Stealth Mole

THE RISE OF NEW RANSOMWARE GROUPS IN 2025

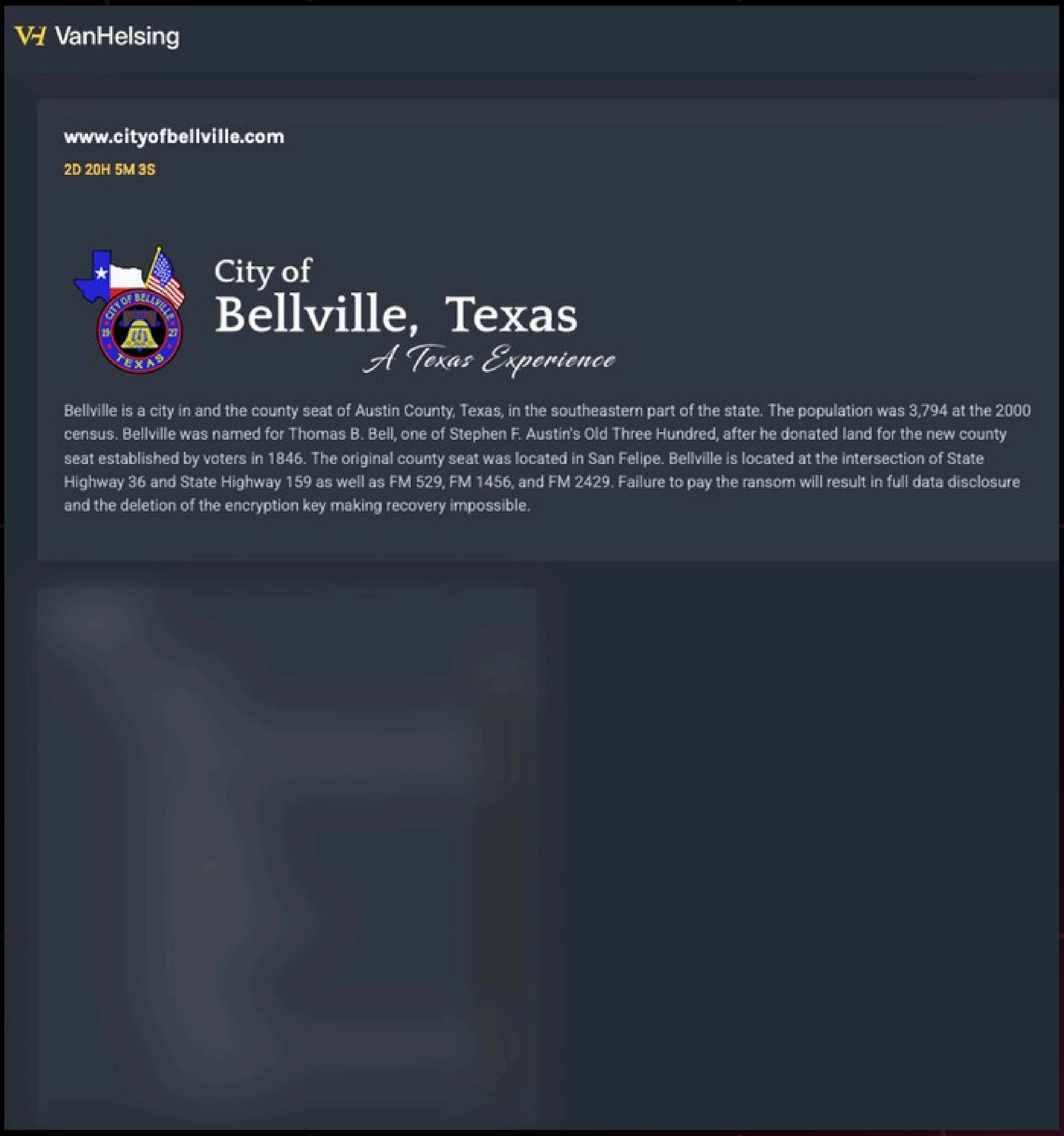
A Deep Dive into VanHelsing, NightSpire, and Frag

VANHELSING

First Observed: March 7,2025

Tactic: Data is exfiltrated before encryption to increase leverage.

Within just two weeks of its debut, **VanHelsing** has been linked to three confirmed attacks, targeting **government entities, manufacturing firms, and pharmaceutical companies in France, Australia, Italy and United States**. What makes VanHelsing unique is its ability to attack **Windows, Linux, BSD, ARM, and ESXi systems**, broadening its impact.



VanHelsing

www.cityofbellville.com

2D 20H 5M 3S

City of
Bellville, Texas
A Texas Experience

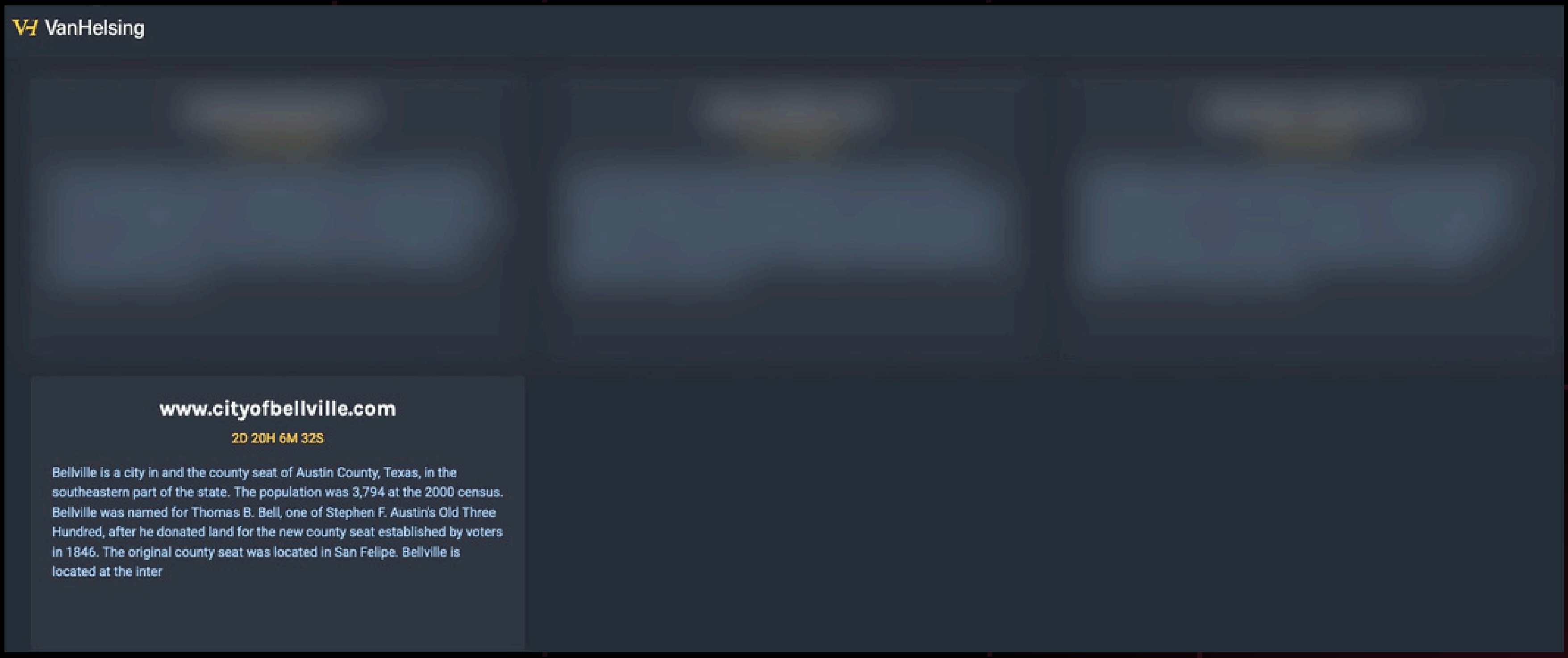
Bellville is a city in and the county seat of Austin County, Texas, in the southeastern part of the state. The population was 3,794 at the 2000 census. Bellville was named for Thomas B. Bell, one of Stephen F. Austin's Old Three Hundred, after he donated land for the new county seat established by voters in 1846. The original county seat was located in San Felipe. Bellville is located at the intersection of State Highway 36 and State Highway 159 as well as FM 529, FM 1456, and FM 2429. Failure to pay the ransom will result in full data disclosure and the deletion of the encryption key making recovery impossible.

Stealth Mole

VANHELSING

Key Features:

- Uses **Curve25519 and ChaCha20 encryption** to lock files with a ".vanhelsing" extension.
- **Exfiltrates data before encryption**, increasing pressure on victims.
- Has an affiliate-based model, where **experienced hackers join for free**, and **new members pay a $5,000 deposit**.
- Ransom demands reach up to **$500,000**.



[redacted]

www.cityofbellville.com

2D 20H 6M 32S

Bellville is a city in and the county seat of Austin County, Texas, in the southeastern part of the state. The population was 3,794 at the 2000 census. Bellville was named for Thomas B. Bell, one of Stephen F. Austin's Old Three Hundred, after he donated land for the new county seat established by voters in 1846. The original county seat was located in San Felipe. Bellville is located at the inter

Sources:

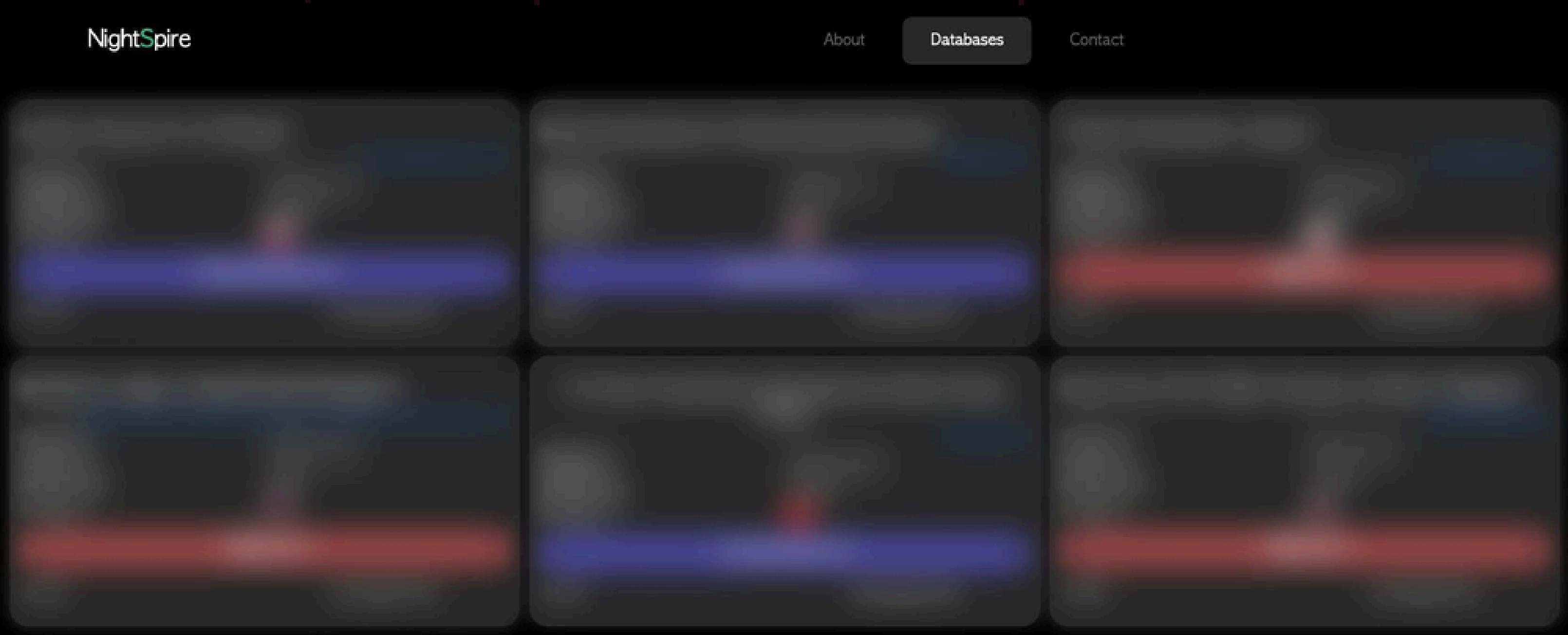
- https://www.bleepingcomputer.com/news/security/new-vanhelsing-ransomware-targets-windows-arm-esxi-systems/
- https:/www.cyfirma.com/research/vanhelsing-ransomware/

NIGHTSPIRE

First Appearance: Early 2025

Tactic: Double extortion with data publication countdowns

Despite its recent appearance, it has rapidly gained attention due to its **aggressive tactics and high-impact operations**. The group operates under a Ransomware-as-a-Service (RaaS) model and uses a **double extortion strategy**, involving both data encryption and the threat of public exposure via its dedicated **Data Leak Site (DLS)**.

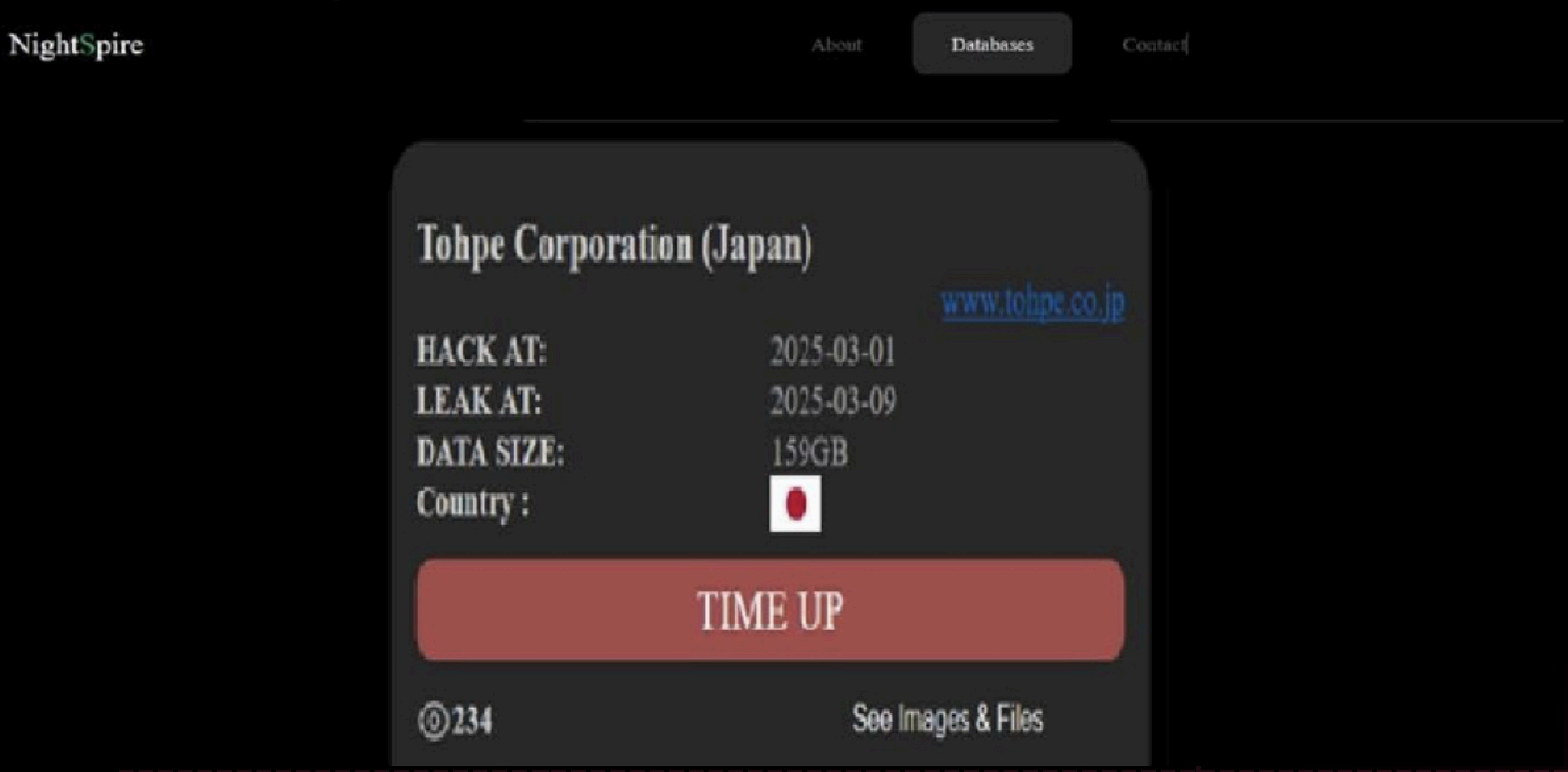


Key Insights:

- Claims to **exploit known vulnerabilities** in enterprise networks.
- Uses **ProtonMail, OnionMail, and Telegram** for negotiations.
- Leverages **fear-based tactics**, including countdown timers for data exposure.

NIGHTSPIRE

In **March 2025**, NightSpire attacked **Tohpe Corporation (Japan)**, a **manufacturing giant** specializing in paints and high-performance materials. This incident was observed on **underground forums.** The leaked data is believed to **include sensitive internal information**.



Tohpe Corporation (Japan)

www.tohpe.co.jp

HACK AT: 2025-03-01
LEAK AT: 2025-03-09
DATA SIZE: 159GB
Country :

©234

Impact of the Attack:

- **159GB** of confidential data compromised.
- Severe **financial loss** and **reputational damage**.
- Attack disclosed on **underground forums**, exposing sensitive corporate information.

Sources:

- https://cyberpress.org/nightspire-ransomware-group/?amp=1
- https://www.cyfirma.com/news/weekly-intelligence-report-21-mar-2025/

Stealth Mole

FRAG

First Observed: February 28, 2025

Tactic: Exploited Vulnerability & Attack Chain

The Frag ransomware group, has quickly emerged as a **significant cyber threat**. In just one month, the group has compromised at least **30 victims** across various industries.

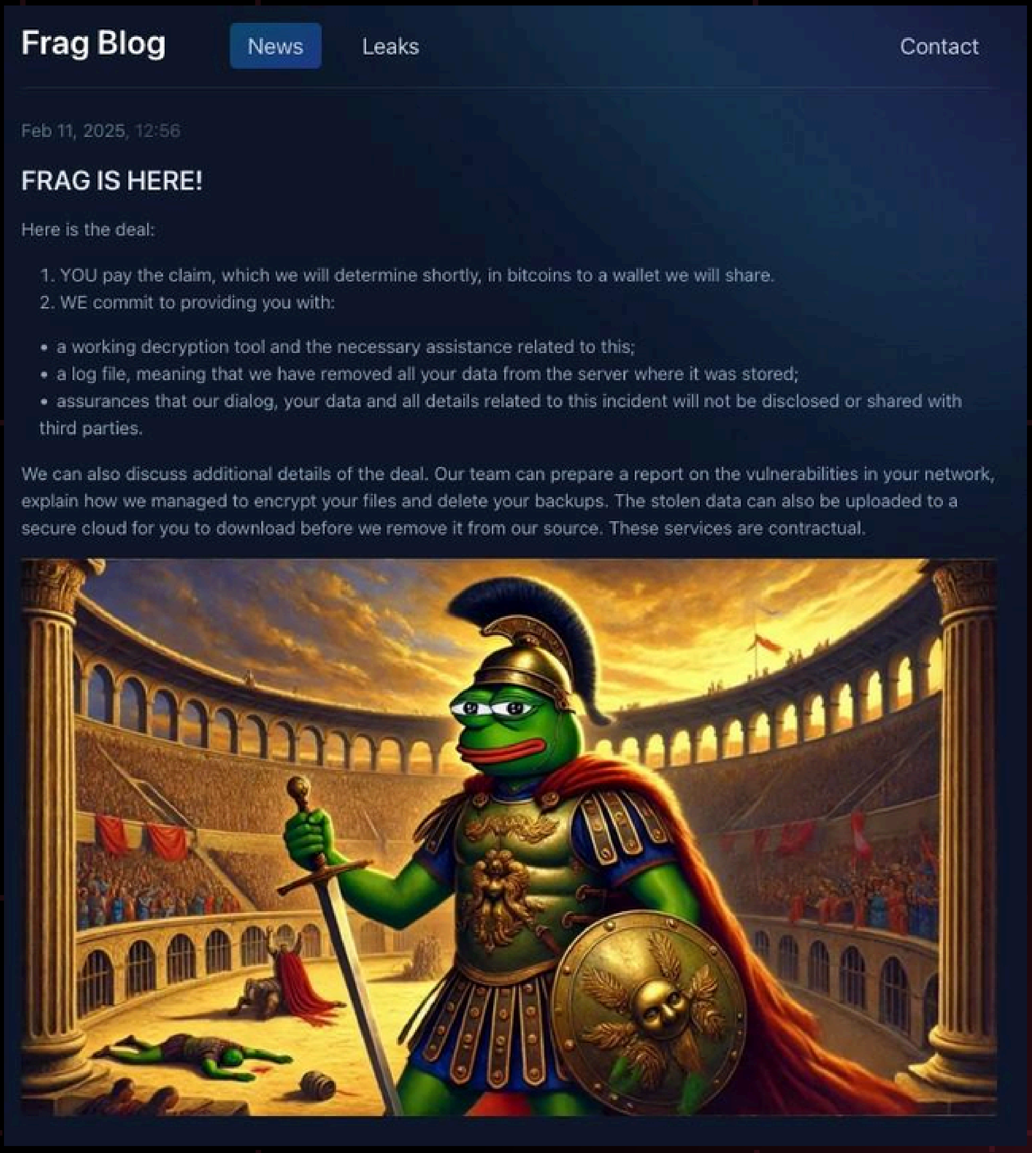
Notable Features:

- Exploits **CVE-2024-40711**, a **Veeam Backup & Replication vulnerability**.
- Gains **initial access through VPN weaknesses**.
- Creates **persistent admin accounts** for long-term infiltration.
- Uses **double extortion tactics** to pressure victims into paying.

FRAG

Frag has impacted multiple industries, including **healthcare, technology, financial services, and hospitality etc.** Some of the major victims include:

- **Seaquest Seafood (USA)** – Large-scale data encryption & extortion.
- **Woodbine Hospitality (USA)** – Customer information exposed.
- **Komoto Healthcare (USA)** – Sensitive patient data leaked.
- **Maine Highlands Federal Credit Union (USA)** – Financial data at risk.
- **Texas Fifth Wall Roofing Systems (USA)** – Internal operations disrupted.



Feb 11, 2025, 12:56

FRAG IS HERE!

Here is the deal:

1. YOU pay the claim, which we will determine shortly, in bitcoins to a wallet we will share.
2. WE commit to providing you with:

- a working decryption tool and the necessary assistance related to this;
- a log file, meaning that we have removed all your data from the server where it was stored;
- assurances that our dialog, your data and all details related to this incident will not be disclosed or shared with third parties.

We can also discuss additional details of the deal. Our team can prepare a report on the vulnerabilities in your network, explain how we managed to encrypt your files and delete your backups. The stolen data can also be uploaded to a secure cloud for you to download before we remove it from our source. These services are contractual.

Sources:

- https://cyberpress.org/frag-ransomware/

Stealth Mole

WHY RAAS MAKES RANSOMWARE MORE DANGEROUS

Ransomware groups like **VanHelsing, NightSpire, and Frag** thrive due to the **RaaS model**, which enables less skilled cybercriminals to launch sophisticated attacks. Key aspects of this model include:

- **Low entry barrier**: Anyone can buy ransomware tools.
- **Profit-sharing schemes**: Operators take **20%, affiliates take 80%**.
- **Continuous updates**: Frequent software improvements increase effectiveness.

The emergence of VanHelsing, NightSpire, and Frag highlights the **increasing sophistication** of ransomware threats. Is your company prepared?

Stealth Mole

Talk to us to learn how you can build a solid cyber defense strategy today