Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Jan 14 - 20, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - SocGholish
  - Lumma Stealer
- **New Threat Protections - 182**

The following threats were added to Crystal Eye this week:

1. SocGholish

SocGholish is an opportunistic threat that employs malicious JavaScript injections in legitimate websites to deliver fake browser update prompts. When users interact with these prompts, they inadvertently download a .js file, often compressed within a .zip archive, leading to potential system compromise.

Rules Created: 39
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1204.001	User Execution: Malicious Script

2. Lumma Stealer

Lumma Stealer is a sophisticated malware that exploits fake CAPTCHA pages to distribute itself, targeting Windows users. The malware is distributed via phishing sites that trick victims into executing malicious PowerShell commands. Lumma Stealer steals sensitive data like credentials, financial information, and personal files. It leverages various CDN platforms for delivery and evades detection using base64 encoding and clipboard manipulation. This malware is particularly dangerous due to its stealth tactics and the growing trend of fake CAPTCHA attacks.

Rules Created: 121
Rule Set Type:

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

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.002	Spearphishing Link
Execution	T1059.001	PowerShell
Defence Evasion	T1027	Obfuscated Files or Information
Credential Access	T1115	Clipboard Data
Collection	T1056	Input Capture
Command-and-Control	T1095	Non-Application Layer Protocol

Known exploited vulnerabilities (Week 3 January 2024):

Vulnerability	CVSS	Description
CVE-2023-48365	9.9 (Critical)	Qlik Sense HTTP Tunnelling Vulnerability
CVE-2024-12686	7.2 (High)	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability
CVE-2025-21335	7.8 (High)	Microsoft Windows Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability
CVE-2025-21334	7.8 (High)	Microsoft Windows Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability
CVE-2025-21333	7.8 (High)	Microsoft Windows Hyper-V NT Kernel Integration VSP Heap-based Buffer Overflow Vulnerability
CVE-2024-55591	9.8 (Critical)	Fortinet FortiOS Authorization Bypass Vulnerability
CVE-2024-50603	10.0 (Critical)	Aviatrix Controllers OS Command Injection Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-3rd-week-of-january-2025/539

Updated Malware Signatures (Week 3 January 2024)

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.
Mirai	A malware that turns networked devices running out-of-date Linux-based firmware—such as routers, IP cameras, and other Internet of Things (IoT) devices—into remotely controlled bots. These bots are then used as part of a botnet in large-scale Distributed Denial of Service (DDoS) attacks.
Tofsee	A malware that is used to send spam emails, conduct click frauds as well as crypto mining.
Upatre	Upatre is also a malware dropper that downloads additional malware on an infected machine. It is usually observed to drop banking trojan after the initial infection.

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. Presented below is a detailed breakdown of ransomware group activities during this period.

Ransomware Group	Overall Percentage of total attack coverage
Blackbasta	6.72%
Lynx	14.29%
Hunters	3.36%
Inc Ransom	9.24%
Everest	5.04%
LockBit 3.0	6.72%
Dragonforce	1.68%
RansomHub	5.88%
Clop	2.52%
FunkSec	5.88%
Rhysida	0.84%
Sarcoma	2.52%
Leaked Data	4.2%
8Base	5.04%
Akira	4.2%
Fog	2.52%
Qilin	1.68%
Killsec3	1.68%
Space Bears	0.84%
Wikileaksv2	0.84%
SafePay	6.72%
Kairos	2.52%
Cactus	1.68%
Eraleign	0.84%
3Am	0.84%
Morpheus	0.84%

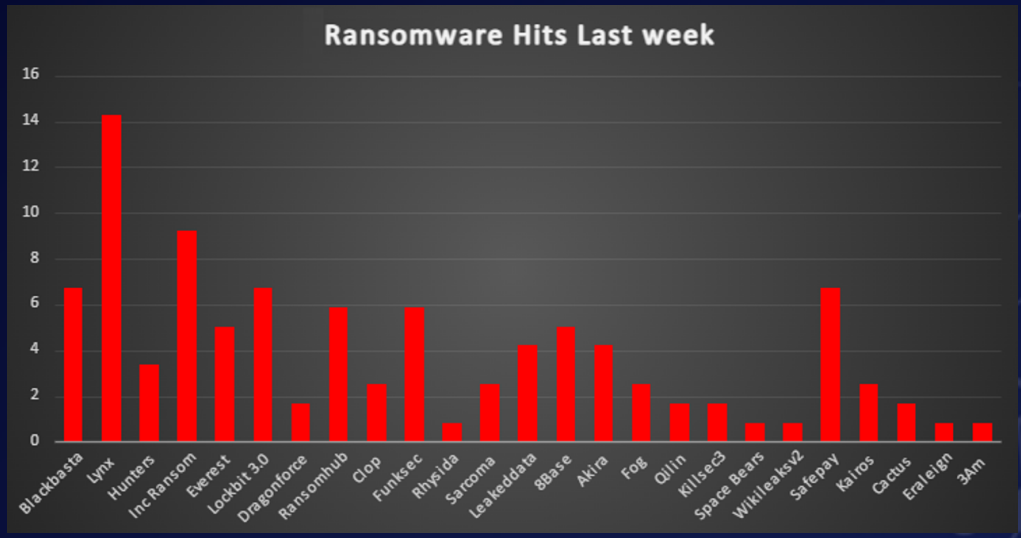

Figure 1: Ransomware Group Hits Last Week

Lynx Ransomware: INC Ransomware Revamped

In July 2024, Red Piranha researchers identified a ransomware strain named Lynx, believed to be a direct successor—or "rebrand"—of the INC ransomware family. Since its emergence, Lynx has actively targeted diverse industries, including retail, real estate, architecture, financial, and environmental services across the United States and the United Kingdom. While INC ransomware initially impacted both Windows and Linux platforms, only Windows-based Lynx samples have been confirmed so far, operating under a ransomware-as-a-service (RaaS) model.

A comparative analysis of the Lynx and INC ransomware binaries revealed an overall similarity score of approximately 48%, with a 70.8% overlap in functions. Although these shared elements strongly suggest code reuse, Red Piranha emphasises that the available evidence alone does not definitively prove Lynx's direct derivation from INC's source code. Nevertheless, the similarities point to critical overlapping capabilities and tactics.

```
C:\Users [redacted]c94ce3e72edccb6c2fea99ca49e299d>win.exe --help
Usage: win.exe <ARGUMENTS>
Arguments:
        --file <filePath>       Encrypt only specified file
        --dir <dirPath>         Encrypt only specified directory
        --help                  Print this message
        --verbose               Enable verbosity
        --stop-processes        Try to stop processes via RestartManager
        --encrypt-network       Encrypt network shares
        --load-drives           Load hidden drives
        --hide-cmd              Hide console window
        --no-background         Don't change background image
        --no-print              Don't print note on printers
        --kill                  Kill processes/services
```

Figure 2: Command-line options present in the malware

Detailed Tactics, Techniques, and Procedures (TTPs)

1. Delivery and Initial Compromise
   - Phishing Emails
     Lynx operators frequently utilise phishing emails carrying malicious attachments or embedded links. Unsuspecting users who open these attachments or click the links unwittingly install the ransomware.
   - Malicious Downloads
     Compromised websites, fake software updates, and malicious advertisements (malvertising) can also deliver Lynx onto target systems.
2. Process and Service Management
   - Termination of Key Services
     Lynx terminates processes and services—particularly those related to backups, databases, and security solutions—to prevent interference with the encryption process.
   - Use of RestartManager and System APIs
     System APIs (e.g., EnumDependentServicesW, ControlService) help enumerate and stop dependent services, ensuring maximum coverage during the attack.
3. Shadow Copy Deletion
   - Backup Removal
     By employing commands like vssadmin, Lynx deletes volume shadow copies to remove potential restore points, making data recovery more difficult for victims.
   - Success Logs
     Internal logging indicates successful deletion with messages such as "Successfully delete shadow copies from %c:," confirming the operation.
4. File Encryption
   - Robust Encryption Algorithms
     Lynx uses AES-128 (often in CTR mode) and Curve25519 to encrypt victim files. This dual-layered approach matches the sophistication seen in high-profile ransomware families.
   - Selective or Broad Targeting
     The ransomware can encrypt entire drives, network shares, or specific directories and file types through command-line options like –file, --dir <dirPath>, and –encrypt-network.
   - .lynx Extension & Ransom Note
     Once encrypted, files receive a ".lynx" extension. The ransom note is encoded with Base64 and instructs victims to access Tor-based chat portals to negotiate or obtain decryption keys.
5. Double Extortion
   - Data Exfiltration
     Before encrypting data, Lynx exfiltrates sensitive information, leveraging the threat of public disclosure to pressure victims into paying.
   - Anonymous Negotiation Channels
     Multiple Tor mirrors provide resilient, decentralised communication points. Even if one mirror is disrupted, attackers can remain operational through backups.
6. Ransomware-as-a-Service (RaaS)
   - Affiliate-Driven Model
     Lynx's RaaS structure enables affiliates—who join for a portion of the ransom proceeds—to deploy the malware. This approach broadens the ransomware's reach and fuels constant evolution in tactics.

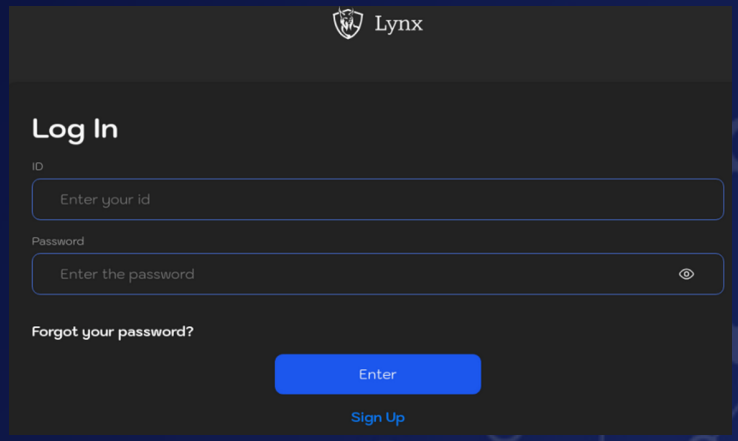

Figure 3: Login Screen of Lynx Ransomware

Indicators of Compromise (IOCs)
Red Piranha has identified several URLs and onion addresses linked to Lynx ransomware activity:

- Suspicious Domain:
  hxxp://lynxblog.net/
- Onion Sites (for login and disclosures):
  - hxxp://lynxch2k5xi35j7hlbmwl7d6u2oz4vp2wqp6qkwol624cod3d6iqiyqd[.]onion/login
  - hxxp://lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd[.]onion/disclosures
- Ransom Note Tor Mirrors:
  - hxxp://lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad.onion/login
  - hxxp://lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad.onion/login
  - hxxp://lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad.onion/login
  - hxxp://lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd.onion/login

Security teams should monitor for network traffic or DNS queries associated with these URLs, as any activity might indicate a compromise.

IOCs

file	02472036db9ec498ae565b344f099263f3218ecb785282150e8565d5cac92461
file	05e4f234a0f177949f375a56b1a875c9ca3d2bee97a2cb73fc2708914416c5a9
file	11cfd8e84704194ff9c56780858e9bbb9e82ff1b958149d74c43969d06ea10bd
file	1754c9973bac8260412e5ec34bf5156f5bb157aa797f95ff4fc905439b74357a
file	1a7c754ae1933338c740c807ec3dcf5e18e438356990761fdc2e75a2685ebf4a
file	29a25e971dbb87d3adcee75693782d978a3ca9f64df0a59b015ca519a4026c49
file	3156ee399296d55e56788b487701eb07fd5c49db04f80f5ab3dc5c4e3c071be0
file	36e3c83e50a19ad1048dab7814f3922631990578aab0790401bc67dbcc90a72e
file	508a644d552f237615d1504aa1628566fe0e752a5bc0c882fa72b3155c322cef
file	571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b
file	63e0d4e861048f581c9e5c64b28a053eb0023d58eebf2b943868d5f68a67a8b7
file	64b249eb3ab5993e7bcf5c0130e5f31cbd79dabdcad97268042780726e68533f
file	7f104a3dfda3a7fbdd9b910d00b0169328c5d2facc10dc17b4378612ffa82d51
file	82eb1910488657c78bef6879908526a2a2c6c31ab2f0517fcc5f3f6aa588b513
file	869d6ae8c0568e40086fd817766a503bfe130c805748e7880704985890aca947
file	9ac550187c7c27a52c80e1c61def1d3d5e6dbae0e4eaeacf1a493908ffd3ec7d
file	a0ceb258924ef004fa4efeef4bc0a86012afdb858e855ed14f1bbd31ca2e42f5
file	c41ab33986921c812c51e7a86bd3fd0691f5bba925fae612f1b717afaa2fe0ef
file	ca9d2440850b730ba03b3a4f410760961d15eb87e55ec502908d2546cd6f598c
file	d147b202e98ce73802d7501366a036ea8993c4c06cdfc6921899efdd22d159c6
file	e17c601551dfded76ab99a233957c5c4acf0229b46cd7fc2175ead7fe1e3d261
file	eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc
file	ee1d8ac9fef147f0751000c38ca5d72feceeaae803049a2cd49dcce15223b720
file	f96ecd567d9a05a6adb33f07880eebf1d6a8709512302e363377065ca8f98f56
file	fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced
file	fef674fce37d5de43a4d36e86b2c0851d738f110a0d48bae4b2dab4c6a2c373e
domain	lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd.onion
domain	lynxblog.net
domain	lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd.onion
domain	lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd.onion
domain	lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad.onion
domain	lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad.onion
domain	lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad.onion
domain	lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd.onion
domain	lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwdclrjngrfoid.onion
domain	lynxch2k5xi35j7hlbmwl7d6u2oz4vp2wqp6qkwol624cod3d6iqiyqd.onion
domain	lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd.onion
domain	lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7xx5doqd.onion
domain	lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd.onion
domain	lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd.onion
domain	lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad.onion
domain	lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad.onion
domain	lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad.onion

IP: lynxblog.net
176.53.146.99
185.185.70.215
185.254.158.169

Mitigations

1. Regular Backups and Offline Storage
2. Endpoint Protection and Monitoring
3. Network Segmentation
4. Patch Management and System Hardening
5. User Awareness and Phishing Prevention
6. Incident Response Preparedness

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States remains the most heavily impacted nation, accounting for a staggering 44.54% of global incidents—underscoring its continued vulnerability to ransomware threats. Brazil follows with 5.04% of recorded attacks, highlighting a prominent threat in South America. Meanwhile, Canada, Spain, and Italy each contribute 4.2% of global incidents, reflecting persistent risks in North America and Europe alike. Australia stands at 3.36%, pointing to continued concerns in the Asia-Pacific region.

The UK, France, and Colombia each recorded 2.52% of attacks, while the Netherlands, Mexico, India, the Czech Republic, Germany, and Egypt each accounted for 1.68%. A broader range of countries—including Belgium, Thailand, Dominica, a portion of the United States reported simply as "USA," Jamaica, Argentina, Uruguay, Indonesia, Jordan, Chile, Nigeria, an "Unknown" designation, Singapore, New Zealand, Ecuador, Malta, Mongolia, Poland, and Taiwan—each contributed 0.84% to the overall ransomware landscape.

This distribution illustrates the global and persistent nature of ransomware threats, with North America continuing to bear the brunt of attacks. The findings further emphasise the critical need for strengthened cybersecurity measures, proactive defence strategies, and heightened vigilance across all sectors to counter the unrelenting rise in ransomware incidents worldwide.

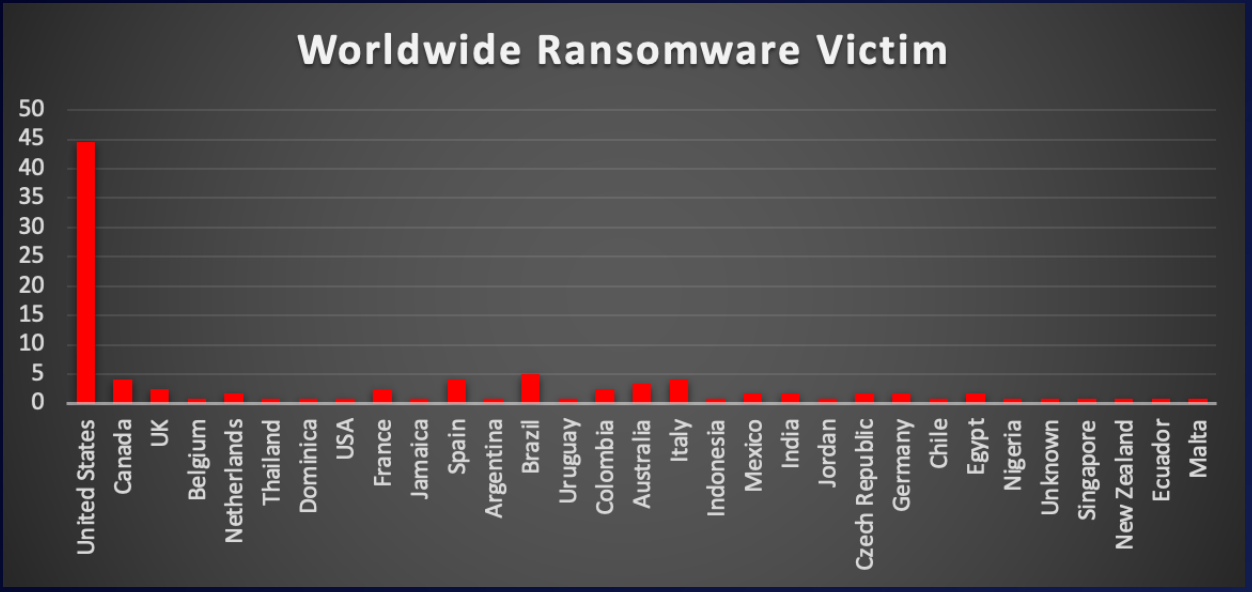

Figure 4: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis reveals Technology Services as the most targeted sector, accounting for 8.42% of the total reported incidents. Next in line are Manufacturing and Healthcare, each at 6.32%, followed by Construction at 5.79%. The Retail sector stands at 4.74%, illustrating the widespread nature of ransomware threats across multiple key industries.

Business Services and Law Firms both reported 3.16% of attacks. Government, Education, and Financial Services each recorded 2.63%, underscoring consistent risk levels in public, academic, and financial arenas. Further down the list, Food tallied 2.11%, while Real Estate and Accounting each contributed 1.58% of incidents. Industries such as Architecture, Non-Profit, Entertainment, Logistics, Insurance, and Hospitality each experienced 1.05% of ransomware attacks, highlighting a noticeable level of exposure across varied sectors. Meanwhile, Transportation, Technology (distinct from Technology Services), Food & Beverage, Telecommunications, Marketing, Automotive, Pharmaceuticals, Infrastructure, and Religion all showed smaller yet significant impacts at 0.53% each.

This analysis underscores the pervasive and indiscriminate nature of ransomware, cutting across critical infrastructure, public services, and commercial enterprises alike. Organisations must adopt robust cybersecurity frameworks, invest in proactive threat detection, and develop effective incident response strategies to mitigate the evolving ransomware landscape effectively.

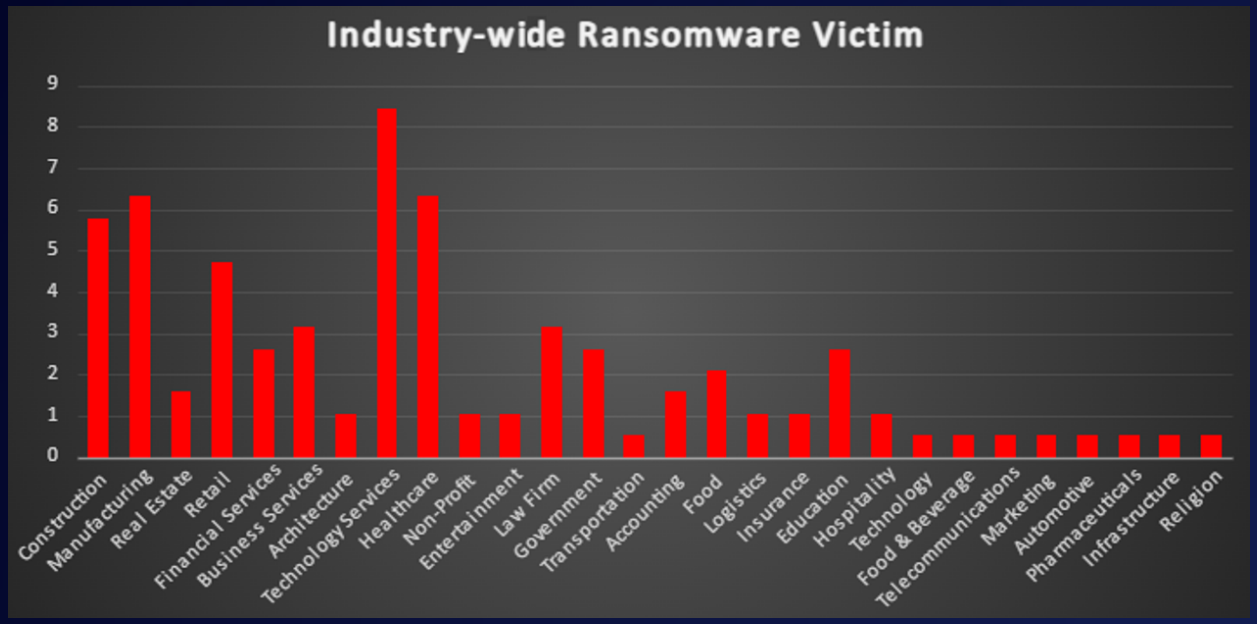

Figure 5: Industry-wide Ransomware Victims