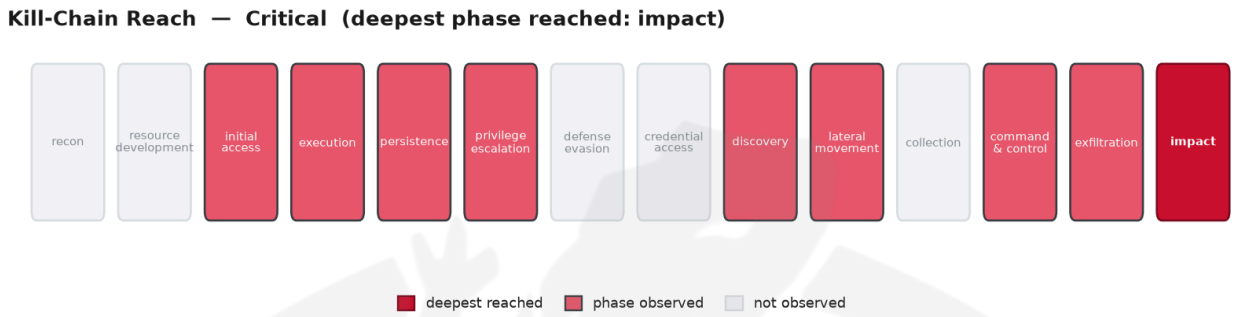
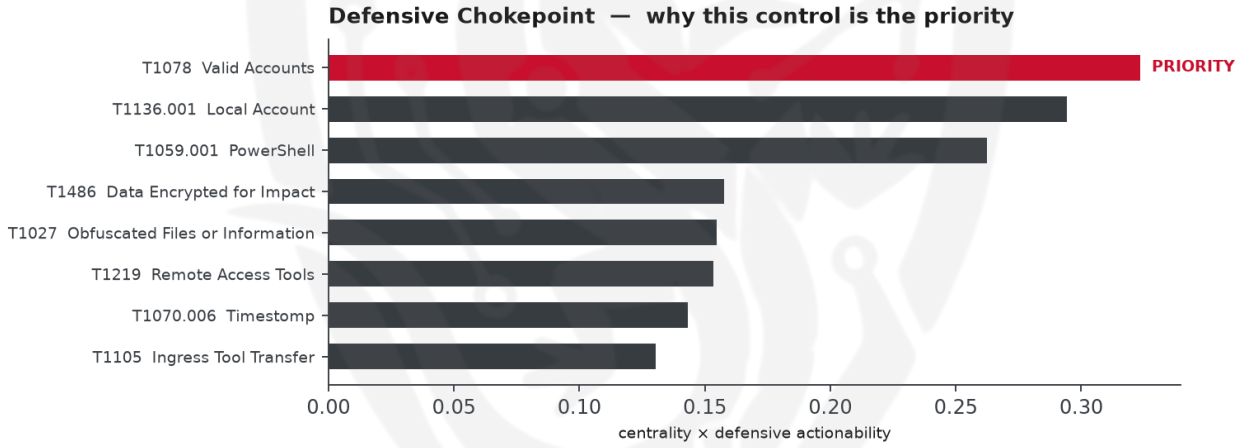
THREAT REPORT: ROOTBOY

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The source attributes this activity to ROOTBOY, a threat actor utilizing the Prinz Eugen ransomware to target organizations in South Africa, France, the United States of America, and Canada, primarily in the finance, government, and education sectors. The threat actor's campaign involves a range of techniques to impair defenses and exfiltrate data. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the threat. The threat actor's use of valid accounts is a key technique in their attack chain.

Threat Overview

The threat actor, attributed by the source to ROOTBOY, is using the Prinz Eugen malware family to target victims. The central vulnerability exploited is currently unknown. The threat actor is targeting organizations in multiple countries and sectors, including finance, government, and education.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving external remote services, service stop, impairing defenses, and data exfiltration. The priority technique is T1078 Valid Accounts, which is the graph chokepoint. To counter this, the priority control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

The malicious infrastructure is hosted on Play2Go International Limited. There are no corroborated malware families from abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, with the highest confidence seen being 0%. These findings are based on third-party enrichment and corroboration, and do not override the source pulse.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1133 External Remote Services
- T1489 Service Stop
- T1562 Impair Defenses
- T1567 Exfiltration Over Web Service
- T1219 Remote Access Tools
- T1070.006 Timestomp
- T1136.001 Local Account
- T1083 File and Directory Discovery
- T1059.001 PowerShell
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1070.004 File Deletion
- T1105 Ingress Tool Transfer
- T1021.001 Remote Desktop Protocol
- T1490 Inhibit System Recovery
- T1078.003 Local Accounts

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.3235).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4564; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
Akira	0.4564
FIN10	0.4339
APT18	0.4216
Play	0.4158
Medusa Group	0.3951

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	212[.]80[.]7[.]74	AbuseIPDB 0% (DE) · AS215439 Play2Go International Limited
Domain	6cudc5cqa2bjpwdhcwm2lj6dbqejjjqzeo6ipwvmbazr6cgu7vfk3dad[.]onion	
Domain	stndrdbnk[.]cc	
Domain	prinzfkbjiazbrur4mjje6mntjc4vydx3iatkkzycufoylqcoo4y7pqd[.]onion	
Domain	captchafestung[.]sbs	
Domain	darkempire[.]fun	

Type	Indicator	Context
Domain	g-captchafestung[.]sbs	
Domain	old-pidop[.]ru	
Domain	festung-e[.]duckdns[.]org	
URL	hxxps://212[.]80[.]7[.]74/serverscan[.]ps1	
URL	hxxps://212[.]80[.]7[.]74/stager/mini	
URL	hxxps://212[.]80[.]7[.]74/stager/ps1	
Hash	686213cc11d36af764de824801bced9366dfca3823fe0d51b752f74149bcf1f4	
Hash	17dd3f59f13f54a34761cef0c2b73cd7	
Hash	9d94e2a15b75e1ef4487429ac71fc13e186c4a2d	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.