INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-20 18:48 UTC

Prinz Eugen Ransomware Group Uses Go-Based Encryptor, Abuses RMM Tools, Leaves No Ransom Note

THREAT ACTOR | HIGH | CVSS 7.5

SCC Item ID	SCC-TAC-2026-0025
Type	Threat Actor
Severity	HIGH
CVSS Base Score	7.5
Affected Products	No specific vendor products targeted; RemotePC RMM tool abused for persistence; Standard Bank confirmed as named victim
Published	2026-06-20T11:23:46
Discovery Source	Rss

Executive Summary

A newly identified ransomware group called Prinz Eugen is actively targeting organizations using stolen RDP credentials, deploying a Go-based encryptor that prioritizes recently modified files to maximize operational disruption. The group deliberately omits ransom notes, delaying victim detection and extending the window before incident response begins. Standard Bank has been named as a confirmed victim, and the group's abuse of legitimate remote management tooling makes detection significantly harder without specific behavioral controls in place.

Technical Analysis

Prinz Eugen operates independently of the RaaS ecosystem, reducing the typical intelligence visibility that affiliate-based groups provide. Initial access is gained via stolen RDP credentials (T1078, T1133). The group abuses RemotePC, a legitimate RMM tool, for persistence and lateral movement (T1219), consistent with living-off-the-land tradecraft (T1036, T1059, T1027) designed to blend with normal administrative traffic. The Go-based encryptor targets recently modified files first (T1083, T1486), maximizing disruption to active business workflows before detection occurs. No ransom note is left on compromised systems, a deliberate tactic (T1070.004) that delays victim recognition of a ransomware event versus other incident types. Additional observed techniques include archive collection (T1560), exfiltration over C2 (T1041), ingress tool transfer (T1105), local account creation (T1136.001), command interpreter abuse (T1059), and defense evasion via obfuscation (T1027) and security tool impairment (T1562). Relevant weaknesses include CWE-311 (missing

encryption of sensitive data, from the victim's perspective) and CWE-693 (protection mechanism failure, specifically detection gaps created by LotL and no-note tactics). Malwarebytes ThreatDown has published IOCs. No CVE is associated with this item; exploitation relies on credential abuse and tool misuse rather than a software vulnerability.

Action Checklist

1. Step 1: Containment. Audit all active RDP sessions immediately; disable external RDP access or restrict it to VPN-only. Block RemotePC executables and associated network endpoints at the perimeter if RemotePC is not an authorized tool in your environment. Isolate any systems showing unexpected RemotePC installation or unusual file modification patterns. Reference: CISA Advisory AA23-025A on malicious RMM tool use.
2. Step 2: Detection. Ingest Malwarebytes ThreatDown IOCs into your SIEM and EDR platforms now. Hunt for RemotePC process execution (remotepc.exe, rpcsuite.exe) on hosts where it is not inventoried as authorized software (CIS 2.1, CIS 2.3). Query authentication logs for RDP logons from unfamiliar source IPs or outside business hours (NIST AU-6, AU-12). Alert on mass file modification events, especially targeting recently written files across shared drives. Look for command interpreter invocations (cmd.exe, powershell.exe) spawned from RMM parent processes (MITRE T1059). Monitor for deletion of VSS shadow copies and event log clearing (T1070.004, T1562).
3. Step 3: Eradication. Rotate all RDP credentials immediately; prioritize accounts with domain or local admin privileges (D3-CRO, NIST AC-2). Remove unauthorized RemotePC installations and revoke any associated RemotePC account sessions. Audit all local accounts created in the past 30 days against your authorized account inventory (T1136.001, CIS 5.1, D3-LAM). Enforce MFA on all remote access paths: RDP, VPN, and any RMM tool in use (CIS 6.4, D3-MFA). Remove or quarantine any identified malware artifacts per ThreatDown IOCs.
4. Step 4: Recovery. Restore encrypted systems from clean, verified backups taken prior to the intrusion window. Validate restored systems against your asset inventory before returning to production (CIS 1.1). Monitor restored hosts for 72 hours for re-infection indicators, including unexpected RMM process spawns and rapid file modification bursts. Confirm shadow copy and backup integrity before declaring recovery complete (NIST CP controls).
5. Step 5: Post-Incident. Conduct a credential exposure review: identify how RDP credentials were stolen and whether credential reuse extends to other systems. Implement an RMM allowlist policy; only approved tools should be permitted to execute (CIS 2.3, NIST CM controls). Formalize a detection rule for 'no ransom note' ransomware scenarios: alert on mass encryption behavior even in the absence of a dropped note file. Review and strengthen audit logging coverage per NIST AU-2 and AU-12 to ensure RMM activity and RDP sessions are captured with sufficient fidelity for forensic reconstruction.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership and legal/privacy counsel if encrypted systems contain PII, PHI, or financial records (triggering breach notification obligations under GDPR, HIPAA, or PCI DSS), if Prinz Eugen's deliberate omission of a ransom note means encryption may have progressed undetected for days before discovery, or if RemotePC persistence is confirmed on domain controllers or backup infrastructure indicating potential for full domain compromise.
Recovery Notes	Restore only from backups with timestamps predating the earliest confirmed Prinz Eugen RDP logon identified in authentication logs — do not assume the most recent backup is clean, as the group's no-ransom-note strategy is specifically designed to extend the undetected encryption window. Before declaring recovery complete, verify that VSS shadow copies have been re-created, RemotePC is absent from all restored hosts, and all RDP credentials rotated during eradication are enforced across every restored system. Maintain active Sysmon monitoring on all recovered hosts for a minimum of 72 hours, treating any remotepc.exe execution or mass file modification burst as an immediate re-isolation trigger.
Forensic Artifacts	Windows Security Event Log (EVTX) — Event ID 4624 Logon Type 10 (RDP interactive) entries with source IP and account name, establishing the stolen-credential RDP access chain specific to Prinz Eugen's initial access vector | USN Change Journal (fsutil usn readjournal output) — records the Go encryptor's file modification sequence, confirming the recently-modified-file prioritization behavior unique to this group and establishing blast radius boundaries | Prefetch files (C:\Windows\Prefetch\REMOTEPC*.pf and encryptor binary prefetch) — provide first-execution timestamps for RemotePC abuse and the Go-based encryptor, critical for establishing the intrusion timeline in the absence of a ransom note | RemotePC installation registry artifacts (HKLM\SOFTWARE\RemotePC, associated scheduled tasks, and %AppData%\RemotePC session logs) — evidence of RMM persistence mechanism specific to this group's tooling, preserved before uninstall | LSASS memory dump (pre-credential-rotation) — preserves evidence of the credential theft technique used to obtain the RDP credentials that enabled Prinz Eugen's initial access, supporting root cause determination and reuse scope analysis

Per-Action IR Details

Step 1: Containment — Audit all active RDP sessions immediately; disable external RDP access or restrict it to VPN-only. Block RemotePC executables and associated network endpoints at the perimeter if RemotePC is not an authorized tool in your environment. Isolate any systems showing unexpected RemotePC installation or unusual file modification patterns. Reference: CISA Advisory AA23-025A on malicious RMM tool use.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), 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: Run 'netstat -ano | findstr :3389' and 'qwinsta /server:' on each Windows host to enumerate live RDP sessions. Use Windows Firewall with 'netsh advfirewall firewall add rule name=Block_RDP dir=in action=block protocol=TCP localport=3389' to drop external RDP immediately. Block RemotePC network endpoints (remotepc.com, *.remotepc.com) via hosts file or perimeter ACL. Script a sweep with PowerShell: 'Get-Process remotepc,rpcsuite -ErrorAction SilentlyContinue | Select-Object Name,Id,MachineName' across the estate.

Evidence: Before isolating any host, capture: (1) full memory dump using WinPmem or ProcDump targeting remotepc.exe/rpcsuite.exe PIDs to preserve in-memory Go encryptor artifacts; (2) 'netstat -ano' and 'Get-NetTCPConnection' output to document active RDP source IPs and RemotePC C2 connections; (3) 'qwinsta' output showing all active RDP session tokens before revocation; (4) Windows Security Event Log entries — Event ID 4624 (Logon Type 10, RDP) and 4778 (Session Reconnected) — exported to preserve stolen-credential logon chain; (5) file system timeline snapshot (via 'fsutil usn readjournal C: csv > usn.csv') to record the encryptor's file modification

sequence targeting recently written files before isolation destroys the live USN journal state.

Step 2: Detection — Ingest Malwarebytes ThreatDown IOCs into your SIEM and EDR platforms now. Hunt for RemotePC process execution (remotepc.exe, rpcsuite.exe) on hosts where it is not inventoried as authorized software (CIS 2.1, CIS 2.3). Query authentication logs for RDP logons from unfamiliar source IPs or outside business hours (NIST AU-6, AU-12). Alert on mass file modification events — especially targeting recently written files across shared drives. Look for command interpreter invocations (cmd.exe, powershell.exe) spawned from RMM parent processes (MITRE T1059). Monitor for deletion of VSS shadow copies and event log clearing (T1070.004, T1562).

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 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config; Event ID 1 (Process Create) will catch remotepc.exe/rpcsuite.exe parent-child chains and cmd.exe/powershell.exe spawned from RMM processes. Use Event ID 23 (File Delete) and ID 26 (File Delete Detected) to catch VSS and log clearing. Write a PowerShell loop: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.Properties[8].Value -eq 10}' filtered against a known-good IP allowlist to surface stolen-credential RDP logons. For mass file modification, run: 'Get-ChildItem -Recurse \\\shares | Where-Object {$_.LastWriteTime -gt (Get-Date).AddHours(-2)} | Measure-Object' and alert if count exceeds a defined threshold. No-SIEM teams can use Chainsaw against collected EVTX files with the Sigma rule set to detect VSS deletion (vssadmin delete shadows) and log clearing (wevtutil cl).

Evidence: This step is primarily observational and does not alter live state; however, if IOC ingestion triggers automated EDR quarantine of remotepc.exe, capture the process memory dump and parent-process tree (Sysmon Event ID 1 chain) before quarantine executes. Preserve: Windows Security EVTX (4624/4625/4778 for RDP credential abuse), System EVTX (7045 for new service installs by RemotePC installer), Application EVTX, and VSS-related entries in the Volume Shadow Copy service log. Export the USN Change Journal to detect the encryptor's priority-based file selection pattern targeting recently modified files.

Step 3: Eradication — Rotate all RDP credentials immediately; prioritize accounts with domain or local admin privileges (D3-CRO, NIST AC-2). Remove unauthorized RemotePC installations and revoke any associated RemotePC account sessions. Audit all local accounts created in the past 30 days against your authorized account inventory (T1136.001, CIS 5.1, D3-LAM). Enforce MFA on all remote access paths — RDP, VPN, and any RMM tool in use (CIS 6.4, D3-MFA). Remove or quarantine any identified malware artifacts per ThreatDown IOCs.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Before rotating credentials, dump LSASS memory with ProcDump ('procdump -ma lsass.exe lsass.dmp') on suspected hosts to preserve credential artifacts for forensic analysis. Use 'net user /domain' and 'Get-LocalUser | Where-Object {$_.Enabled -eq $true}' to enumerate accounts; cross-reference creation dates with 'net user /domain | findstr "Password last set"'. Remove RemotePC via 'wmic product where name="RemotePC" call uninstall' and delete residual directories under %ProgramFiles%\RemotePC and %AppData%\RemotePC. For MFA enforcement without enterprise tooling, enable Windows Hello for Business or configure Azure AD Conditional Access (free tier) to require MFA on RDP-exposed accounts. Quarantine Go encryptor binary artifacts matched to ThreatDown IOC hashes using 'Get-FileHash -Algorithm SHA256' compared against the published IOC list.

Evidence: Before rotating any credential or removing RemotePC: (1) capture LSASS memory dump to preserve evidence of credential theft technique used by Prinz Eugen; (2) export full registry hive HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList and SAM hive to document all local accounts

including any created during the intrusion window; (3) export RemotePC installation registry keys (HKLM\SOFTWARE\RemotePC and HKCU\SOFTWARE\RemotePC) and associated scheduled tasks ('schtasks /query /fo CSV /v > tasks.csv') before uninstall destroys them; (4) collect prefetch files (C:\Windows\Prefetch\REMOTEPC*.pf) to establish first-execution timestamps; (5) snapshot 'net session' and 'net use' outputs to record any active SMB sessions the threat actor may still hold before credential rotation closes them.

Step 4: Recovery — Restore encrypted systems from clean, verified backups taken prior to the intrusion window. Validate restored systems against your asset inventory before returning to production (CIS 1.1). Monitor restored hosts for 72 hours for re-infection indicators, including unexpected RMM process spawns and rapid file modification bursts. Confirm shadow copy and backup integrity before declaring recovery complete (NIST CP controls).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Verify backup integrity before restoration by comparing SHA-256 hashes of backup archives against pre-incident checksums stored offline. After restoration, deploy Sysmon immediately on each recovered host and enable Event ID 1/3/11 logging to catch remotepc.exe re-execution, outbound connections to RemotePC infrastructure, and new file creation matching Go encryptor naming patterns. Run a scheduled PowerShell job every 15 minutes for the 72-hour watch window: 'Get-ChildItem -Recurse | Group-Object DirectoryName | Where-Object {$_.Count -gt 50}' to detect the encryptor's mass modification behavior targeting recently written files before it reaches scale. Confirm VSS is re-enabled ('vssadmin list shadows') and a new shadow copy exists post-restoration.

Evidence: Before returning restored hosts to production, verify: (1) backup timestamp predates the earliest confirmed Prinz Eugen RDP logon (Event ID 4624 Type 10) in your authentication logs to establish a clean restore point; (2) restored file hash sampling against known-good checksums to confirm the Go encryptor did not modify backup-staged files prior to encryption; (3) absence of RemotePC registry keys and executables on restored image; (4) VSS integrity confirmed via 'vssadmin list shadows' showing current shadow copies with post-restoration timestamps. During the 72-hour monitoring window, treat any remotepc.exe or rpcsuite.exe process creation (Sysmon Event ID 1) or rapid sequential LastWriteTime changes across shared paths as an immediate re-infection indicator requiring re-isolation.

Step 5: Post-Incident — Conduct a credential exposure review: identify how RDP credentials were stolen and whether credential reuse extends to other systems. Implement an RMM allowlist policy — only approved tools should be permitted to execute (CIS 2.3, NIST CM controls). Formalize a detection rule for 'no ransom note' ransomware scenarios: alert on mass encryption behavior even in the absence of a dropped note file. Review and strengthen audit logging coverage per NIST AU-2 and AU-12 to ensure RMM activity and RDP sessions are captured with sufficient fidelity for forensic reconstruction.

NIST Phase: Post Incident

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), NIST AC-2 (Account Management), CIS 2.3 (Address Unauthorized Software), CIS 5.2 (Use Unique Passwords), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use HaveIBeenPwned API or offline breach corpus tools (e.g., h8mail) to determine whether compromised RDP accounts appeared in prior credential dumps, establishing the likely stolen-credential source. Implement an application allowlist for RMM tools using Windows Software Restriction Policies or AppLocker with a deny-by-default rule blocking remotepc.exe and rpcsuite.exe hashes. For the 'no ransom note' detection gap, write a Sigma rule targeting Windows Security Event Log that triggers when more than 200 file rename/write events occur within a 60-second window across monitored directories — this catches Prinz Eugen's recently-modified-file prioritization pattern regardless of note presence. Archive all collected forensic artifacts (EVTX exports, memory dumps, USN journals, prefetch files) for a minimum of 12 months per AU-11 guidance to support any regulatory notification or legal proceedings.

Evidence: Post-incident forensic reconstruction should draw on: (1) the full RDP authentication log chain (Event ID 4624 Type 10 with source IPs) to establish the credential theft timeline and determine if reuse extends to other systems in the estate; (2) Prefetch and Shimcache entries for remotepc.exe and the Go encryptor binary to establish precise first-execution timestamps and execution frequency; (3) USN Change Journal exports showing the encryptor's file selection sequence (recently modified files first) to reconstruct blast radius and inform backup restore point selection; (4) any RemotePC account portal logs obtained via the RemotePC vendor to identify attacker-controlled account registrations used for persistence; (5) DNS query logs or proxy logs for outbound connections to *.remotepc.com during the intrusion window to establish the full C2 and exfiltration timeline.

Detection Guidance

Primary detection sources: EDR telemetry, Windows Security Event Logs, and SIEM. Key behavioral indicators: (1) RemotePC process execution (remotepc.exe, rpcsuite.exe) on hosts not in authorized software inventory, cross-reference CIS 2.1 software inventory; (2) RDP logon events (Event ID 4624, Logon Type 10) from external or unexpected source IPs, especially outside business hours; (3) rapid, sequential file modification events across shared network drives targeting recently written files - this is the encryptor's file prioritization behavior (T1083, T1486); (4) command interpreter processes (cmd.exe, powershell.exe) spawned by RMM parent processes; (5) deletion of Volume Shadow Copies (vssadmin.exe delete shadows) and Windows Event Log clearing (wevtutil.exe cl); (6) new local account creation events (Event ID 4720) not correlated with provisioning workflows (T1136.001); (7) outbound connections to RemotePC infrastructure from hosts where RemotePC is not authorized (T1219). Malwarebytes ThreatDown has published specific IOCs; ingest these into SIEM and EDR blocklists immediately. The absence of a dropped ransom note means standard 'ransomware note file creation' alerts will not fire; detection must rely on behavioral indicators, not artifact-based signatures. Apply NIST AU-6 review cadence to RMM and RDP log sources at increased frequency during the monitoring period.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/new-prinz-eugen-ransomware-prioritizes-recent-files-for-encryption/`	BleepingComputer report linking to Malwarebytes ThreatDown IOC publication — retrieve current IOC list from this source	HIGH

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1219** — Remote Access Tools
- **T1083** — File and Directory Discovery
- **T1036** — Masquerading
- **T1136.001** — Local Account
- **T1070.004** — File Deletion

- **T1560** — Archive Collected Data
- **T1133** — External Remote Services
- **T1041** — Exfiltration Over C2 Channel
- **T1105** — Ingress Tool Transfer
- **T1021.001** — Remote Desktop Protocol
- **T1059** — Command and Scripting Interpreter
- **T1027** — Obfuscated Files or Information
- **T1562** — Impair Defenses
- **T1078** — Valid Accounts

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CA-7** — Continuous Monitoring
- **SI-4** — System Monitoring
- **SI-3** — Malicious Code Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **AC-2** — Account Management
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

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

- **A.8.24** — Use of cryptography

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1219	Remote Access Tools	Command-And-Control
T1083	File and Directory Discovery	Discovery
T1036	Masquerading	Defense-Evasion
T1136.001	Local Account	Persistence
T1070.004	File Deletion	Defense-Evasion
T1560	Archive Collected Data	Collection
T1133	External Remote Services	Persistence
T1041	Exfiltration Over C2 Channel	Exfiltration
T1105	Ingress Tool Transfer	Command-And-Control
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1059	Command and Scripting Interpreter	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1562	Impair Defenses	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-prinz-eugen-rans...	T3

Source	URL	Tier
What Is an RMM Tool? Security Risks Explained - Red Canary	https://redcanary.com/threat-detection-report/trends/rmm-tools/	T3
How Threat Actors Abuse Remote Management Tools - Huntress	https://www.huntress.com/blog/daisy-chaining-rogue-rmm-tools	T3
Your Screen Is Being Monitored: Initial Access via RMM Tools	https://reliaquest.com/blog/rmm-tool-abuse/	T3
Protecting Against Malicious Use of Remote Monitoring and ... - CISA	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a	T1

Generated 2026-06-20 18:48 UTC by TJS Security Command Center