | ForEach-Object { nslookup $_ }' to identify any resolving domains still not blocked. Review Windows Defender exclusion paths via 'Get-MpPreference | Select-Object ExclusionPath' on each host to catch inadvertent whitelisting of known REvil staging directories such as %TEMP%\REvil or %AppData%\REvil-associated paths.

Evidence: Before modifying blocklists, capture current firewall deny-list state and EDR exclusion policy exports as forensic baselines. Pull DNS query logs from your resolver for the past 90 days and search for domains listed in CISA AA21-131A C2 infrastructure. Preserve Windows Defender exclusion registry keys at 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Exclusions\' before any changes. Document all existing EDR policy exports with timestamps so any prior misconfiguration creating a whitelist gap for REvil file paths (e.g., agent installer paths used during the Kaseya VSA supply-chain attack) is preserved as evidence of potential exposure window.

Detection — Review SIEM and EDR telemetry for REvil/GandCrab TTPs: look for VSS deletion commands (vssadmin.exe delete shadows), PowerShell encoded commands, scheduled task creation by non-standard accounts, and lateral movement via SMB or RDP from unexpected internal hosts. Cross-reference endpoint logs against CISA advisory AA21-131A IOC list.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config and hunt for REvil-specific execution chain: Event ID 1 (Process Create) where ParentImage matches Kaseya VSA agent path 'C:\Program Files (x86)\Kaseya\' or 'C:\kworking\' spawning cmd.exe or powershell.exe. Query Windows Security Event Log for Event ID 4688 (Process Creation) filtering on CommandLine containing 'vssadmin delete shadows', 'wmic shadowcopy delete', or 'bcdedit /set {default} recoveryenabled No'. For scheduled task creation, query Event ID 4698 (Scheduled Task Created) in the Security log filtered to tasks created by accounts outside your standard admin baseline. For lateral movement, parse Windows Security Event ID 4624 (Logon Success) Type 3 (Network) and Event ID 4625 (Logon Failure) to identify SMB or RDP spray patterns from internal hosts. Use the free Sigma rule 'proc_creation_win_vssadmin_delete_shadows.yml' from the SigmaHQ repository converted to PowerShell or Splunk SPL for no-cost detection.

Evidence: Preserve Sysmon operational log (Microsoft-Windows-Sysmon/Operational) and Windows Security Event Log from all endpoints before any remediation. Capture full PowerShell Script Block Logging output (Event ID 4104) and Module Logging (Event ID 4103) to recover encoded command payloads — REvil consistently used Base64-encoded PowerShell for initial staging during Kaseya VSA exploitation. Collect Windows Task Scheduler operational log ('Microsoft-Windows-TaskScheduler/Operational', Event ID 106 Task Registered) to document any persistence tasks. Export SMB access logs from all file servers and domain controllers covering the period 2019–2021 and current date if legacy exposure is suspected. Capture memory from any system showing VSS deletion activity before rebooting — REvil's encryption keys and ransom configuration blob exist only in memory during active encryption.

Eradication — No new patch or config change is required by this announcement. If REvil-related artifacts are found during detection review, follow CISA guidance AA21-265A for full eradication steps including credential rotation for all privileged accounts, RDP exposure audit, and review of managed service provider (MSP) access paths.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AC-1 (Policy and Procedures — Access Control), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For MSP/RMM access path audit without enterprise tooling, run 'netstat -ano' on all servers and cross-reference listening ports against known RMM tool port ranges (Kaseya VSA: TCP 443/5721; ConnectWise: TCP 443/8040; Datto: TCP 443); terminate and document any unrecognized RMM agent processes. For credential rotation prioritization, use 'net localgroup administrators' and 'net group "Domain Admins" /domain' to enumerate privileged accounts and rotate all passwords via Active Directory for accounts that had interactive sessions during the suspected exposure window. For RDP audit, run 'Get-ItemProperty HKLM:\System\CurrentControlSet\Control\Terminal Server' to confirm RDP is disabled where not required, and query Windows Firewall logs for inbound TCP 3389 connections from external IPs over the prior 90 days using 'Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall"' filtered on port 3389.

Evidence: Before rotating credentials, collect a full Active Directory account audit including last logon timestamps via 'Get-ADUser -Filter * -Properties LastLogonDate, PasswordLastSet' to establish which privileged accounts were active during suspected REvil dwell time. Preserve a copy of all MSP/RMM agent configuration files and connection logs before removing or reconfiguring agents — during Kaseya VSA attacks, REvil operators abused the VSA software deployment feature and logs at 'C:\kworking\agent.log' and Kaseya VSA server-side audit logs document the malicious package push. Capture registry run keys ('HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run', 'HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run') and scheduled tasks XML exports ('schtasks /query /fo LIST /v > tasks_baseline.txt') from all affected systems before eradication to preserve evidence of REvil persistence mechanisms.

Recovery — If prior REvil/GandCrab exposure is confirmed during review, validate backup integrity and offline backup availability before any restoration. Confirm backups were not accessible from the

compromised environment (T1490 inhibits recovery when backups are network-connected).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 11.1 (Establish and Maintain a Data Recovery Process), CIS 11.3 (Protect Recovery Data)

Compensating: Verify backup integrity without enterprise backup validation tools by booting a known-clean system from read-only media and mounting backup volumes in read-only mode, then running 'Get-FileHash -Algorithm SHA256' across a statistically representative sample of restored files and comparing hashes against pre-incident file hash baselines if available. To confirm backup network isolation, review backup agent service account membership — REvil specifically targeted network-connected backup repositories (Veeam, Windows Server Backup) using T1490; run 'net use' and 'Get-SmbConnection' on backup servers to confirm no active shares to domain-joined hosts. For GandCrab-era exposure (2019), note that no universal decryptor exists for all GandCrab variants post v5.2 — confirm with Europol's No More Ransom project (nomoreransom.org) before assuming backup restoration is the only recovery path.

Evidence: Before initiating any restoration, snapshot the current encrypted file system state — document encrypted file extensions (.aedc5, .sodinokibi, .revil, or victim-specific extensions generated by REvil's configuration) and preserve the ransom note files ('[0-9A-Z]{8}-readme.txt' naming pattern used by REvil) as forensic artifacts. Collect Volume Shadow Copy enumeration output ('vssadmin list shadows') to confirm whether VSS copies were successfully deleted by the REvil VSS deletion routine (T1490) or whether any pre-attack shadows survive and are usable for recovery. Preserve Windows Event Log entries showing the exact timestamp of VSS deletion commands to establish encryption timeline and potential data loss window.

Post-Incident — This attribution event is a prompt to audit RaaS-relevant control gaps: MFA coverage on VPN and RDP, MSP/third-party access segmentation, VSS and backup access controls, and offline backup retention policy. Map current controls against NIST CSF Respond/Recover functions and CIS Benchmark v8 Controls 10 (Data Recovery) and 12 (Network Infrastructure Management).

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Conduct a structured RaaS-specific tabletop exercise using the Kaseya VSA and JBS Foods attack chains as scenarios — both are publicly documented and require no paid simulation platform. For MFA gap audit without a commercial IAM tool, run 'Get-ADUser -Filter * -Properties "msDS-SupportedEncryptionTypes", PasswordLastSet | Where-Object {$_.Enabled -eq $true}' to identify accounts without MFA-enforced authentication methods, then cross-reference against VPN and RDP access logs. For MSP segmentation audit, enumerate all third-party RMM agents using 'Get-Service | Where-Object {$_.DisplayName -match "Kaseya|ConnectWise|Datto|N-able|Solarwinds"}' and verify each has a documented, time-limited access policy. Update your Sigma detection rule library with REvil/GandCrab-specific rules from SigmaHQ (search tag 'ransomware') and schedule monthly review cadence aligned to CISA advisory releases.

Evidence: Document the lessons-learned output as a formal gap register mapping each identified control deficiency to the specific REvil/GandCrab TTP it would have mitigated (e.g., absence of MFA on RDP mapped to T1133 External Remote Services and T1078 Valid Accounts, the primary REvil initial access vectors). Preserve all SIEM/EDR query results from the detection review phase as evidence of detection coverage gaps — these constitute the baseline for measuring improvement. Archive the BKA advisory, CISA AA21-131A, and AA21-265A alongside your internal gap register to satisfy NIST SI-5 (Security Alerts, Advisories, and Directives) documentation requirements and support future audit evidence.

Detection Guidance

No new IOCs have been released by BKA in conjunction with this announcement. For historical REvil and GandCrab detection, reference CISA Advisory AA21-131A (REvil) and FBI FLASH CU-000149-MW. Note: These advisories are from 2021; verify CISA's current REvil/GandCrab documentation for the latest IOCs and behavioral indicators. Key behavioral indicators: (1) vssadmin.exe or wmic.exe invoked to delete shadow copies, Windows Event ID 4688 or Sysmon Event ID 1 with these command lines; (2) registry modifications under HKLM\SOFTWARE\WOW6432Node\Facebook (a known REvil persistence key in some variants); (3) files encrypted with .sodinokibi or randomized extensions with ransom note 'readme.txt' or '[random]-readme.txt'; (4) outbound encrypted traffic to Tor exit nodes or unusual high-entropy domains from endpoints. For Kaseya VSA-specific detection, review for agent procedure execution anomalies and lateral movement originating from Kaseya service accounts. Threat hunting hypothesis: search for scheduled tasks created by accounts that do not normally create them, combined with subsequent PowerShell execution, maps to T1053 and T1059 patterns consistent with REvil affiliate behavior.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`See CISA AA21-131A for full IOC list`	REvil C2 infrastructure documented in CISA advisory — no new IOCs released with BKA attribution announcement	LOW
HASH	`See CISA AA21-131A and FBI FLASH CU-000149-MW`	REvil ransomware binary hashes; historical, affiliates frequently repackage	LOW

Framework Mappings

MITRE-ATTACK

- **T1489** — Service Stop
- **T1195** — Supply Chain Compromise
- **T1041** — Exfiltration Over C2 Channel
- **T1657** — Financial Theft
- **T1078** — Valid Accounts
- **T1071** — Application Layer Protocol
- **T1566** — Phishing
- **T1486** — Data Encrypted for Impact
- **T1490** — Inhibit System Recovery
- **T1573** — Encrypted Channel

NIST-800-53R5

- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring

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

CIS-V8

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1489	Service Stop	Impact
T1195	Supply Chain Compromise	Initial-Access
T1041	Exfiltration Over C2 Channel	Exfiltration
T1657	Financial Theft	Impact
T1078	Valid Accounts	Defense-Evasion
T1071	Application Layer Protocol	Command-And-Control

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1490	Inhibit System Recovery	Impact
T1573	Encrypted Channel	Command-And-Control

Sources

Source	URL	Tier
Germany Doxes “UNKN,” Head of RU Ransomware Gangs REvil ...	https://krebsonsecurity.com/2026/04/germany-doxes-unkn-head-of-ru-r...	T3
Germany Doxes “UNKN,” Head of RU Ransomware Gangs REvil ...	https://databreaches.net/2026/04/06/germany-doxes-unkn-head-of-ru-r...	T3
Germany's BKA named 31-year-old Daniil Shchukin as UNKN, head ...	https://x.com/Cyber_O51NT/status/2041056620604498042	T3
The Cyber Security Hub™'s Post - LinkedIn	https://www.linkedin.com/posts/the-cyber-security-hub_germany-doxes...	T3
Germany's BKA has identified a key figure behind the ... - Instagram	https://www.instagram.com/p/DWx_l7bDwfG/	T3

Generated 2026-04-06 13:18 UTC by TJS Security Command Center