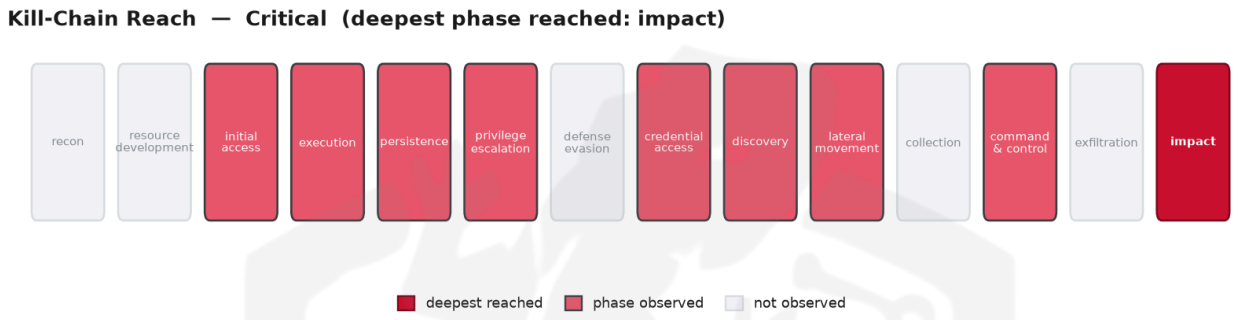
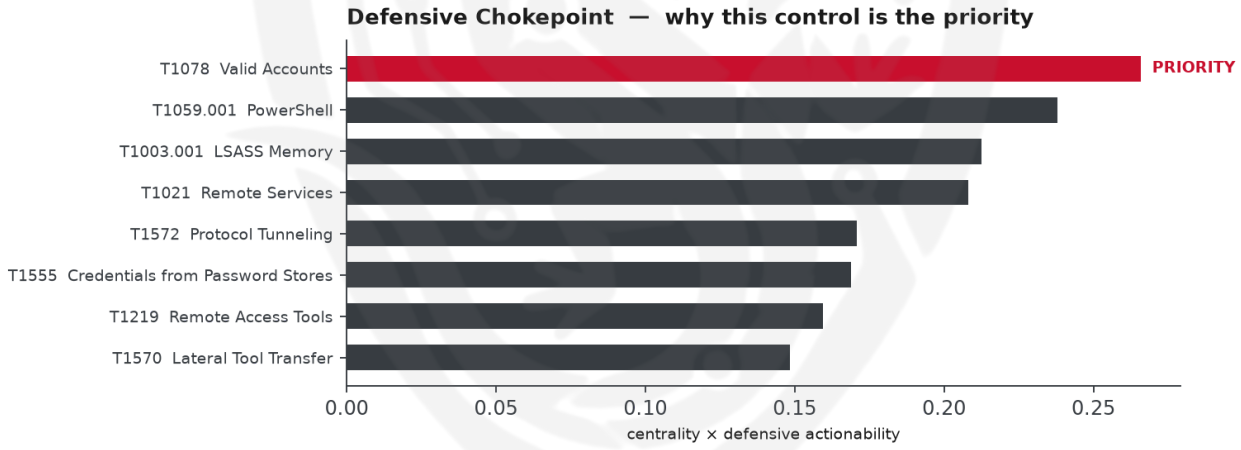
THREAT REPORT: TOY GHOULS' GENIELOCKER RANSOMWARE CAMPAIGN

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 Toy Ghouls, a threat actor targeting the Russian Federation's manufacturing, construction, finance, retail, and technology sectors with the GenieLocker ransomware. The actor is utilizing various techniques to compromise and encrypt data, making it a high-priority threat. Priority should be given to enforcing multi-factor authentication and disabling dormant accounts to mitigate the attack. The threat actor's use of valid accounts is a critical technique that requires immediate attention.

Threat Overview

Toy Ghouls, the attributed threat actor, is using the GenieLocker ransomware, along with other malware families such as RedAlert, LockBit, and Babuk, to target organizations in the Russian Federation. The victimology indicates that the threat actor is focusing on multiple sectors, including manufacturing,

construction, finance, retail, and technology. The central vulnerability exploited is currently unknown due to insufficient data.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving external remote services, service stop, system checks, and remote access tools. The priority technique identified is T1078 Valid Accounts, which is the graph chokepoint. To counter this, the lead 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 RoyaleHosting BV, as observed by third-party sources. However, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence level of 80% or higher, with the highest confidence seen being 0%. These findings are attributed to their respective sources, including RoyaleHosting BV and AbuseIPDB.

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
- T1497.001 System Checks
- T1021.004 SSH
- T1135 Network Share Discovery
- T1555 Credentials from Password Stores
- T1219 Remote Access Tools
- T1572 Protocol Tunneling
- T1021 Remote Services
- T1003.001 LSASS Memory
- T1083 File and Directory Discovery
- T1059.001 PowerShell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1486 Data Encrypted for Impact
- T1570 Lateral Tool Transfer
- T1027.002 Software Packing
- T1018 Remote System Discovery
- T1021.001 Remote Desktop Protocol
- T1490 Inhibit System Recovery

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2658).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4256; 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	0.4256
Medusa Group	0.3915
Fox Kitten	0.3689
Indrik Spider	0.365
Play	0.3525

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	89[.]125[.]66[.]101	AbuseIPDB 0% (NL) · AS212477 RoyaleHosting BV
Hash	18f61c6d686cffd131c9fd3f3437064b	
Hash	25480dad40152ef3d0c6d38eecc9bd9b	
Hash	34a7f28e0bb69b0d49bacc88bdf20ac1	
Hash	34b8828635f88078735799a3c1ac8e28	
Hash	3a4479b51890373bfc4a011ef41fe376	

Type	Indicator	Context
Hash	58c0dda52b8f069660166d61fd74f911	
Hash	5d62c1349b8981c396c9a23f4f8f053c	
Hash	780c8f4c6f077da4da96582987920362	
Hash	7dad78584795aa5c160520cc6accf260	
Hash	824ca1e906cc073ee5b0f3519df69a8f	
Hash	9201e35e2993612612919a3c71302cab	
Hash	9969a8221312dba70dd5cbddf83a146c	
Hash	9cd514ff2809ce0b993e3b8649e82a94	
Hash	a50eaaf514f4f84e61ca2455a8789753	
Hash	a8842616c9057d5cf6e1fe1fa8c3c160	
Hash	b893eafed0659f70d4ac250f09073723	
Hash	c68b6862725777651085650db34947fc	
Hash	d3e06eb34d8eee7ef92cac3ad0a20ff5	
Hash	d661cf666b9acbab7cfeae1127a261a9	
Hash	d87d0b01d95acc936b7dc47b8f41937a	
Hash	de3cfbb50f66079bfee20a6f64e59433	
Hash	f08f476f26b01d142ca73923de65fc0c	
Hash	f7b9e36e94163a9a303160945f99267a	
Hash	fd46a80c2f45577263328984edf7f4dc	

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

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1078 Valid Accounts (initial-access)

- **Observed here:** T1078 Valid Accounts was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 29+ groups that use Valid Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The Toy Ghouls could pivot to using T1047 Windows Management Instrumentation to maintain their access and evade detection, as this technique allows them to leverage the existing Windows management infrastructure to execute commands and gather information, potentially exploiting the trust placed in legitimate administrative tools. This technique may be particularly appealing to the Toy Ghouls as it enables them to blend their malicious activity with normal administrative tasks, making it more challenging for defenders to distinguish between legitimate and malicious behavior. To counter this potential move, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command