Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 23 - 29, 2025

Report Summary:

- **New Threat Detection Added**
  - GachiLoader

Weekly Detected Threats

The following threats were added to Crystal Eye this week:

1. GachiLoader

GachiLoader is Node.js-based malware loader that deploys infostealers. It is being used as part of a malware campaign dubbed YouTube Ghost Network, as it is being distributed through compromised accounts that are used to promote malicious videos.

The GachiLoader itself has its code heavily obfuscated, making static analysis difficult.

Threats Protected: 1
Class Type: Malware
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Reject	Drop

Kill Chain:

Tactic	Technique ID	Technique Name
Execution	T1059.007	Command and Scripting Interpreter: JavaScript
Defence Evasion	T1027.002	Obfuscated Files or Information: Software Packing
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocol

Current Threat Summary

Known exploited vulnerabilities (Week 4 December 2025)

Vulnerability	CVSS	Description
Digiever DS-2105 Pro	8.8	Digiever DS-2105 Pro contains a missing authorisation vulnerability which could allow for command injection via time_tzsetup.cgi endpoint.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-4th-week-of-december-2025/628

Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. In the past week, our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. This report provides a detailed analysis of PayoutsKing, an emerging data extortion group that has rapidly expanded operations targeting healthcare, government, and critical infrastructure sectors.

Ransomware Hits Last Week

Qilin dominated this week's ransomware landscape, responsible for 26.78% of all reported incidents. That level of share put it far ahead of every other actor, signalling either a concentrated campaign push or a sizeable batch of delayed victim disclosures landing in the same period.

A strong second tier was formed by SafePay (10.38%), Warlock (9.29%), Direwolf (7.65%), and Akira (6.01%). Together, this group represented a large chunk of overall activity, reflecting sustained, multi-victim operations and consistent publishing of new cases across regions and industries.

A broader mid-tier cluster, Lynx and DevMan2 (each 3.83%), Inc Ransom and The Gentlemen (each 3.28%), Sinobi and DragonForce (each 2.73%), followed by Anubis and Everest (each 2.19%), and RansomHouse (1.64%), maintained a steady operational tempo. None of these crews matched Qilin individually, but collectively they contributed a significant share of the week's observable pressure.

Smaller but still active operators included Play, Morpheus, Interlock, Nova, Worldleaks, Leaknet, Chaos, Nightspire (each 1.09%), with Coinbase Cartel, Handala, Benzona, Securotrop, BlackShrantac, Crypto24, Space Bears, PayoutsKing, Termite, KillSec3 (each 0.55%) appearing at low volumes. While these long-tail actors each accounted for only a small fraction of total incidents, their combined footprint underlines how fragmented and resilient the ransomware ecosystem remains.

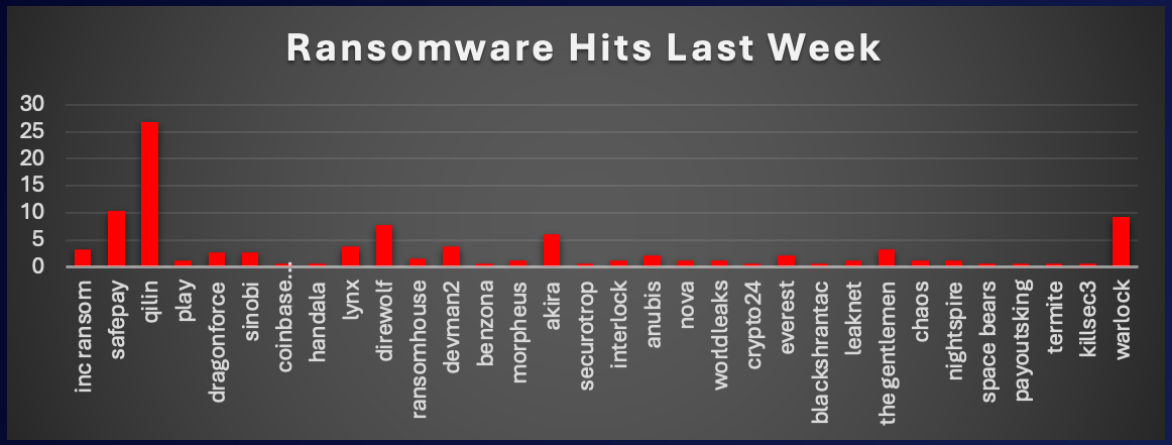


Figure 1: Ransomware Group Hits Last Week

PayoutsKing Ransomware

PayoutsKing is a relatively new ransomware/extortion group that emerged around mid-2025. Unlike many gangs, it explicitly claims not to operate as a Ransomware-as-a-Service (RaaS) and has no affiliates, meaning the core actors conduct attacks themselves. Within weeks of appearing, PayoutsKing accumulated numerous victims across different industries and countries. As of early July 2025, it had approximately 12 publicly claimed victims (about half in the U.S.), growing to over 20 by late July. By December 2025, the group had at least 43 victims listed on its dark web leak site, including organisations in manufacturing, healthcare, construction, education, finance, and more across the US, Europe, and elsewhere.

The group is profit-driven, focusing on double extortion – they encrypt files to disrupt victim operations and steal large volumes of data to pressure victims into paying. PayoutsKing's Tor leak site often initially redacts victim names (e.g. posting only a partial name) and later reveals the full identity along with proof of stolen data if ransom demands are not met. They have advertised extremely large data thefts (hundreds of GB to multiple TB of data) from some victims, underscoring the threat of sensitive information exposure.

Technically, PayoutsKing does not appear to introduce novel malware or techniques but rather uses established ransomware tactics effectively. Reports suggest their approach is pragmatic and opportunistic, exploiting common security gaps rather than advanced zero-days. Initial intrusion vectors are typically mundane – phishing emails carrying malware or credentials theft, reused or weak passwords, and exposed Remote Desktop services are frequently tied to their breaches. Once inside a network, the actors conduct internal reconnaissance and then deploy an encryption payload to lock files with the .payoutsking extension and drop a ransom note named PAYOUTS-README.txt.

In several cases, PayoutsKing also exfiltrated data before encryption, enabling them to threaten leaks (classic double-extortion). They maintain a Tor-based leak site for publishing stolen data and use an encrypted peer-to-peer Tox messenger ID for negotiations. The group employs sophisticated defence evasion techniques, including forcing systems into safe mode using bcdedit commands (similar to Snatch and Black Basta ransomware), which allows the ransomware to execute while security products are loaded with reduced functionality. They specifically target and terminate backup services, including Veeam and BackupExec, to prevent recovery.

PayoutsKing's rise in 2025 – from first sightings in June to dozens of victims by year's end – demonstrates how quickly a new group can inflict damage by leveraging common attack paths and aggressive extortion tactics. The group maintained operational activity throughout December 2025, with eight victims claimed between December 16-25, demonstrating continued threat operations. In summary, PayoutsKing is an independent ransomware operation defined by large-scale data theft, straightforward but effective techniques, and public shaming of victims to maximise pressure. It remains an active threat as of late 2025, with attacks observed in multiple regions.

Tactics, Techniques, and Procedures (TTPs)

PayoutsKing's operational TTPs align with many modern ransomware campaigns, combining credential-based intrusion, living-off-the-land tactics, data theft, and destruction of backups.

Initial Access
The group commonly gains entry via phishing and stolen or weak credentials. Spear-phishing emails carrying malware loaders or lures may be used to infect an initial machine. In other cases, PayoutsKing actors leverage compromised RDP/VPN accounts or other exposed remote services to directly access networks. There are no specific zero-day exploits attributed to PayoutsKing as of December 2025.

Execution
Once inside, the attackers execute the ransomware payload on target systems, often after hours or during weekends to avoid immediate detection. After gaining domain admin privileges, they might distribute the ransomware binary via SMB file shares or Active Directory group policy, then launch it using PowerShell or PsExec. The malware encrypts files on infected machines, appending the .payoutsking extension.

Privilege Escalation & Lateral Movement
The attackers harvest credentials using tools like Mimikatz or LSASS dumping to obtain admin hashes/passwords. Using these credentials, PayoutsKing moves laterally through SMB/Windows Admin Shares or Remote Desktop connections. They use PsExec/WMIC to remotely execute the ransomware on multiple machines, employing network discovery commands to map the environment.

Defence Evasion

PayoutsKing disables antivirus and endpoint security tools, turning off Microsoft Defender's real-time protection via registry or PowerShell. They inhibit system recovery by deleting backups and shadow copies using commands like vssadmin delete shadows /all /quiet or wmic shadowcopy delete.

A distinctive technique is safe boot modification via bcdedit /set {current} safeboot minimal. This forces infected systems to reboot into safe mode, where security products load with significantly reduced functionality. This technique, previously observed in Snatch and Black Basta ransomware, allows the encryption payload to execute with minimal interference. PayoutsKing specifically targets backup services using the sc stop VeeamTransportSvc and sc stop BackupExecAgentAccelerator commands.

Collection & Exfiltration

Data theft prior to encryption is a defining trait. The attackers locate sensitive data and exfiltrate hundreds of gigabytes to terabytes. Given PayoutsKing's use of Tor infrastructure, they likely exfiltrate data via encrypted channels to their dedicated .onion file servers. By the time ransomware is detonated, data has typically already been exfiltrated.

Command-and-Control

PayoutsKing does not use a long-running C2 beacon or custom backdoor. Communication for extortion is handled out-of-band using a TOX ID for peer-to-peer encrypted chat with victims, rather than a web portal or email. The leak site is on Tor with instructions to use Tox.

Impact

The primary impact is file encryption rendering systems unusable. PayoutsKing's ransomware encrypts files with the .payoutsking extension and drops the PAYOUTS-README.txt ransom note. If the ransom is not paid within the deadline, the group publishes stolen data on its leak site. They maximise damage by deleting backups and sometimes deleting log files or using anti-forensic measures.

MITRE ATT&CK Matrix for PayoutsKing

Tactic	Technique	ATT&CK ID
Initial Access	Spearphishing Attachment (malicious email)	T1566.001
Initial Access	Valid Accounts (stolen RDP/VPN credentials)	T1078.002
Execution	User Execution: Malicious File	T1204.002
Execution	Command-Line Interface (PowerShell, CMD)	T1059.003
Persistence	Scheduled Task/Job	T1053.005
Persistence	Create Account (local admin)	T1136.001
Privilege Escalation	OS Credential Dumping (LSASS)	T1003.001
Defence Evasion	Disable Security Tools	T1562.001
Defence Evasion	Safe Boot Modification	T1562.001
Credential Access	Credential Dumping (Mimikatz)	T1003.001
Discovery	Network Share Discovery	T1135
Discovery	Account Discovery (domain admins)	T1087.002
Lateral Movement	Remote Services (SMB/PsExec)	T1021.002
Lateral Movement	Remote Desktop Protocol	T1021.001
Collection	Archive Data (compress stolen files)	T1560.001
Collection	Data from Information Repositories	T1213
Exfiltration	Exfiltration Over C2 Channel (Tor)	T1041
Exfiltration	Exfiltration to Cloud Storage	T1567.002
Command-and-Control	Non-Standard Protocol (Tor)	T1090.003
Command-and-Control	Remote Access Software	T1219
Impact	Inhibit System Recovery (delete backups)	T1490
Impact	Data Encrypted for Impact	T1486
Impact	Data Destruction (backup/log wiping)	T1485

Indicators of Compromise (IOCs)

File Indicators

Encrypted File Extension: .payoutsking

Ransom Note Filename: PAYOUTS-README.txt

Malware Sample Hashes (SHA-256)

7a46ff94e373ea6c55d5e5a37cc87d15e1b99ff45080e9244d60a9c547b4e125

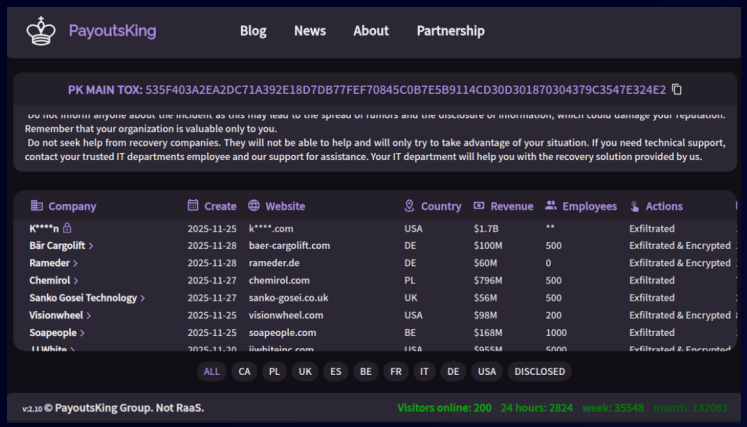
0d2e1c73321e3c41eae5f4dd95d67f1e53b1168a1e4628d0f1d5b938bcef8d91

Network Infrastructure

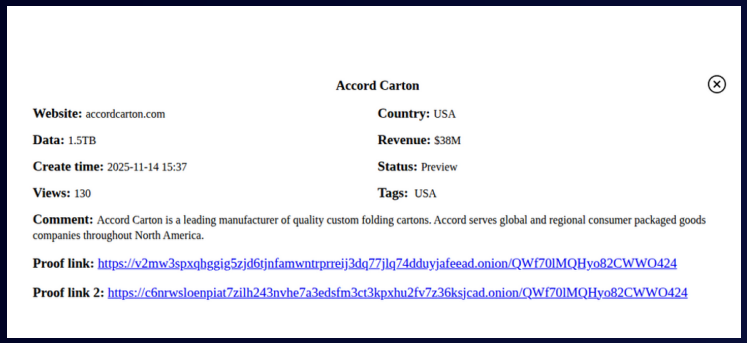
Tor Hidden Services:

Primary Leak Site:

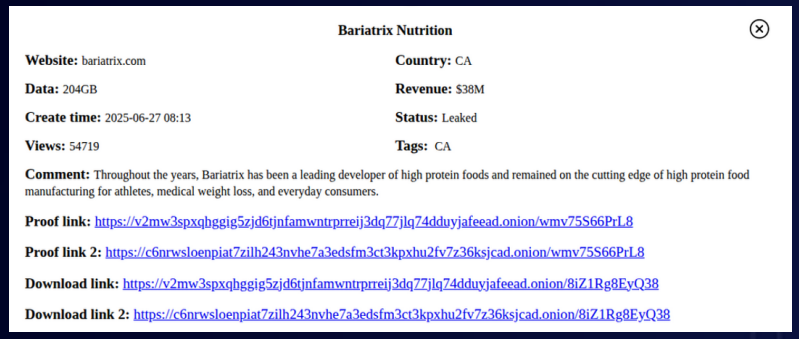
payoutsgn7cy6uliwevdqspncjpfxpmzgirwl2au65la7rfs5x3qnbqd.onion



Alternative Leak Site:
payouts7dlsgwf2rlbnfuvq27wlxud3nfbxbpbxvn4ehx3vwpwpwoydqd.onion



File Server 1: v2mw3spxqhggig5zjd6tjnfamwntrprreij3dq77jlq74dduyjafeead.onion



File Server 2: c6nrwsloenpiat7zilh243nvhe7a3edsfm3ct3kpxhu2fv7z36ksjcad.onion
Communication Infrastructure
Tox Messenger ID:
535F403A2EA2DC71A392E18D7DB77FEF70845C0B7E5B9114CD30D3018703043
79C3547E324E2
Process Artifacts
psexesvc.exe: PsExec service (lateral movement)
sqlwriter.exe: SQL VSS Writer (terminated pre-encryption)
defrag.exe: Scheduled task abuse
Remote Access Tools
AnyDesk
TeamViewer
Command-Line Indicators
vssadmin delete shadows /all /quiet
bcdedit /set {current} safeboot minimal
wmic shadowcopy delete
netsh advfirewall set allprofiles state off
sc stop VeeamTransportSvc
sc stop BackupExecAgentAccelerator
Registry Modifications
HKLM\SOFTWARE\Policies\Microsoft\Windows
Defender\DisableRealtimeMonitoring = 1

CE 5.5 MITIGATION

- Enable Anti-Phishing (all engines ON) – Signature, heuristic, SSL-mismatch and cloaked-URL detection to block phishing-led initial access.
- Enforce Web Filter policies – Block malicious categories, newly registered domains, risky MIME types and executable file extensions.
- Apply IDPS with network segmentation – Monitor lateral movement, exploit attempts and admin tool abuse with Security policy set to Alert.
- Activate DLP in Alert/Reject mode – Detect and disrupt outbound exfiltration of sensitive data used in double-extortion attacks.
- Enable SIEM Agent and alert escalation – Centralise ransomware indicators and accelerate SOC response through CE 5.5 event correlation.
- Deploy Anti-Malware File Scanner – Scan, quarantine and alert on dropped ransomware payloads and staging artifacts.

Worldwide Ransomware Victims

The United States remained the primary hotspot for ransomware activity, accounting for 40.44% of all identified victims. That means roughly four out of every ten known cases during this period were US-based, keeping it far ahead of any other single country in terms of exposure.

A strong second tier consisted of Germany (6.56%), Canada (6.01%), Brazil (4.92%), and the United Kingdom (3.83%). Together, these major economies formed the bulk of non-U.S. activity, reflecting mature digital infrastructure, high incident visibility, and attractive victim profiles for extortion operators.

A broad mid-band followed, led by Japan and Malaysia (each 2.73%), Italy (2.19%), and a cluster including France, Australia, Spain, Thailand, and Poland (each 1.64%). Beneath them, countries such as Peru, Paraguay, Tunisia, Guatemala, Bolivia, Finland, Argentina, New Zealand, Mexico (each 1.09%) showed that both established and emerging markets continue to feature regularly in victim data.

Below that, a long tail of single-incident geographies, Belgium, Singapore, Iran, Slovakia, Denmark, Chile, Oman, Egypt, Taiwan, Netherlands, Cyprus, China, Ireland, India, South Africa, Slovenia, Serbia, Switzerland, Bulgaria, Portugal, Russia, and Czech Republic (each 0.55%), appeared at low individual volumes. While each contributes only a small fraction, their combined footprint underlines that ransomware remains a globally distributed problem, touching dozens of countries rather than being confined to a handful of high-profile targets.

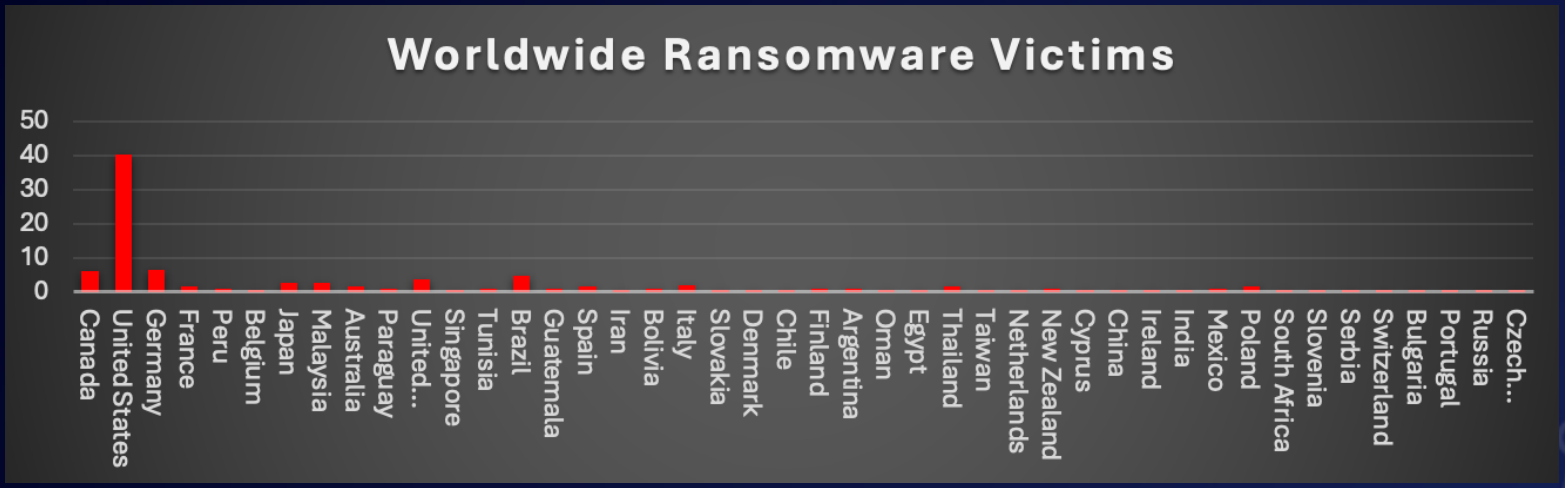


Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing remained the most heavily targeted sector this week, accounting for 18.03% of all identified ransomware victims. This keeps production environments and supply-chain–critical operations at the top of the risk ladder, where downtime directly translates into financial loss and gives threat actors strong leverage during extortion.

A powerful second tier consisted of Business Services (13.11%), Retail (11.48%), and Construction (11.48%). Together, these sectors represent a large band of project-driven, customer-facing, and service-oriented organisations that handle payments, contracts, and sensitive client data, exactly the mix attackers look for when choosing victims with both high urgency and high ability to pay.

A broad mid-band followed, led by IT and Hospitality (each 4.92%), Education and Finance (each 4.37%), and Transportation, Federal entities (each 3.28%), with Law Firms, Organisations, and Electronics (each 2.73%) also featured regularly in disclosures. This layer shows that knowledge-based industries, public sector bodies, and core service providers are now routine fixtures in the ransomware ecosystem rather than occasional outliers.

Lower-volume but still active verticals include Consumer Services, Energy, and Healthcare (each 2.19%), Real Estate and Agriculture (each 1.64%), and Telecommunications (1.09%), with Insurance and Architecture (each 0.55%) forming the long tail. While individually smaller in share, this spread makes it clear that ransomware pressure cuts across almost every major industry, if an organisation runs digital operations and holds monetisable data, it sits somewhere inside this threat envelope.

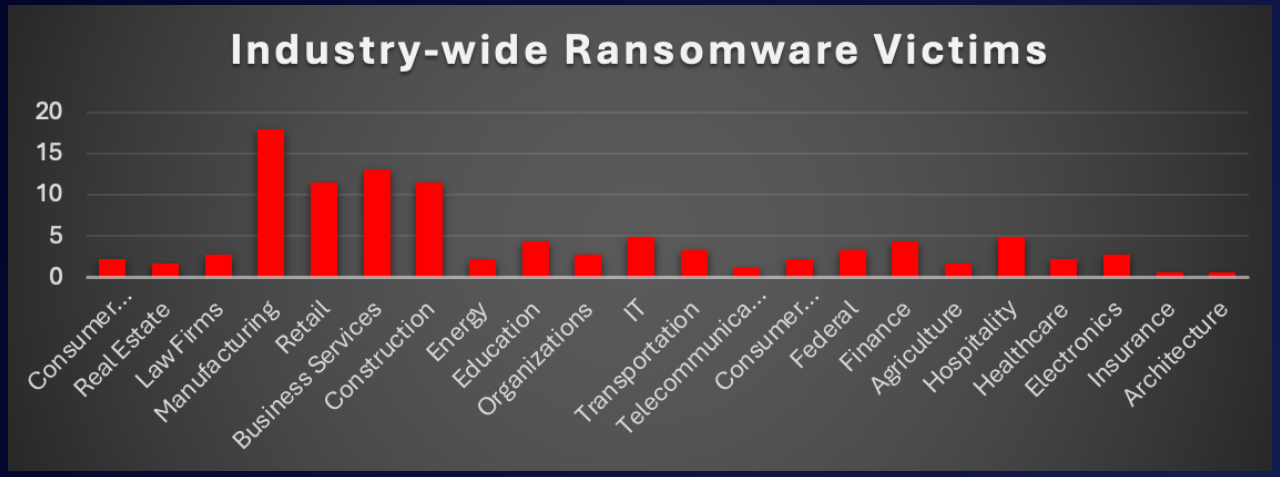


Figure 6: Industry-wide Ransomware Victims