Red Piranha
unified threat management

# THREAT INTELLIGENCE REPORT

July 29 - Aug 04, 2025

# Report Summary:

- **New Threat Detection Added**
  - Kimsuky

- **Detection Summary**
  - **Threat Protections integrated into the Crystal Eye - 120**
  - **Newly Detected Threats - 5**

# The following threats were added to Crystal Eye this week:

## 1. Kimsuky

Kimsuky is a North Korea-based APT. This group has been active since at least 2012. The group started off targeting South Korea but has expanded its targets to the United States, Japan, Russia and Europe.

These new threats have been found to target Korean users who use either Facebook, email or Telegram. Facebook users were sent friend requests by the threat actor, and then they were sent a specific malicious document. Email addresses were obtained from Facebook as well to try to lure the victim to open the malicious document. The Telegram approach is similar to other techniques except that it requests a mobile number from Facebook users.

The malicious document's end objective is to collect data from the device and transmit it to an actor-controlled domain. This domain also acts as a C2 connector, so the attackers can send custom commands to the infected device.

**Threats Protected: 11**
**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:** Command-and-Control/Domain-c2
**Kill Chain:**

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Establish Accounts | T1585.001 | Establish Accounts – Social Media Accounts |
|  | T1585.002 | Establish Accounts – Email Accounts |
| Command and Scripting Interpreter | T1059 | Execution |
| Collection | T1560 | Archive Collected Data |
| Command-and-Control | T1071.001 | Application Layer Protocol: Web Protocols |

# Current Threat Summary

## Known exploited vulnerabilities (Week 1 August 2025)

| Vulnerability | CVSS | Description |
|---|---|---|
| PaperCut NG/MF | 8.4 (High) | PaperCut NG/MF contains a cross-site request forgery (CSRF) vulnerability that can enable the configuration of the device upon visiting an external resource provided by an attacker. Once specific device configurations have been set, it is possible to achieve remote code execution on the printer via a print job sent across the network. |
| Cisco Identity Services Engine | 10 (Critical) | Cisco Identity Services Engine contains a vulnerability that can allow a remote unauthenticated attacker to execute arbitrary code on the device via an API request. Exploitation of this vulnerability can result in the ability to manage operating system commands with elevated permissions. |

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-5th-week-of-july-2025/582

## Updated Malware Signatures (Week 1 August 2025)

| Threat | Description |
|---|---|
| PlanetStealer | PlanetStealer is Golang-based malware designed to steal sensitive information on victim devices. It is designed to steal information such as credentials, browser cookies (commonly used for authentication), cryptowallets and more. This information is exfiltrated using a Telegram webhook. |

## 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 Victims – Weekly Overview

Beast takes the top spot this week, responsible for 12.6% of all reported ransomware incidents. This surge signals a potentially new campaign, aggressive affiliate scaling, or updated tooling pushing it into the spotlight.

Inc Ransom follows with 9.45%, maintaining a strong and consistent footprint, typically leveraging data leak extortion strategies against enterprise environments.

Both SafePay and Global posted 8.66%, continuing to exhibit high-volume attacks across various industries and geographies, suggesting active affiliate participation and automation-driven payload delivery.

Qilin and Akira each registered 7.09%, showing their persistent presence on the global ransomware stage, often known for double extortion tactics and wide targeting scopes.

Warlock held 5.51%, while several mid-tier groups, including Lynx, D4rk4rmy, Everest, DragonForce, J Group, BlackByte-Crux, and Sinobi, each reported between 3.15% and 3.94%, indicating active but moderately scaled campaigns.

Arcus Media and DireWolf accounted for 2.36%, and smaller activity clusters emerged from Kairos, WorldLeaks, BQTLock, Play, and Medusa (each at 1.57%).

Finally, Abyss-Data, Brain Cipher, Qilin-Securotrop, Rhysida, and Devman2 each contributed 0.79% of total incidents, representing the "long tail" of ransomware: smaller groups launching opportunistic, precision-based, or regionally confined attacks.

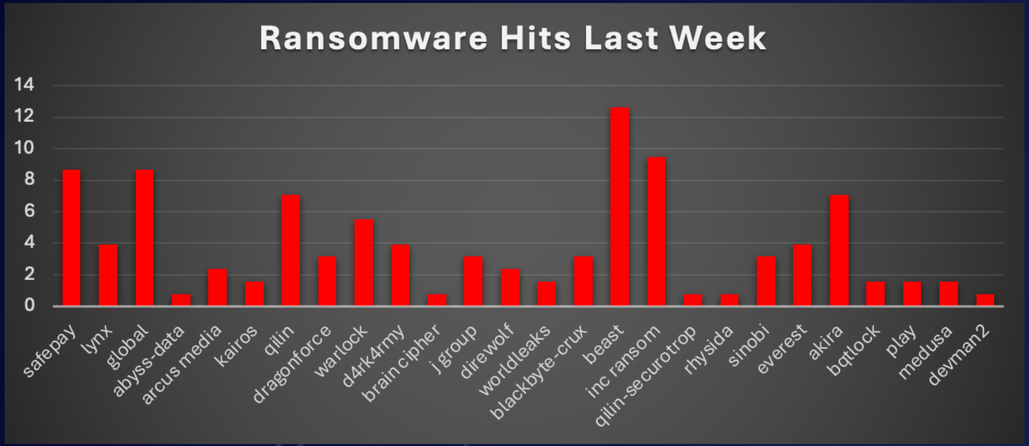


*Figure 1: Ransomware Group Hits Last Week*

## Beast Ransomware

Beast is a Tor-centric, double-extortion ransomware operation that surfaced prominently in early 2025 and has rapidly evolved into a low-noise but high-impact actor. Unlike many traditional ransomware groups, Beast avoids clear-web infrastructure, instead favouring onion-based leak sites and peer-to-peer negotiation channels. This tactic not only complicates attribution but also circumvents typical domain and IP-based detections.

Affiliates deploy the malware manually or semi-automatically, often executing encryption and exfiltration without persistent C2 beaconing. This infrastructure-minimal model suggests a preference for stealth over scale, drawing parallels to emerging “offline” ransomware families.

Detailed TTPs
Below is a refined breakdown of Beast’s observed Tactics, Techniques & Procedures (TTPs).

Initial Access
Valid Accounts (T1078)
Beast affiliates gained access via brute-forced or previously leaked RDP/SSH credentials, frequently targeting misconfigured Linux and Windows servers.

Execution
Command and Scripting Interpreter (T1059)
Malware payloads were manually launched or dropped via bash or PowerShell one-liners that initiated encryption and loaded auxiliary tools.

Persistence
Boot or Logon Initialisation Scripts (T1037.004)
On Linux systems, a persistence mechanism was set via /etc/profile.d/beast.sh, which silently executed on every shell session. Windows targets employed scheduled tasks and HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

Defence Evasion
Obfuscated Files or Information (T1027)
Beast’s ELF payloads were UPX-packed and used filename padding (.log, .conf) to blend with legitimate configuration files.

Credential Access
Credential Dumping (T1003)
Harvesting of /etc/shadow (Linux) and LSASS memory (Windows) was performed using open-source tooling like mimit or nanodump.

Discovery
System Information Discovery (T1082)
The malware probed hostnames, disk space, mounted volumes, and user lists using uname, df -h, and whoami to triage target environments.

Lateral Movement
Remote Services (SSH) (T1021.002)
Using captured credentials, the malware propagated laterally via SSH to additional reachable systems inside the 10.x/192.168.x IP ranges.

Collection & Exfiltration
Archive Collected Data (T1560.001)
Data was compressed via tar and zip, and staged in /tmp/.beast/ before transfer.

Exfiltration Over Alternative Protocol (T1048)
Stolen data was exfiltrated over custom SSH tunnels to attacker the infrastructure or uploaded to Tor-based drop servers.

TTP Mapping to MITRE ATT&CK

| Phase | Technique | ATT&CK ID |
|---|---|---|
| Initial Access | Valid Accounts | T1078 |
| Execution | Command and Scripting Interpreter | T1059 |
| Persistence | Logon Initialisation Scripts | T1037.004 |
| Defence Evasion | Obfuscated Files/Information | T1027 |
| Credential Access | Credential Dumping | T1003 |
| Discovery | System Information Discovery | T1082 |
| Lateral Movement | Remote Services (SSH) | T1021.002 |
| Collection | Archive Collected Data | T1560.001 |
| Exfiltration | Exfiltration Over Alt. Protocol | T1048 |
| Impact | Data Encrypted for Impact | T1486 |

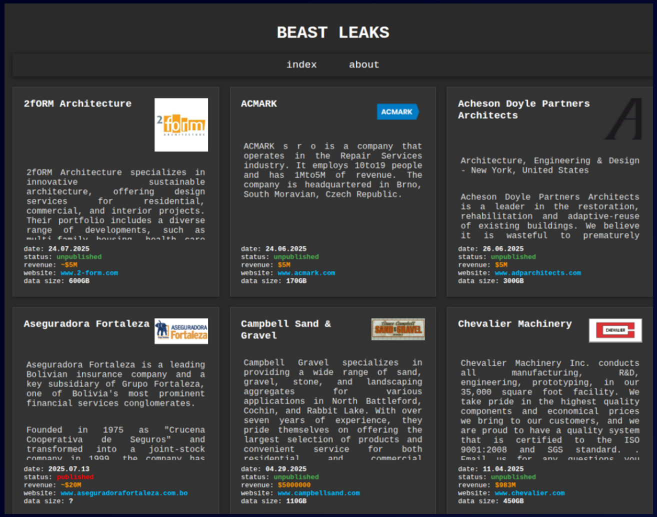
## IOCs

### IP

- 144.91.79.54

### Onion URLs

- beast6azu4f7fxjakiayhnssybibsgjnmy77a6duufqw5afjzfjhzuqd.onion



BEAST LEAKS

index about

**2fORM Architecture**

2fORM Architecture specializes in innovative sustainable architecture, offering design services for residential, commercial, and interior projects. Their portfolio includes a diverse range of developments, such as multi-family housing, health care

date: 24.07.2025
status: unpublished
revenue: ~$5M
website: www.2-form.com
data size: 600GB

**ACMARK**

ACMARK s r o is a company that operates in the Repair Services industry. It employs 10to19 people and has 1Mto5M of revenue. The company is headquartered in Brno, South Moravian, Czech Republic.

date: 24.06.2025
status: unpublished
revenue: $5M
website: www.acmark.com
data size: 170GB

**Acheson Doyle Partners Architects**

Architecture, Engineering & Design - New York, United States

Acheson Doyle Partners Architects is a leader in the restoration, rehabilitation and adaptive-reuse of existing buildings. We believe it is wasteful to prematurely

date: 26.06.2025
status: unpublished
revenue: $5M
website: www.adparchitects.com
data size: 300GB

**Aseguradora Fortaleza**

Aseguradora Fortaleza is a leading Bolivian insurance company and a key subsidiary of Grupo Fortaleza, one of Bolivia's most prominent financial services conglomerates.

Founded in 1975 as "Crucena Cooperativa de Seguros" and transformed into a joint-stock company in 1999 the company has

date: 2025.07.13
status: published
revenue: ~$20M
website: www.aseguradorafortaleza.com.bo
data size: ?

**Campbell Sand & Gravel**

Campbell Gravel specializes in providing a wide range of sand, gravel, stone, and landscaping aggregates for various applications in North Battleford, Cochin, and Rabbit Lake. With over seven years of experience, they pride themselves on offering the largest selection of products and convenient service for both residential and commercial

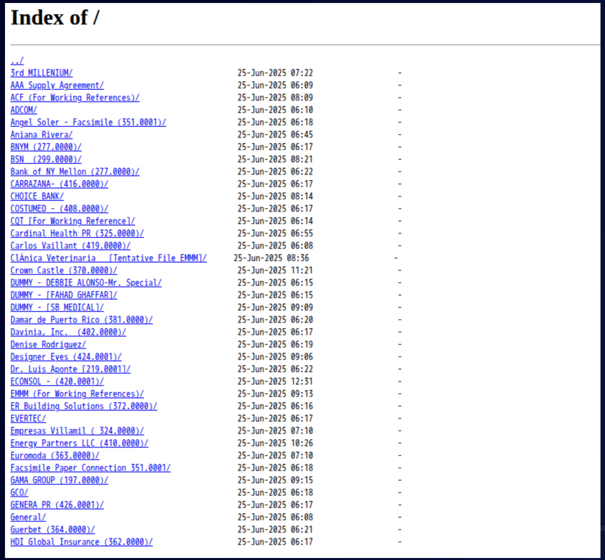
date: 04.29.2025
status: unpublished
revenue: $5000000
website: www.campbellsand.com
data size: 110GB

**Chevalier Machinery**

Chevalier Machinery Inc. conducts all manufacturing, R&D, engineering, prototyping, in our 35,000 square foot facility. We take pride in the highest quality components and economical prices we bring to our customers, and we are proud to have a quality system that is certified to the ISO 9001:2008 and SGS standard. . Email us for any questions you

date: 11.04.2025
status: unpublished
revenue: $983M
website: www.chevalier.com
data size: 450GB

- ooie6tet7ggcmlgvtmyvok4s6vha6ecwczssbchbyxrg2r6v2m6zkkad.onion ( File Server)



```
Index of /

../
3rd MILLENIUM/                                 25-Jun-2025 07:22       -
AAA Supply Agreement/                          25-Jun-2025 06:09       -
ACF (For Working References)/                  25-Jun-2025 08:09       -
ADCOM/                                         25-Jun-2025 06:10       -
Angel Soler - Facsimile (351.0001)/            25-Jun-2025 06:18       -
Aniana Rivera/                                 25-Jun-2025 06:45       -
BNYM (277.0000)/                               25-Jun-2025 06:17       -
BSN  (299.0000)/                               25-Jun-2025 08:21       -
Bank of NY Mellon (277.0000)/                  25-Jun-2025 06:22       -
CARRAZANA- (416.0000)/                         25-Jun-2025 06:17       -
CHOICE BANK/                                   25-Jun-2025 08:14       -
COSTUMED - (408.0000)/                         25-Jun-2025 06:17       -
CQT [For Working Reference]/                   25-Jun-2025 06:14       -
Cardinal Health PR (325.0000)/                 25-Jun-2025 06:55       -
Carlos Vaillant (419.0000)/                    25-Jun-2025 06:08       -
ClÃnica Veterinaria  [Tentative File EMMM]/   25-Jun-2025 08:36       -
Crown Castle (370.0000)/                       25-Jun-2025 11:21       -
DUMMY - DEBBIE ALONSO-Mr. Special/             25-Jun-2025 06:15       -
DUMMY - [FAHAD GHAFFAR]/                       25-Jun-2025 06:15       -
DUMMY - [SB MEDICAL]/                          25-Jun-2025 09:09       -
Damar de Puerto Rico (381.0000)/               25-Jun-2025 06:20       -
Davinia, Inc.  (402.0000)/                     25-Jun-2025 06:17       -
Denise Rodriguez/                              25-Jun-2025 06:19       -
Designer Eyes (424.0001)/                      25-Jun-2025 09:06       -
Dr. Luis Aponte [219.0001]/                    25-Jun-2025 06:22       -
ECONSOL - (420.0001)/                          25-Jun-2025 12:31       -
EMMM (For Working References)/                 25-Jun-2025 09:13       -
ER Building Solutions (372.0000)/              25-Jun-2025 06:16       -
EVERTEC/                                       25-Jun-2025 06:17       -
Empresas Villamil ( 324.0000)/                 25-Jun-2025 07:10       -
Energy Partners LLC (410.0000)/                25-Jun-2025 10:26       -
Euromoda (363.0000)/                           25-Jun-2025 07:10       -
Facsimile Paper Connection 351.0001/           25-Jun-2025 06:18       -
GAMA GROUP (197.0000)/                         25-Jun-2025 09:15       -
GCO/                                           25-Jun-2025 06:18       -
GENERA PR (426.0001)/                          25-Jun-2025 06:17       -
General/                                       25-Jun-2025 06:08       -
Guerbet (364.0000)/                            25-Jun-2025 06:21       -
HDI Global Insurance (362.0000)/               25-Jun-2025 06:17       -
```

### Mail IDs.

recovery24.email@onionmail.com
blackpool@zohomail.eu
ambulafixdata@zohomail.eu
ambulafixdata@onionmail.org
br.fixdata24@proton.me
br.fixdata24@onionmail.com
helpdata24@zohomail.eu
helpdata24@onionmail.org

### TOX ID

92E5D1A8ECFC69E7967E7A9DC1C9A735CD8DCE965D12EF01F19966C7101EAF071B4CDEA310E9

## Concise Mitigation with CE 5.0

### Email & Sandbox

- Quarantine inbound ZIP/TAR/ISO archives containing ELF or EXE binaries.
- Block DNS/TLS connections to .onion domains and associated Tor proxy gateways.

### Endpoint Protection

- HIPS: Alert on new files in /etc/profile.d/, .bashrc, or HKCU\Run.
- Monitor for tools like rclone, scp, mimit, and abnormal lsass.exe access.

### Network Controls

- IPS/IDS: Block outbound SSH traffic on non-standard ports (e.g., 2222).
- Sinkhole known Beast onion URLs; monitor Tor process invocation.

### Access Management

- Enforce MFA on all exposed SSH/RDP services.
- Alert on first-time access from foreign ASN/IPs or impossible logins.

### Backup & Recovery

- Implement immutable, offline backups rotated daily.
- Simulate restore events every 30 days for incident readiness.

## Worldwide Ransomware Victims

The United States continues to be the most heavily impacted country by ransomware, accounting for a dominant 59.06% of all reported incidents this week. Its vast digital infrastructure and concentration of high-value industries make it the most consistent target for both well-known and emerging threat actors.

The United Kingdom follows at 6.3%, remaining one of the top European targets due to its advanced economy, reliance on digital services, and global business ties.

Spain and Germany both registered 3.94%, reflecting a persistent threat landscape in Western Europe where professional services, manufacturing, and public sectors are frequently affected.

Italy came in at 3.15%, with Australia and Canada following at 2.36% each—highlighting ransomware's expanding reach into both Asia-Pacific and North American regions beyond the U.S.

A mid-tier of countries—including Thailand, Netherlands, Turkey, Brazil, and Belgium—each experienced 1.57% of incidents, suggesting continued threat actor interest across diverse geographies.

The long tail includes multiple nations that each reported 0.79% of attacks:
Mexico, Greece, Jordan, Ireland, Argentina, Poland, Lebanon, Singapore, Malaysia, Denmark, France, Bolivia, Colombia, and Guyana. This reflects the increasingly global distribution of ransomware activity, where threat actors cast a wide net, often exploiting opportunistic or low-barrier entry points across industries and regions.

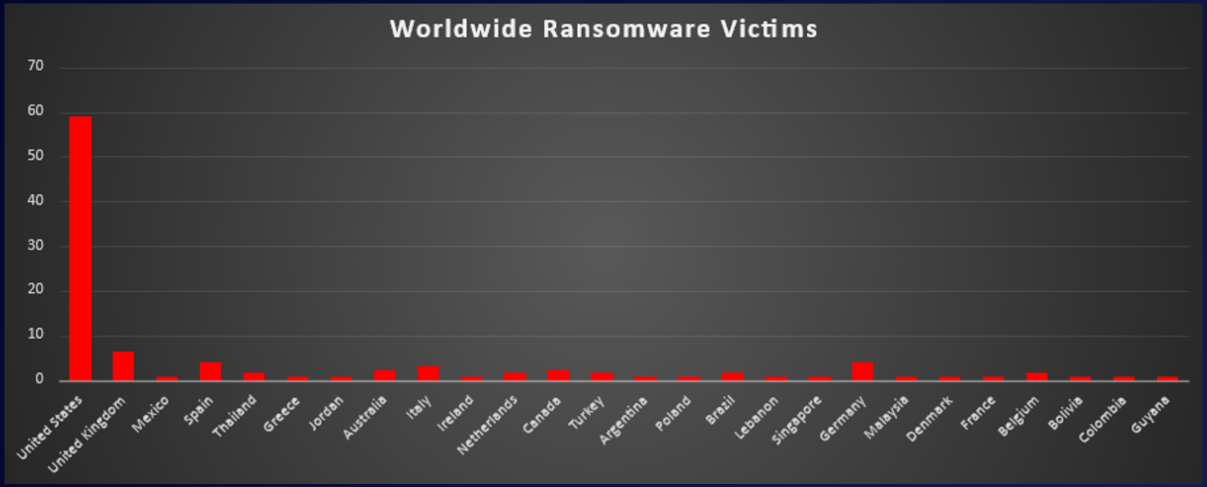


*Figure 4: Ransomware Victims Worldwide*

## Industry-wide Ransomware Victims

Manufacturing remains the most targeted industry this week, accounting for 18.11% of reported ransomware incidents. Its operational criticality, legacy systems, and limited downtime tolerance make it an ongoing priority for attackers.

Business Services follow closely at 11.81%, reflecting persistent targeting of firms that provide IT, consulting, and operational support to multiple sectors, often acting as indirect gateways into larger networks.

Construction and Retail each reported 11.02%, both sectors being attractive to ransomware operators due to their broad vendor ecosystems, financial transactions, and often underdeveloped cybersecurity practices.

Hospitality and Education both logged 7.87%, indicating that threat actors focus on sectors with significant customer data and digital dependencies but typically lacking mature security controls.

Law Firms came in at 6.3%, reaffirming their status as frequent targets due to sensitive legal data, contracts, and time-sensitive operations.
Mid-tier victims include Real Estate and Finance (3.15% each), and Consumer Services, IT, Transportation, and Organisations (each at 2.36%)—representing sectors with varied digital maturity but high extortion leverage.

Smaller but still significant incidents affected Healthcare, Federal, Energy, Agriculture, and Media & Internet (each at 1.57%), showing a widespread impact across both public and private sector verticals.

Finally, Telecommunications, Minerals & Mining, and Insurance each registered 0.79%, underscoring ransomware's wide net across both high-profile and niche sectors.

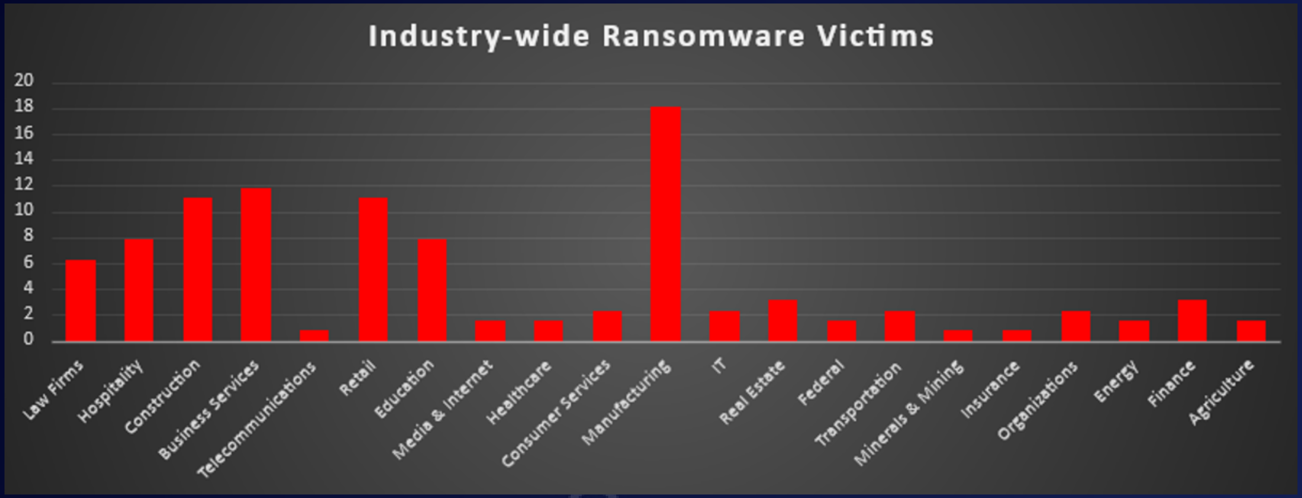


*Figure 5: Industry-wide Ransomware Victims*