Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 30, 2025 - Jan 05, 2026

Report Summary:

- **New Threat Detection Added**
  - ClickFix

- **Detection Summary**
  - **New Threat Protection: 76**
  - **Newly Detected Threats: 5**

Weekly Detected Threats

The following threats were added to Crystal Eye this week:

1. ClickFix

ClickFix is a social engineering attack technique that attempts to trick users into performing an action via keyboard combinations, resulting in the installation of additional malware. This technique has been employed by various threat actors to mimic everything from CAPTCHAs to error pages and is commonly integrated into phishing campaigns.

Threats Protected: 4
Class Type: Exploit Kit
Rule Set Type:

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

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spear phishing Attachment
	T1566.002	Phishing: Spear phishing Link
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1204.001	User Execution: Malicious Link
	T1204.004	User Execution: Malicious Copy and Paste

Current Threat Summary

Known exploited vulnerabilities (Week 1 January 2026)

Vulnerability	CVSS	Description
CVE-2025-14847	8.7	MongoDB Server contains a vulnerability within the zlib implementation that can allow an unauthenticated remote attacker to read uninitialised heap memory via an arbitrarily crafted zlib header. This vulnerability can result in the exposure of memory contents which may reveal additional information which can be used by an attacker in further attacks.

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-january-2026/629

Updated Malware Signatures (Week 1 January 2026)

Threat	Description
XWorm	A Remote Access Trojan (RAT) and malware loader that's commonly used in cyberattacks to give attackers full remote control over a victim's system. It's part of a growing trend of commercialised malware sold or rented on dark web forums, often under the guise of a “legitimate tool.”

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 BQTLock, an emerging Ransomware-as-a-Service (RaaS) platform.

Ransomware Hits Last Week

LockBit 5 overwhelmingly dominated this week's activity, responsible for 35.03% of all reported incidents. This gave it more than a third of the entire observable ecosystem, pointing to a major campaign push, a substantial wave of leak-site publications, or both, and putting it far ahead of every other active group.

A strong second tier was formed by Qilin (15.82%), SafePay (10.73%), and Play (7.34%), with DragonForce (5.08%) just behind. Collectively, these crews accounted for another large slice of global activity, reflecting sustained, multi-victim operations across multiple regions and sectors and confirming their status as some of the most aggressive LockBit-adjacent pressures in the ecosystem.

A mid-tier cluster, Inc Ransom and Ransomware Blog (each 3.39%), BQTLock (2.82%), DevMan2 (2.26%), and Handala and Leaknet (each 1.69%), followed by RansomHouse, Kazu, Walocker, and The Gentlemen (each 1.13%), maintained a steady operational tempo. These groups did not individually rival LockBit 5 or Qilin, but together they contributed a meaningful share of this week's double-extortion and data-theft activity.

Smaller but still active operators, Morpheus, Nova, Gunra, Medusa, Cloak, Space Bears, Rhysida, Nightspire, Everest, TridentLocker, and Interlock (each 0.56%), appeared at low volumes yet continued to populate the long tail of the ecosystem. Individually minor but collectively persistent, this long-tail activity underscores the fragmentation, churn, and resilience of the broader ransomware landscape even in weeks where one family, like LockBit 5, clearly dominates the headlines.

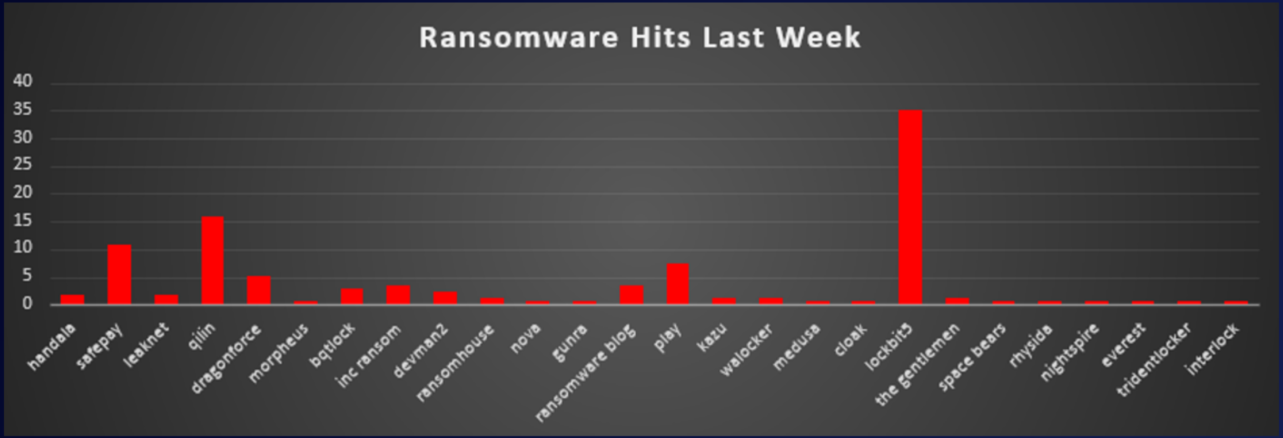


Figure 1: Ransomware Group Hits Last Week

BQTLock Ransomware

BQTLock is a ransomware family that emerged in mid-2025 and operates as a Ransomware-as-a-Service (RaaS) platform. It uses hybrid encryption, combining AES-256 for files with RSA-4096 for key protection, and appends the ".bqtlock" extension to encrypted files. The group follows a double-extortion model where victims receive ransom notes (typically named READ_ME-NOW with random identifiers) warning that failure to contact the attackers within 48 hours will double the ransom demand, and that decryption keys will be destroyed after 7 days. Following this deadline, stolen data may be published for sale. The group accepts Monero (XMR) cryptocurrency for payment using a tiered "wave" pricing scheme ranging from 13 XMR (Wave 1) up to 40 XMR (Wave 3) for standard decryption, though much larger ransoms have been demanded from high-value targets.

BQTLock is notable for blending ideological messaging with cybercrime operations. The operation appears to be led by individuals using the aliases "ZeroDayX" (also known as "ZeroDayX1") and "Fuch0u," who maintain connections to the pro-Palestinian hacktivist group Liwaa Mohammed. While the group frequently makes anti-Western and pro-Palestine statements in their communications, security researchers believe the primary motivation is financial gain rather than political activism. The operators develop the malware and recruit affiliates to conduct attacks in exchange for profit sharing. Starting in the Middle East region, BQTLock has expanded its targeting globally and demonstrates ongoing technical development with increasingly sophisticated capabilities. By late 2025, confirmed victims included organisations such as a US military alumni network, an American engineering firm, and various European businesses. The group tends to target sectors with potentially weaker security postures, including education, healthcare, small-to-medium enterprises, and local government, while also selecting targets that align with their stated political messaging, such as organisations in the United States, Europe, and Israel. Operations have continued into 2026, with an Israeli IT company suffering a significant 526GB data breach in January.

Detailed Tactics, Techniques, and Procedures (TTPs)

Initial Access

BQTLock operations typically begin through common entry methods. The group may exploit exposed Remote Desktop Protocol (RDP) services using credentials obtained through various means, including purchases from initial access brokers or targeting weak passwords. Phishing campaigns delivering ZIP archives are also used, with these files often disguised to appear as legitimate software updates. The archives contain the main malware executable (commonly named Update.exe) along with supporting DLL files. Other potential entry points include exploiting unpatched vulnerabilities in internet-facing applications.

Execution & Defence Evasion

Once executed, BQTLock creates a log file (bqt_log.txt) in the Windows Temp directory while avoiding sensitive system locations. The malware gathers basic system information and establishes a mutex with a unique identifier to prevent multiple infections on the same system. Several anti-analysis features are incorporated, including checks for debugging environments and virtual machine detection capabilities (though these may be disabled in early versions). The malware queries external services like icanhazip.com to determine the victim's public IP address. String obfuscation and runtime decoding techniques make static analysis more difficult for security researchers.

Privilege Escalation & Persistence

BQTLock seeks to run with elevated system privileges. It enables the SeDebugPrivilege token to interact with system-level processes. If administrative privileges are not already present, the malware may create a new local administrator account (for example, using names like "BQTLockAdmin" with simple passwords). The malware implements User Account Control (UAC) bypass techniques that vary by Windows version - these may involve abusing legitimate system utilities such as CMSTP.exe, fodhelper.exe, or eventvwr.exe through registry modifications. For maintaining access, BQTLock creates scheduled tasks that execute at system logon with high privileges, often using innocuous names that mimic legitimate Windows maintenance tasks. Some variants also employ process hollowing, where the malware injects its code into legitimate processes like explorer.exe to hide its presence.

Discovery & Credential Access

After gaining adequate privileges, BQTLock performs system reconnaissance, including collecting the computer name, username, and hardware identifiers. It enumerates all available drives and network shares to understand the scope of data available for encryption. More recent variants include credential harvesting capabilities targeting popular web browsers such as Chrome, Edge, Firefox, Opera, and Brave by accessing their password storage databases. Retrieved credentials are typically saved to temporary files for later exfiltration. The malware also captures screenshots of the victim's desktop. To ensure successful file encryption, BQTLock identifies and terminates certain processes, particularly security software and backup services, that might interfere with its operations. It also executes commands to delete Volume Shadow Copies and disable Windows recovery features, limiting the victim's ability to restore data without paying.

Command-and-Control & Exfiltration

BQTLock establishes contact with the command-and-control infrastructure to report successful infections. Observed C2 servers include specific IP addresses that host control panels for the operators. The malware transmits system information, including the OS version, hostname, created account credentials, public IP address, hardware identifiers, and campaign tracking data. In response, the C2 server provides a unique identifier that gets embedded in the ransom note to facilitate victim tracking. The malware includes backup C2 mechanisms using platforms like Telegram's bot API and Discord webhooks, which help the traffic blend with normal communications while providing operators with instant notifications. Stolen data, including screenshots and harvested credentials, is exfiltrated via HTTP/HTTPS connections to these alternative channels.

Impact and Encryption

Prior to encrypting files, BQTLock may modify the victim's desktop wallpaper to display a ransom message and change file icons to visually signal the attack. The malware then scans the file system for encryption targets, typically avoiding system directories and very large files to maintain system stability. Using multi-threaded processing for speed, BQTLock encrypts files using a hybrid approach: it generates random AES-256 encryption keys for each file, then encrypts those keys with an embedded RSA-4096 public key. This makes recovery without the attacker's private decryption key essentially impossible. Files are temporarily renamed during processing before receiving the final .bqtlock extension. Ransom notes are placed in directories throughout the system, providing contact instructions. After encryption, the malware typically removes itself from the system to reduce forensic evidence. The operators then leverage their dual-extortion approach: the ransom notes provide contact methods and threaten both permanent data loss if the ransom isn't paid within 7 days, and public release of stolen data on their Tor-based leak site if negotiations fail.

MITRE ATT&CK TTP Matrix

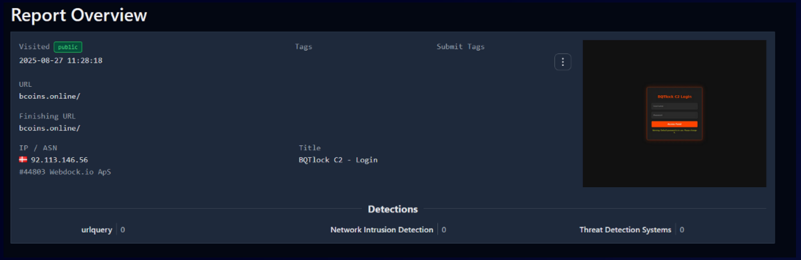
The table below summarises BQTLock's tactics and techniques mapped to the MITRE ATT&CK framework:

Tactic	Technique	ATT&CK ID
Initial Access	Valid Accounts: Use of stolen or weak RDP credentials	T1078
Initial Access	Phishing: Delivery via malicious ZIP archives	T1566
Initial Access	Exploit Public-Facing Application	T1190
Execution	User Execution: Malicious file execution	T1204
Execution	Windows Management Instrumentation	T1047
Execution	Process Injection: Process Hollowing	T1055.012
Execution	Command and Scripting Interpreter	T1059
Persistence	Scheduled Task/Job	T1053
Persistence	Create Account: Local Account	T1136.001
Persistence	Modify Registry	T1112
Privilege Escalation	Bypass User Account Control	T1548.002
Privilege Escalation	Access Token Manipulation	T1134
Defence Evasion	Masquerading	T1036
Defence Evasion	Indicator Removal: File Deletion	T1070.004
Defence Evasion	Virtualization/Sandbox Evasion	T1497
Defence Evasion	Impair Defences: Disable or Modify Tools	T1562.001
Defence Evasion	Debugger Evasion	T1622
Credential Access	Credentials from Web Browsers	T1555.003
Credential Access	OS Credential Dumping	T1003
Discovery	Process Discovery	T1057
Discovery	System Information Discovery	T1082
Discovery	File and Directory Discovery	T1083
Lateral Movement	Remote Services	T1021
Lateral Movement	Replication Through Removable Media	T1091
Collection	Data from Local System	T1005
Collection	Data Staged	T1074
Collection	Screen Capture	T1113
Command-and-Control	Application Layer Protocol: Web Protocols	T1071.001
Command-and-Control	Web Service	T1102
Exfiltration	Exfiltration Over C2 Channel	T1041
Exfiltration	Exfiltration Over Alternative Protocol	T1048.003
Impact	Data Encrypted for Impact	T1486
Impact	Inhibit System Recovery	T1490
Impact	Defacement	T1491

Note: This mapping represents observed and inferred techniques based on available reporting. As BQTLock continues to evolve, additional techniques may be employed by the operators and their affiliates.

Indicators of Compromise (IOCs)

Infrastructure / C2:
92.113.146[.]56 – BQTLock Command-and-Control server
208.99.44[.]55 – BQTLock Command-and-Control server
104.16.185[.]241 – HTTP C2 communication endpoint - bcoins[.]online



Report Overview

Visited public
2025-08-27 11:28:18

Tags

Submit Tags

URL
bcoins.online/

Finishing URL
bcoins.online/

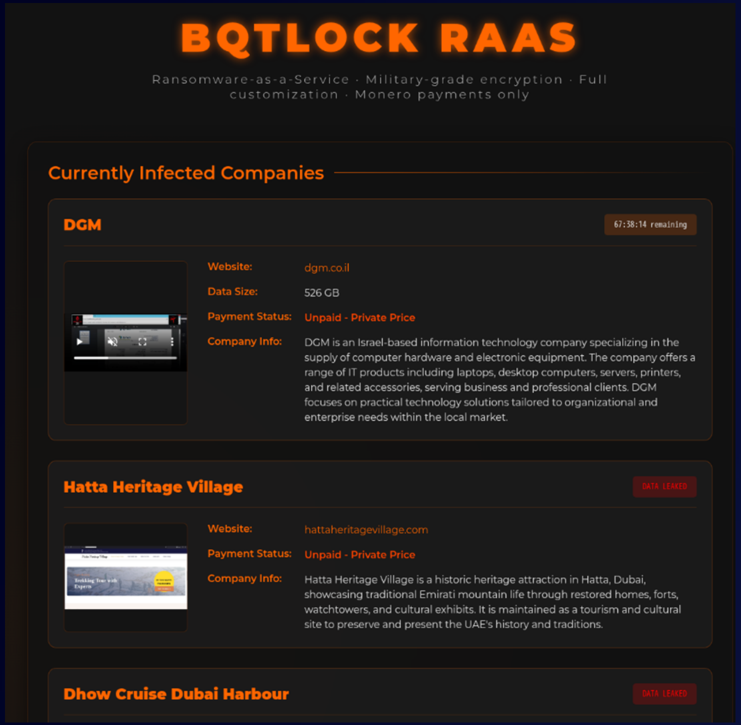
IP / ASN
92.113.146.56
#44803 Webdock.io ApS

Title
BQTlock C2 - Login

Detections

urlquery	Network Intrusion Detection	Threat Detection Systems
0	0	0

C2 panel domain
yywhylvqeqynzik6ibocb53o2nat7lmzn5ynjpar3stndzcgmy6dkgid[.]onion



BQTLOCK RAAS

Ransomware-as-a-Service · Military-grade encryption · Full customization · Monero payments only

Currently Infected Companies

DGM 67:38:14 remaining

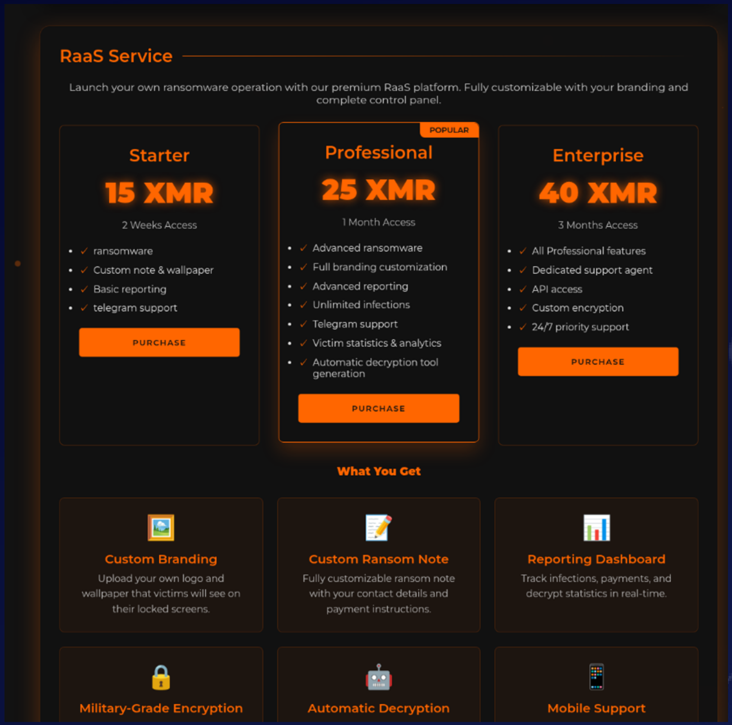
Website: dgm.co.il
Data Size: 526 GB
Payment Status: Unpaid - Private Price
Company Info: DGM is an Israel-based information technology company specializing in the supply of computer hardware and electronic equipment. The company offers a range of IT products including laptops, desktop computers, servers, printers, and related accessories, serving business and professional clients. DGM focuses on practical technology solutions tailored to organizational and enterprise needs within the local market.

Hatta Heritage Village DATA LEAKED

Website: hattaheritagevillage.com
Payment Status: Unpaid - Private Price
Company Info: Hatta Heritage Village is a historic heritage attraction in Hatta, Dubai, showcasing traditional Emirati mountain life through restored homes, forts, watchtowers, and cultural exhibits. It is maintained as a tourism and cultural site to preserve and present the UAE's history and traditions.

Dhow Cruise Dubai Harbour DATA LEAKED

Actor Communications: - Email: bqtlock@tutanmail.com, BQTlock@tutamail.com –



RaaS Service

Launch your own ransomware operation with our premium RaaS platform. Fully customizable with your branding and complete control panel.

Starter
15 XMR
2 Weeks Access
- ✓ ransomware
- ✓ Custom note & wallpaper
- ✓ Basic reporting
- ✓ telegram support

PURCHASE

POPULAR
Professional
25 XMR
1 Month Access
- ✓ Advanced ransomware
- ✓ Full branding customization
- ✓ Advanced reporting
- ✓ Unlimited infections
- ✓ Telegram support
- ✓ Victim statistics & analytics
- ✓ Automatic decryption tool generation

PURCHASE

Enterprise
40 XMR
3 Months Access
- ✓ All Professional features
- ✓ Dedicated support agent
- ✓ API access
- ✓ Custom encryption
- ✓ 24/7 priority support

PURCHASE

What You Get

Custom Branding
Upload your own logo and wallpaper that victims will see on their locked screens.

Custom Ransom Note
Fully customizable ransom note with your contact details and payment instructions.

Reporting Dashboard
Track infections, payments, and decrypt statistics in real-time.

Military-Grade Encryption

Automatic Decryption

Mobile Support

Monero Wallet:
89RQN2EUmiX6vL7nTv3viqUAgbDpN4ab329zPCEgbceQJuS233uye4eXtYk3MXAtVoKNMmzgVrxXphLZbJPtearY7QVuApr
Telegram Channels:
@BQTlock,
@BQTlock_raas,
@BQTosint,
@Fuch0u,
@ZeroDayX1,
@liwaamohammad,
@anonlb
Twitter/X: @zerodayx1,
@anonlb_

Malware Samples – SHA-256 File Hashes:
425b2f283b71237276f84d941d9c2982c7f61a9aff12ece10e15065b73b7165e
b211537ea626fae4ad2ef5ee2652633dc68aaf20da6eb953a44f266c4106b367
11affbeb18f4d6edcc9a4be5a82f8e23dfc31178887e97119faa5ddc75990494
00005ed250d85fc47e4c3883b8e6179a9888b8140acfeb94a40edc36bd523adb
a6a397fec6c109a1402c6f1144d647843b2093f65fedd27204b40ebeea0640b6
618070d597dd73c43ba5d4bde2baa93a4f6038e3279de3bafe688caa5c409a58
cd5e7b3b59cea14b804f6c01821d1ab94a0046422fe956f623b238c5db0cac99
4369aed581de0fe84c25a1ef2c3cf0bb6bf70df8b51fdf38b3b0b2a55f43261b
862f29aa00bb4ee33729bc6699990dbdf9ef890b8364f8288b173cb1ca5d6787
49f89b2fdef345a9d92fc821e4a226d8ac99e4ca0d2d11b5654f6557800b85f2
881b048234ebed82339244eb0c18580d785944dc82f83949f6adc1a9bc225c3b
f77c203d0c80598954c06a0f6f0c46f8b885ba423d12a21f13ded0168aa11b10
dacbba7f18d0835deb2eeb4e4d82c8f57234767291a90da1a5f3fd02d6bc13c2
fbd67a3bcc964e370931f620a85bf368d7b5797ebc1d53fe3be11a89a90e7961
10938c2d01dc999d2fe1f8c635e3705e7e663077935a17e730c849d1191c76ed
e2622ede1ebe5a37c439a32f0c63c13f893d1e5513b27367502898651cc5464b
590e47944ef0597bf1ff1d41656859b776e7031a4611cbf22d619002cbe49312
97524f4c582e0fbe46b74a7cfe4db9f078f368520cda25f27a50c5d2c50161f9
56eec59a5fe3f5a3c2c836701557bf1956770f465cd9e049995b86aef76a3e39
b61ae633616d7dd29aaf0b170fdfbe8f282c0f8bdcb1c52aedee473ce4bf5789
780e34c72404fd464669626ae554b81393d2bae95293284b375bb5d989914486
5b992a3438e344dddcdd66151a40efb3452b2ff37cdc40b37db612afeb29ed29
008ec0226066572f4b27f100d08443120b9dd55cefbec2bbff994b5b552e546c
0ccd3f2d7e6637eaf5414e35b97d9d8bf6b8e4182859cace8ca8e02377a4e62a
9547933dd46501af7fc095a3513e48b81178e344b86e075b679259875f0fd5a7
af90666822646e35eb52248f4a89eb715ce9f44459205bc24827a2aafe053548
324eabc27a25f524c94bb62573986b3335ab5181ddc6825d959d16aaaccdc7aa
b7796a3b1812f329c43d5d37bbb6d8032b7bc06b15af29f555eb3e0c7b1b1c3d
9cd62dbace332448712478712 7cff7c63a9f005d8d3aff9bac28c437e5caefc7

Ransom Note Filenames:
READ_ME-NOW_[random_ID].txt,
README_pay_DECRYPT.txt,
README_DECRYPT.txt
Encryption Extension:
.BQTLOCK or .bqtlock
Mutex: Global\{00A0B0C0-D0E0-F000-1000-200030004000}

Registry Keys Modified: HKCU\Software\Classes\ms-settings\Shell\Open\command (Windows 10 UAC bypass), HKCU\Software\Classes\mscfile\shell\open\command (Windows 7/8 UAC bypass)
Scheduled Tasks: Microsoft\Windows\Maintenance\SystemHealthCheck, BQTLock_Startup_[RandomID]
Local Account Created:
Username: BQTLockAdmin, Password: Password123! (added to Administrators group)
User-Agent String:
BQTLockClient
Defenders should monitor for connections to the listed C2 infrastructure, the presence of .bqtlock encrypted files, ransom notes with BQTLock identifiers, and the characteristic artifacts in the Windows Temp directory. Additional IOCs, including YARA rules and Sigma detection signatures, are available through community threat intelligence platforms.

Mitigation (Crystal Eye 5.5)

1. Boundary Firewalls and Internet Gateways: (30 words) Block inbound RDP from the internet, require VPN with multi-factor authentication. Block C2 IPs: 92.113.146.56, 208.99.44.55, 104.16.185.241, domain bcoins.online. Monitor Tor access, implement DNS filtering.
2. Secure Configuration: Apply the least privilege principle and disable unnecessary services. Configure UAC always-notify, restrict CMSTP.exe, fodhelper.exe, and eventvwr.exe. Implement application allowlisting. Enable Windows Defender Application Control against process hollowing attacks.
3. Access Control: Enforce strong passwords minimum twelve characters with complexity requirements. Implement multi-factor authentication for remote and administrative access. Monitor unexpected administrator account creation like "BQTLockAdmin". Review privileged accounts regularly.
4. Malware Protection: Deploy endpoint protection with real-time scanning across all systems. Enable behaviour-based detection for process hollowing and credential dumping. Configure anti-tampering protections. Implement email security with attachment sandboxing for ZIP archives.
5. Patch Management: Establish formal patch management prioritising internet-facing systems and known exploited vulnerabilities. Enable automatic updates where appropriate with testing procedures. Implement a risk-based approach, ensuring critical systems receive updates within fourteen days.
6. Backup and Recovery: Implement a three-two-one backup strategy: three copies, two media types, one offline. Ensure backups are inaccessible from production networks. Test restoration procedures regularly. Consider immutable backups preventing modification for specified retention periods.

Worldwide Ransomware Victims

The United States remained the primary hotspot for ransomware activity, accounting for 33.9% of all identified victims. Roughly one in three known cases this period were US-based, keeping it far ahead of any other single country in terms of observable exposure.

A strong second tier consisted of Germany (5.08%), Spain (5.08%), the United Kingdom (4.52%), India (3.95%), and Turkey (3.39%), with Canada (2.82%) close behind. Together, these major economies formed the bulk of non-US activity, reflecting large digital footprints, regular public disclosure of incidents, and attractive victim profiles for extortion operators.

A broader mid-band followed, including Israel, Italy, Poland, United Arab Emirates, France, and Switzerland (each 2.26%), alongside Brazil, Czech Republic, Portugal, Taiwan, and Saudi Arabia (each 1.69%), plus Netherlands, Mexico, South Korea, Argentina, Lithuania, Venezuela, Singapore, Austria, and Australia (each 1.13%). This group shows that ransomware remains deeply embedded across both established and emerging markets across Europe, the Middle East, Asia-Pacific, and the Americas.

Below that, a long tail of single-incident geographies, Dominican Republic, Guatemala, Uganda, Estonia, Kuwait, Malaysia, Indonesia, Greece, Iran, South Africa, Bangladesh, Zimbabwe, Thailand, New Zealand, Japan, and others (each 0.56%), appeared at low individual volumes. While each contributes only a small fraction of the total, their combined footprint underlines that ransomware is a globally distributed threat, touching dozens of countries rather than being confined to a handful of high-profile regions.

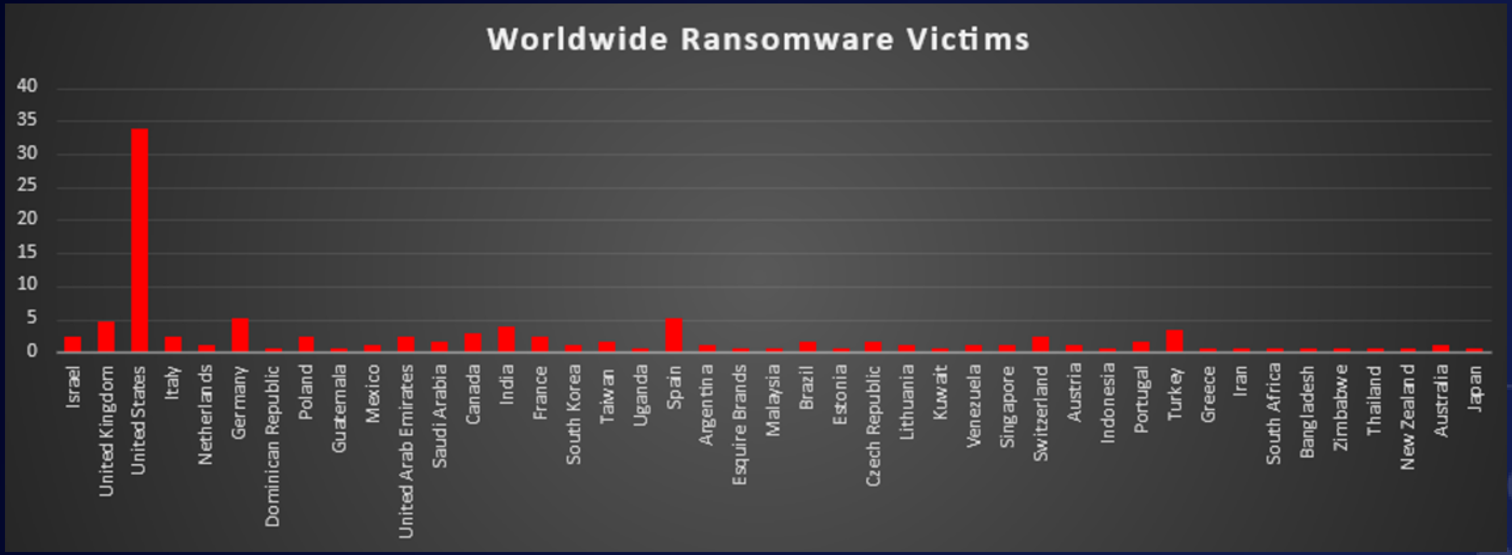


Figure 5: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing was again the most heavily targeted sector, accounting for 22.6% of all identified ransomware victims. That puts production environments and supply-chain–critical operations clearly at the top of the risk ladder, where even short outages translate into direct financial loss and give attackers strong leverage in negotiations.

A strong second tier consisted of Business Services (13.56%), Construction (9.6%), Retail (7.91%), and Education (7.34%). Together, these project-driven, service-oriented and customer-facing industries make up a large chunk of overall victim volume, reflecting heavy reliance on time-sensitive operations, contracts, and customer data, all prime pressure points for extortion.

A broad mid-band followed with Hospitality (5.08%), Healthcare and Finance (each 4.52%), IT and general “Organisations” (each 3.39%), and Energy (2.82%), supported by Consumer Services and Electronics (each 2.26%). This layer shows that both critical services and knowledge-based sectors are now routine fixtures in leak-site data rather than exceptions.

Lower-volume verticals included Federal, Agriculture, and Law Firms (each 1.69%), plus Real Estate, Minerals & Mining, Telecommunications (each 1.13%), and Transportation, Insurance, Media & Internet (each 0.56%), forming the long tail. Individually small but collectively meaningful, these figures underline that ransomware pressure is spread across almost every major industry with digitised operations and monetisable data.

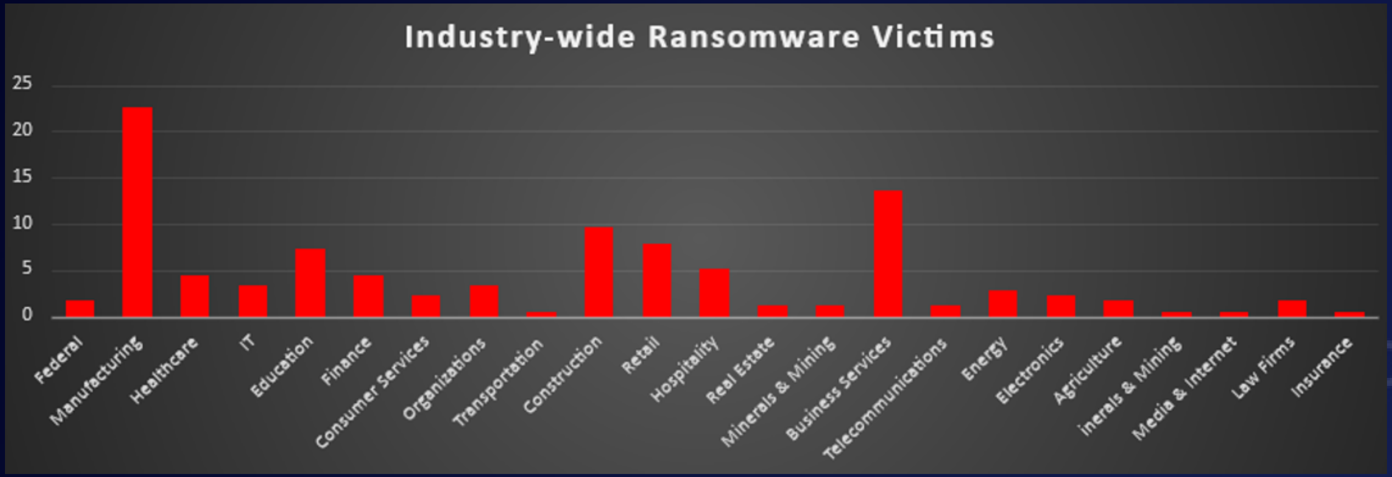


Figure 6: Industry-wide Ransomware Victims