Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

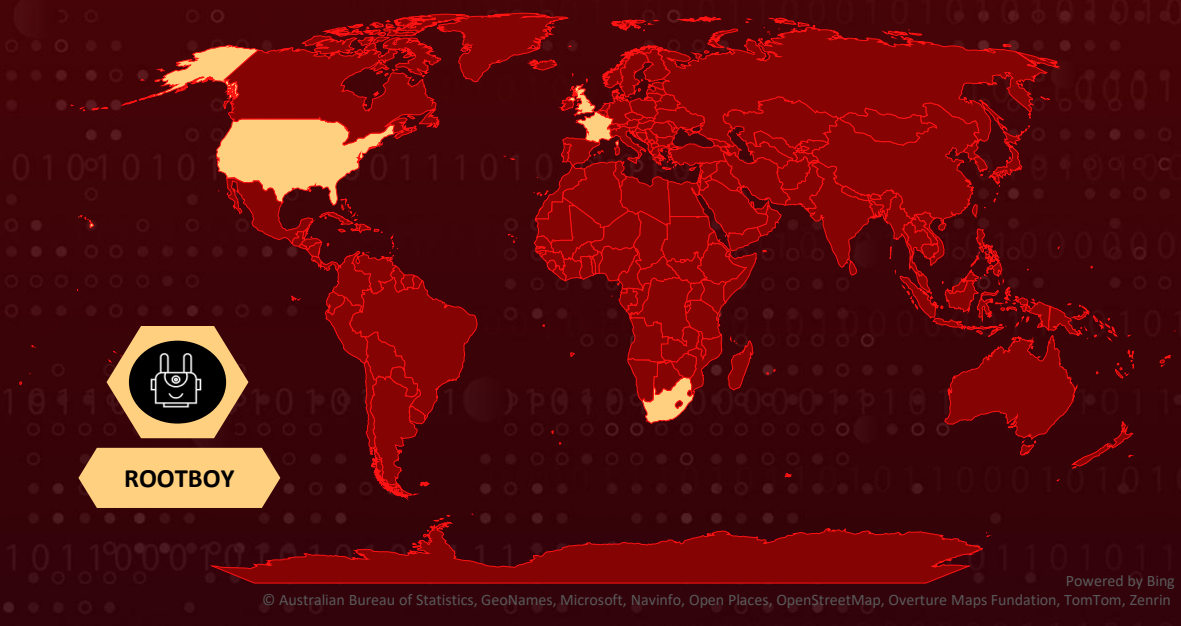
Prinz Eugen: A New Go-Based Ransomware Using Out-of-Band Extortion

Date of Publication	Admiralty Code	TA Number
June 30, 2026	B2	TA2026182

Summary

First Active: April 2026
Targeted Regions: South Africa, France, United States and the United Kingdom
Targeted Platform: Windows
Targeted Industries: Financial Services, Professional services, Education, and Automotive
Malware: Prinz Eugen Ransomware
Threat Actor: ROOTBOY (also operates as avtokz; extortion aliases GERMANIA)
Attack: Prinz Eugen is a new, financially motivated Go-based ransomware operation that surfaced publicly in April 2026, attributed to a likely single operator (ROOTBOY/GERMANIA) running a quiet double-extortion model: it enters through compromised RDP credentials, abuses the legitimate RemotePC RMM tool for PowerShell staging, steals data, encrypts with ChaCha20-Poly1305, and drops no on-disk ransom note in favor of out-of-band negotiation. The encryptor deliberately prioritizes recently modified files to maximize pressure and self-deletes with in-memory key wiping to frustrate forensics, while the actor exfiltrated roughly 1.2 TB from Standard Bank before staging escalating daily leaks once a 1 BTC demand was refused. With deliberate, custom-built tooling, opportunistic cross-sector targeting, and no available decryptor, organizations should treat Prinz Eugen as a serious exfiltration-and-extortion threat through 2026.

Attack Regions



Attack Details

#1 Prinz Eugen is a financially motivated, Go-based ransomware operation that surfaced publicly in April 2026, with the encryptor first analyzed first-hand in May 2026. It runs a deliberately quiet double-extortion model, steal first, encrypt second, but drops no ransom note on disk, pushing all victim communication out-of-band through direct email and a Tor leak portal. A consistent German naming theme runs through the campaign (the cruiser-derived family name, the germania backdoor password, the Festung domains, and the scorched-earth-ausfc Go package).

#2 Attribution points, on current evidence, to a likely single operator tracked as ROOTBOY (previously avtokz on XSS), using the extortion alias GERMANIA, with 'Festung' appearing as a recurring theme in the campaign's C2 domains. The strongest link is a string recovered from the binary that matches an extortion alias the same actor used on a crime forum months before Prinz Eugen existed, tying the encryptor to a named, pre-existing data seller.

#3 Initial access in the investigated intrusion is assessed to have come through compromised RDP credentials, after which the operator used Chrome to download the encryptor (servertool.exe) into the user's Music folder. Persistence relied on a manually created backdoor local administrator (net user admin germania /add) and abuse of the legitimate RemotePC (IDrive) RMM tool to launch PowerShell stagers, a Living-off-the-Land, hands-on-keyboard style. Reporting on the Standard Bank case describes roughly three weeks of dwell time and lateral movement through enterprise applications and databases.

#4 The encryptor performs a fully recursive, depth-unlimited directory walk and deliberately encrypts the most recently modified files first, the active, least-backed-up data, to maximize pressure to pay. It uses ChaCha20-Poly1305 with a 32-byte master key, per-file random IVs, a three-stage KDF (Argon2id to SHA-256 to HKDF-SHA256), 1 MB chunking, and a CHV1 file header, appending the .prinzeugen extension and optionally deleting originals via a --delete flag. Before exiting it zeroes its key in memory, forces garbage collection, and self-deletes through a cmd.exe ping-delay trick, anti-forensic measures that leave no key in memory and no binary on disk. No free decryptor exists.

#5 Targeting is opportunistic with no single-sector focus, with confirmed victims across Financial Services, professional services, Education, and Automotive in South Africa, France, the US and the UK. The model is exfiltration-led, ~1.2 TB stolen from Standard Bank, then escalating staged daily leaks after the 1 BTC demand was refused. Given the deliberate file-targeting, anti-forensic tradecraft, and credential-led, RMM-assisted intrusion model, organizations should treat Prinz Eugen as a serious exfiltration-and-extortion threat through 2026.

Recommendations

Lock Down and Monitor RDP Access: Prinz Eugen's investigated intrusion gained entry through compromised RDP credentials before any payload was staged. Eliminate internet-exposed RDP, place what remains behind VPN with enforced MFA, alert on anomalous or first-seen RDP logons, and treat affected remote-access credentials as compromised and reset them.

Audit and Restrict RMM Tooling: The operator abused the legitimate RemotePC (IDrive) RMM tool to launch PowerShell stagers and pull additional payloads. Inventory all remote-management software, block or alert on unsanctioned tools like RemotePC, and create high-priority detections for any RMM process spawning PowerShell.

Hunt Rogue Local-Administrator Creation: A backdoor admin was created manually with net user admin germania /add for persistence. Alert on net user … /add and new local-administrator additions from a single session, review local admin membership regularly, and flag suspicious account names such as "admin" or "germania.“

Detect the Encryptor and Its Anti-Forensics: The Go encryptor (servertool.exe) carries a CHV1 file header and a scorched-earth-ausfc package, appends .prinzeugen, then self-deletes via a cmd.exe ping-delay followed by del /F /Q. Deploy signatures and YARA for these artifacts and the known hash, and alert specifically on that self-delete sequence in user-profile directories.

Maintain Offline, Immutable Backups and Protect Fresh Data: No decryptor exists, the --delete flag removes originals, and the encryptor hits the most recently modified files first across OneDrive and Google Drive mounts. Keep offline, immutable backups, apply high-frequency versioning to active data and cloud-sync paths, and routinely test restoration.

Constrain Exfiltration and Prepare for Out-of-Band Extortion: This is an exfiltration-led double-extortion model (~1.2 TB taken from Standard Bank) with no on-host note and negotiation conducted via Tor and direct email. Apply egress monitoring for bulk transfers, block the C2 host 212[.]80[.]7[.]74 and the Festung domains, and update IR playbooks for leak-site monitoring and staged-leak pressure.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
Initial Access	T1078: Valid Accounts	
	T1133: External Remote Services	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
Persistence	T1136: Create Account	T1136.001: Local Account
	T1219: Remote Access Software	
Defense Evasion	T1070: Indicator Removal	T1070.004: File Deletion
	T1027: Obfuscated Files or Information	
Discovery	T1083: File and Directory Discovery	
Lateral Movement	T1021: Remote Services	
Command and Control	T1105: Ingress Tool Transfer	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1486: Data Encrypted for Impact	
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	686213cc11d36af764de824801bced9366dfca3823fe0d51b752f74149bcf1f4
IPv4	212[.]80[.]7[.]74
Domains	stndrdbnk[.]cc, g-captchafestung[.]sbs, festung-e[.]duckdns[.]org
URLs	hxxps[:]//212[.]80[.]7[.]74/serverscan[.]ps1, hxxps[:]//212[.]80[.]7[.]74/stager/mini, hxxps[:]//212[.]80[.]7[.]74/stager/ps1, hxxp[:]//stndrdbnk[.]cc
Email	prinzeugen[@]mail2tor[.]co, standardbankcc[@]cock[.]li
TOR Address	prinzfkbjiazbrur4mjje6mntjc4vydx3iatkkzycufoylqcoo4y7pqd[.]onion, 6cudc5cqa2bjpwdhcwm2lj6dbqejjjqzeo6ipwvmbazr6cgu7vfk3dad[.]onion, prinzkpn6d3itrgcytmsmlcpt5mgwn3ihpck2hsed5cezlbtbi3wklid[.]onion
Bitcoin Address	bc1q2ztpcvqdaptej6uu2ywt9mrlatx6envu34rf0v
Tox ID	496187425B2944D73FBB17CAF3F9FD569B9ED3A08A497A8314CB4F27A51E65081ACEE1E22F21
Filename	servertool.exe
File Extension	.prinzeugen

Recent Breaches

http://www.drivingschoolsoftware.com
http://www.spratleys.co.uk
http://www.standardbank.com
https://www.transitionspro-cvl.fr/

References

https://www.threatdown.com/blog/prinz-eugen-ransomware-a-deep-dive-into-a-new-go-based-encryptor/

https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/prinz-eugen

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

June 30, 2026 • 05:30 AM

More at www.hivepro.com