THREAT INTELLIGENCE REPORT

January 6 – January 12, 2026

Red Piranha
unified threat management

Report Summary:

New Threat Detection Added

- MaskGramStealer
- DeskRat

Detection Summary

- New Threat Protection: 116
- Newly Detected Threats: 6

The following threats were added to Crystal Eye this week:

1. MaskGramStealer

MaskGramStealer is a Go-based information stealer primarily distributed through infected web downloads. It collects a variety of sensitive information from the infected device, including browser data, credentials, crypto wallets, installed software, and running processes, with the collected information exfiltrated over HTTP.

Threats Protected: 8
Class Type: Trojan-Activity
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	T1204.002	User Execution: Malicious File
Discovery	T1217	Browser Information Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
Collection	T1119	Automated Collection
	T1113	Screen Capture
Command-and-Control	T1071.001	Application Layer Protocol: Web Protocols
Exfiltration	T1041	Exfiltration Over C2 Channel

2. DeskRat

DeskRat is a Go-based Remote Access Tool (RAT) that has been observed in recent phishing campaigns by APT36. DeskRat has the capability to browse files, automatically exfiltrate files based on file extensions, as well as execute commands, with both communication and exfiltration of files via WebSockets.

Threats Protected: 5
Class Type: Trojan-Activity
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
Initial Access	T1566.001	Phishing: Spear phishing Attachment
	T1566.002	Phishing: Spear phishing Link
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
	T1204.001	User Execution: Malicious Link
	T1204.002	User Execution: Malicious File
Collection	T1119	Automated Collection
Command-and-Control	T1071.001	Application Layer Protocols: Web Protocols
Exfiltration	T1020	Automated Exfiltration
	T1041	Exfiltration Over C2 Channel

Current Threat Summary

Known Exploited Vulnerabilities (Week 2 - January 2026)

Vulnerability	CVSS	Description
CVE-2009-0556	8.8	Microsoft Office PowerPoint contains a vulnerability that can allow a remote attacker to execute code on the system upon opening a specially crafted PowerPoint file, resulting in an attacker gaining access to the system. This vulnerability affects end-of-life versions for Microsoft Office PowerPoint 2000 SP3, 2002 SP3, 2003 SP3 and Microsoft Office 2004 for Mac.
CVE-2025-37164	10	Hewlett Packard Enterprise (HPE) OneView contains a vulnerability that can allow a remote unauthenticated attacker to execute operating system commands on the system via a HTTP request, this vulnerability affects all versions through v10.20.

For more information, please visit the Red Piranha Forum:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-2nd-week-of-january-2026/632

Updated Malware Signatures (Week 2 - January 2026)

Threat	Description
Lumma Stealer	A type of malware classified as an information stealer. Its primary purpose is to steal sensitive information from infected systems, including but not limited to credentials, financial information, browser data, and potentially other personal or confidential information.

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

Ransomware Hits Last Week

Lynx led this week's activity, responsible for 18.4% of all reported incidents. This made it the single most dominant operator in the ecosystem, indicating a focused campaign window or a concentrated burst of victim disclosures that pushed Lynx ahead of every other active group.

Qilin followed closely with 16.8% of incidents, forming a powerful upper tier alongside Akira (12%) and Sinobi (12%). Together, this cluster represented a large share of all observed ransomware pressure, reflecting sustained, multi-victim operations and consistent leak-site publishing across multiple regions.

A solid mid-tier band included Direwolf (7.2%), Everest (4%), and a trio of groups, Inc Ransom, Interlock, and The Gentlemen (each 3.2%), supported by Handala, Play, and RansomHouse (each 2.4%). These actors did not individually rival Lynx or Qilin, but collectively they contributed a significant portion of global activity through ongoing double-extortion and data-theft campaigns.

Smaller but still active operators, Nova, Vect, Tengu, and Black Shrantac (each 1.6%), maintained a low- to mid-volume presence, adding persistent background noise to the ecosystem.

At the long tail, a wide set of brands, Chaos, Sicari, Brotherhood, Toufan, Rhysida, Medusa, Black Nevas, and Anubis (each 0.8%), appeared in low numbers. Individually minor yet collectively meaningful, this long-tail activity underscores the fragmentation, churn, and resilience of the broader ransomware landscape, even in weeks where a handful of families dominate the totals.

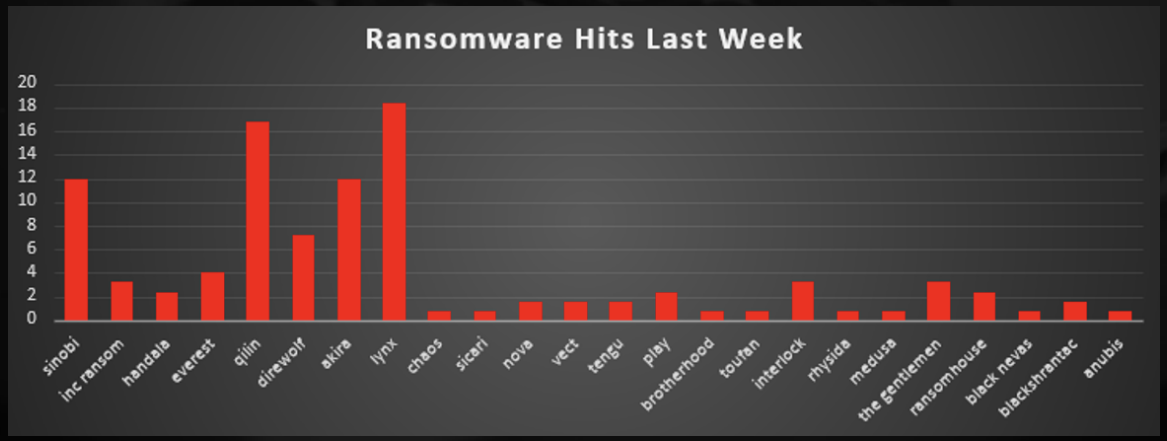


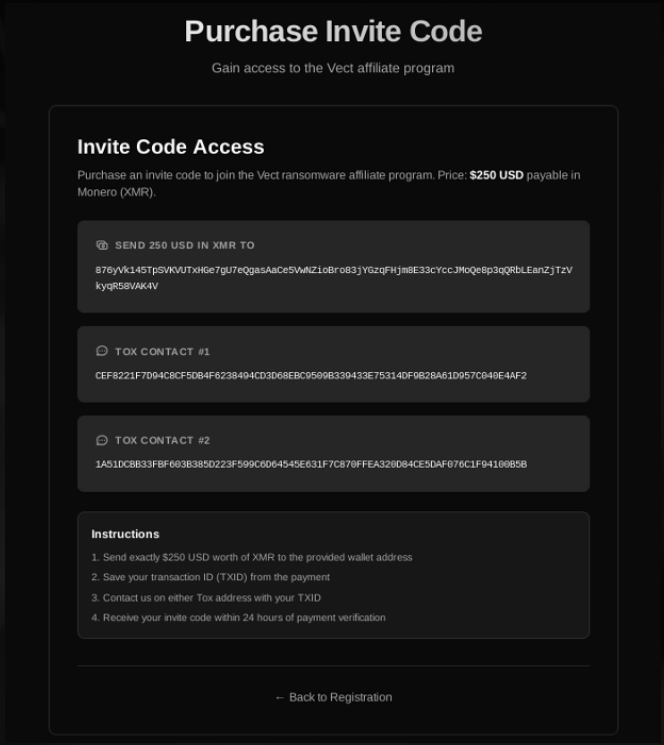
Figure 1: Ransomware Group Hits Last Week

Vect Ransomware

Vect is a newly emerged ransomware family operating as a Ransomware-as-a-Service (RaaS) platform that first appeared in early January 2026. The group claims to have developed custom malware entirely from scratch in C++ without relying on leaked ransomware code, distinguishing it from many contemporary operations that repurpose builders from LockBit 3.0 or Conti. Vect employs the modern ChaCha20-Poly1305 AEAD (Authenticated Encryption with Associated Data) encryption algorithm, which is approximately 2.5 times faster than AES-256-GCM on systems without hardware acceleration, making it highly effective for rapid file encryption across enterprise networks.

The operation demonstrates technical sophistication with multi-platform targeting capabilities spanning Windows, Linux, and VMware ESXi virtualisation environments. Vect's malware includes advanced features such as Windows Safe Mode boot manipulation to bypass security products, built-in LAN scanning for network reconnaissance via DFS and SMB protocols, and automated lateral movement through both SMB-based propagation and Windows Remote Management (WinRM) exploitation. The ransomware also handles Virtual Hard Disk (VHD) files specifically for virtual infrastructure targeting, and terminates security, database, and backup processes to ensure successful encryption.

Vect follows a strict double-extortion model where data is exfiltrated before encryption occurs. The group operates a professional TOR-based infrastructure, including an affiliate recruitment portal requiring a $250 USD entry fee paid in Monero cryptocurrency, a victim negotiation interface branded as "Vect Secure Chat," and a public data leak site titled "VECT RANSOMWARE // DATA ARCHIVE" where victim information is posted when ransom demands are not met. The affiliate program provides members with tiered commission structures, dedicated negotiator support, multilingual capabilities, and comprehensive management tools. Victims receive unique UUID-format Chat IDs in ransom notes, which authenticate them to the TOR-based negotiation portal.



The group's operational security is notable, utilising Monero for payments to maintain financial anonymity, TOX protocol for encrypted peer-to-peer affiliate communications, and exclusively TOR hidden services for infrastructure with no clearnet presence. This combination of custom-built malware, modern encryption, multi-platform capabilities, and strong OPSEC measures suggests Vect is operated by experienced threat actors who may represent a rebrand or new venture by established ransomware affiliates. Initial victims in January 2026 included organisations in Brazil and South Africa spanning the education and manufacturing sectors, with data theft claims ranging from 150GB to complete network compromise, including personally identifiable information and employee records.

Detailed Tactics, Techniques, and Procedures (TTPs)

1) Initial Access (Affiliate-driven RaaS)

- Enters via exposed RDP/VPN or stolen credentials.
- Phishing
- Possible vulnerable external endpoint.

2) Privilege Setup

- Attack requires admin rights to:
  - change boot settings (Safe Mode)
  - stop services/processes
  - push encryption across systems
- Likely achieved through:
  - credential dumping/harvested creds
  - existing admin access from initial compromise

3) Recon + Targeting

- Identifies:
  - file servers, shares, backups
  - virtualisation storage (VHD/VMDK)
  - critical services to kill (DB/backup/security)
- Goal: know what to steal and what to encrypt first.

4) Lateral Movement (Enterprise spread)

- Moves across the network using:
  - SMB admin shares (ADMIN$, C$)
  - remote execution
  - WinRM/PowerShell remoting
- Uses valid creds mass deployment.

5) Data Theft (Double-extortion phase)

- Steals sensitive data before encryption:
  - victim records, PII, internal docs
  - confirmed “large volume theft” claims (ex, 150GB)
- Data staged - exfiltrated.

6) Defence Evasion (Vect’s standout behaviour)

- Forces the infected system into Safe Mode before encryption to weaken EDR.

Typical boot modification:

- bcdedit /set {default} safeboot network
- bcdedit /set {current} safeboot minimal

Why: Safe Mode often prevents security drivers from loading encryption happens “blind”.

7) Process/Service Termination (Unlock + weaken recovery)

Vect kills anything that blocks file access or enables recovery:

- databases: SQL/MySQL/Oracle
- backup tools: Veeam/Commvault/Acronis
- security tooling / monitoring agents

This is done right before encryption.

8) Recovery Kill (Prevent rollback)

Runs commands like:

- vssadmin delete shadows /all /quiet
- wbadmin delete catalog -quiet

Purpose: ensure no easy restore path.

9) Encryption (Impact)

- Encrypts using ChaCha20-Poly1305 (reported)
- Likely multi-threaded fast network-wide impact
- File extension + ransom note name: not publicly confirmed yet

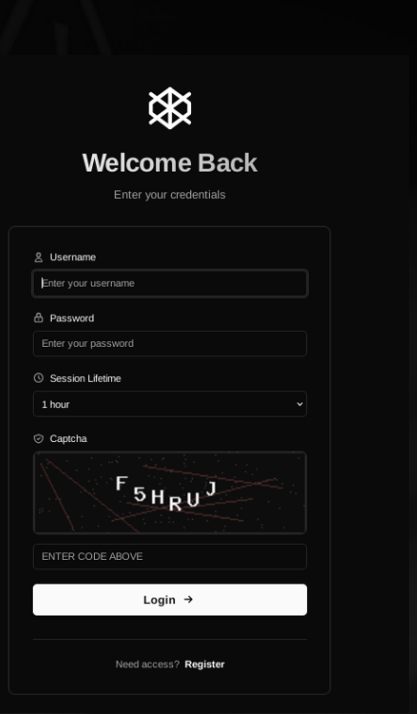
10) C2 / Negotiation/Leak

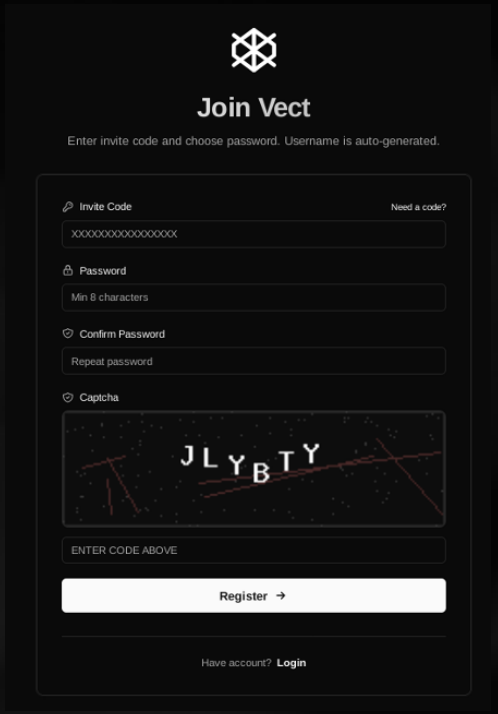
- Victim pushed to the negotiation portal:
  - Tor onion infrastructure
  - also observed clearnet negotiation server: 158.94.210.11:8000
- If no payment, stolen data is published on the leak site with countdown timers.

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

Tactic	Technique	ATT&CK ID
Initial Access	Valid Accounts: Stolen/weak credentials	T1078
Initial Access	External Remote Services: RDP/VPN	T1133
Initial Access	Phishing	T1566
Execution	Command and Scripting Interpreter	T1059
Persistence	Scheduled Task/Job (inferred)	T1053
Privilege Escalation	Access Token Manipulation (inferred)	T1134
Defence Evasion	Safe Mode Boot	T1562.009
Defence Evasion	Impair Defences: Disable Tools	T1562.001
Credential Access	OS Credential Dumping (inferred)	T1003
Discovery	Network Service Discovery: DFS/SMB	T1046
Discovery	System Information Discovery	T1082
Discovery	File and Directory Discovery	T1083
Lateral Movement	Remote Services: SMB/Admin Shares	T1021.002
Lateral Movement	Remote Services: WinRM	T1021.006
Collection	Data from Local System	T1005
Collection	Data from Network Shared Drive	T1039
Command-and-Control	Application Layer Protocol: Web	T1071.001
Command-and-Control	Encrypted Channel: TOR	T1573
Exfiltration	Exfiltration Over C2 Channel	T1041
Impact	Data Encrypted for Impact	T1486
Impact	Inhibit System Recovery	T1490
Impact	Service Stop	T1489

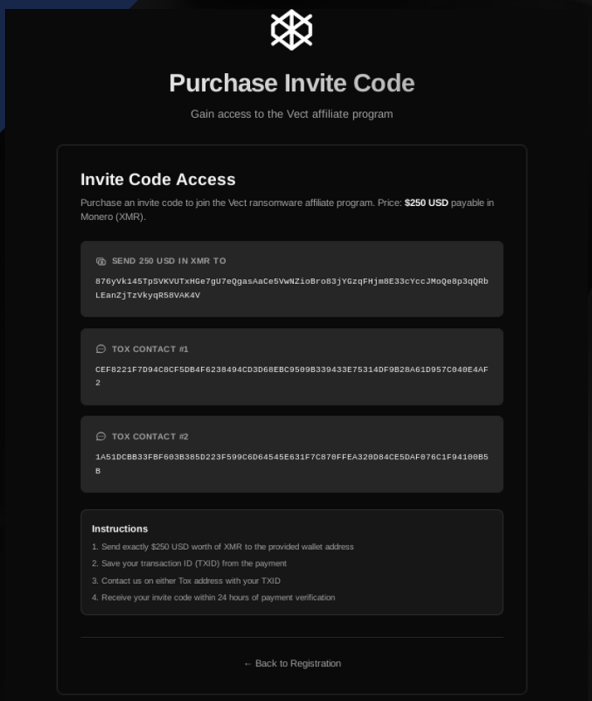
Indicators of Compromise (IOCs)
Infrastructure/C2:
Hosted IP: 158.94.210.11:8000
TOR Onion Domain (Primary Infrastructure):
bu7zr6fotni3qxxoxlcmpikwtp5mjzy7jkxt7akflnm2kwkbdtgtjuid[.]onion
- Hosts: Affiliate recruitment panel (/invite, /register, /login)
- Hosts: Victim negotiation portal (/chat)
- Hosts: Public data leak site (/) titled "VECT RANSOMWARE // DATA ARCHIVE"



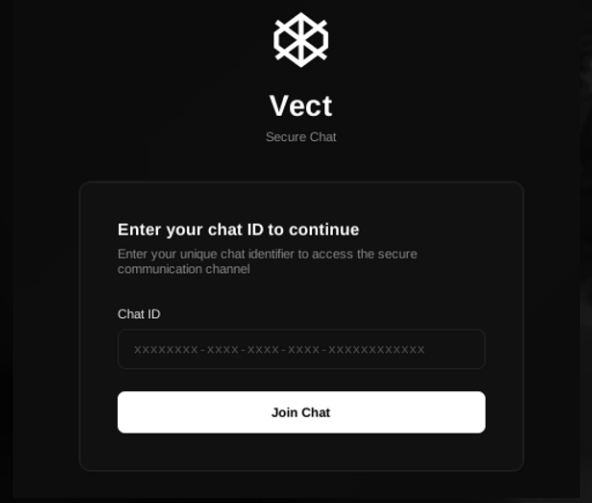


Cryptocurrency Wallets:
Monero (XMR) Wallet:
876yVkL4S7p5rWKbTxHs6e7gbTeqqas4AcC6WwMZ1d8r0B31jYBzqJFHJ88E33cYcc3jfKjQcBp3oqN8bLEan2JTzYkyq8RdVAkTv
Purpose: Affiliate invite code purchase ($250 USD equivalent)

Actor Communications:
TOX Protocol Contacts:
TOX Contact #1:
EEF8221F7D94C8CF0EBHF623B494C03D608EEC9649D83A9433E75314DFB828A01DD57C8A9E4AF2
TOX Contact #2:
1A51DCB233FB86038D802E23F599C6D64543E031FC87dFFEA32D8064CE9D04f70C1F041988B8



Victim Communication System:
Chat Portal Branding: "Vect Secure Chat"



Crystal Eye 5.5 Mitigation Strategies

- Perimeter Control: Block TOR nodes, onion DNS indicators, and restrict internet RDP; enforce VPN + MFA for remote access.
- Segmentation: Separate workstations, servers, and ESXi networks; block SMB/WinRM east-west traffic to stop lateral movement.
- Safe Mode Detection: Alert on bcdedit SafeBoot changes and SafeBoot registry modifications; treat as ransomware precursor activity.
- Endpoint Hardening: Enable EDR tamper protection; prevent process/service termination; application allowlisting to stop unauthorised binaries.
- Access Governance: Enforce MFA everywhere, strong passwords, least privilege, PAWs for admins, and remove stale/excessive privileged accounts.
- Backup Resilience: Use 3-2-1 backups with offline/immutable storage; isolate backup networks; test restore quarterly with runbooks.
- SIEM Correlation: Alert on vssadmin/wbadmin deletions, mass encryption behaviour, service stops, abnormal logons, and TOR traffic patterns.

Worldwide Ransomware Victims

The United States once again dominated the ransomware landscape, accounting for 50.4% of all identified victims this period. That means roughly one in every two known cases hit US-based organisations, keeping the country far ahead of any other single geography in terms of observable exposure.

A clear second tier consisted of Germany (6.4%) and Canada (6.4%), followed by Spain (4.8%) and France and Australia (each 4%). Together, these major economies form the bulk of non-U.S. activity, reflecting large digital footprints, regular breach disclosure, and victim profiles that attackers see as financially attractive.

A mid-band of countries included Malaysia and Italy (each 2.4%), along with Israel, Turkey, the United Kingdom, and India (each 1.6%). This group shows that ransomware pressure is not limited to North America and Western Europe; it is firmly entrenched across key markets in the Middle East and Asia-Pacific as well.

Below that sits a long tail of single-incident geographies, Serbia, Argentina, New Zealand, Singapore, Colombia, South Africa, Mexico, Romania, Poland, the Czech Republic, China, South Korea, Saudi Arabia, Brazil, the United Arab Emirates, and others (each 0.8%). Individually, they contribute only a small fraction of total volume, but collectively, they reinforce the same pattern seen week after week: ransomware is a global problem, touching dozens of countries rather than being confined to a handful of headline markets.

Figure 7: Ransomware Victims Worldwide

Industry-wide Ransomware Victims

Manufacturing and Business Services were the most heavily targeted sectors this week, each accounting for 16% of all identified ransomware victims. That puts production environments and service-heavy organisations jointly at the top of the risk ladder, where operational disruption and client-facing impact give attackers strong leverage during extortion.

A strong second tier consisted of Construction (14.4%) and Retail (14.4%), both of which rely on time-sensitive operations, complex supply chains, and high transaction volumes. For ransomware actors, these conditions create ideal pressure points, project delays, stock outages, and customer impact that can rapidly translate into payment pressure.

A substantial mid-band followed with Education (5.6%), Hospitality and Electronics (each 4%), and Finance (3.2%), supported by Minerals & Mining, Consumer Services, Healthcare, Energy, and Law Firms (each 2.4%). This layer shows that both critical services (finance, healthcare, energy) and data-rich, customer-facing verticals are now routine fixtures in victim disclosures rather than edge cases.

Lower volume but still active categories included Organisations, Media & Internet, Federal entities, Insurance, Transportation (each 1.6%), as well as Telecommunications, IT, and Real Estate (each 0.8%), forming the long tail. While individually smaller in share, this spread confirms that ransomware pressure cuts across almost every major industry with digitised operations and monetisable data, not just the classic “high value” targets.

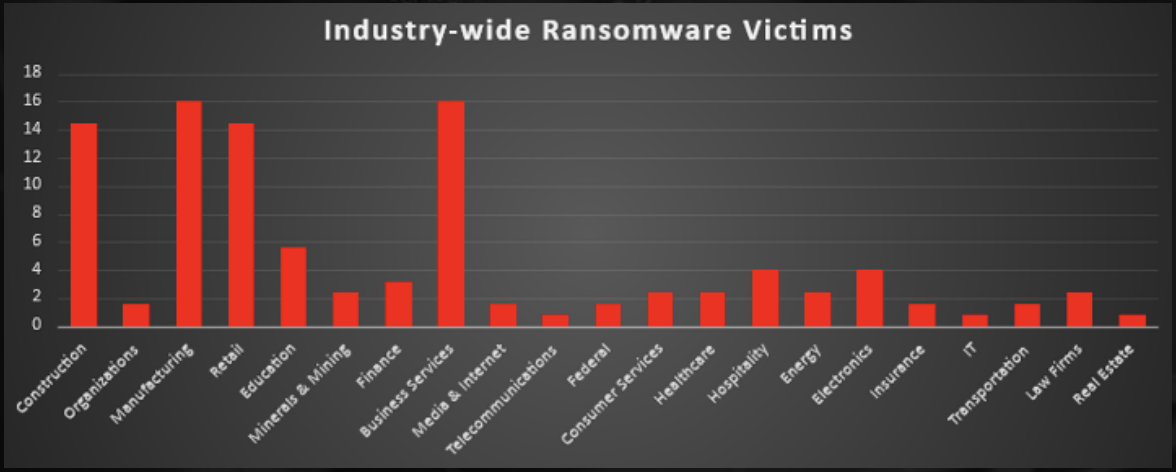


Figure 8: Industry-wide Ransomware Victims