



# **TOP CRYPTO RANSOMWARE PAYMENTS REPORT**





# TOP CRYPTO RANSOMWARE PAYMENTS REPORT

Prepared by ImmuneFi

The team at [ImmuneFi](#), the leading bug bounty and security services platform for web3 which protects over \$60 billion in user funds, has created a comprehensive listing of the top crypto ransomware payments in the industry by reviewing open source data.

## Crypto Ransomware

Ransomware attacks use ransomware, which is a form of malware designed to encrypt files on a device or entire network and make them inaccessible. Ransomware groups carry out these attacks and then demand a ransom in return for returning control of those systems.

With the growth of cryptocurrencies like Bitcoin, ransomware attacks saw a noticeable increase in popularity, as ransomware groups have come to believe that cryptocurrency is anonymous, untraceable, and can facilitate much larger ransom payments than traditional financial systems.



If you're a developer thinking about a bug-hunting career in web3, we got you. Check out our [Web3 Security Library](#), and start taking home some of the \$144M in rewards available on ImmuneFi — the leading bug bounty platform for web3.

<https://immuneFi.com/>

## Top Crypto Ransomware Payments

The top crypto ransomware payments total **\$69,316,140** across 10 specific situations.

<b>CNA Financial</b>	\$40,000,000
<b>JBS</b>	\$11,000,000
<b>CWT</b>	\$4,500,000
<b>Brenntag</b>	\$4,400,000
<b>Colonial Pipeline*</b>	\$4,400,000
<b>Travelex</b>	\$2,300,000
<b>UCSF</b>	\$1,140,895
<b>BRB Bank</b>	\$957,245
<b>Jackson County, Georgia</b>	\$400,000
<b>University of Maastricht*</b>	\$218,000

\*Colonial Pipeline recovered **\$2,300,000** from the ransom payment, and the University of Maastricht recovered the full ransom payment amount. When recovered, the total Bitcoin value from Maastricht's payment was worth **\$510,000**.



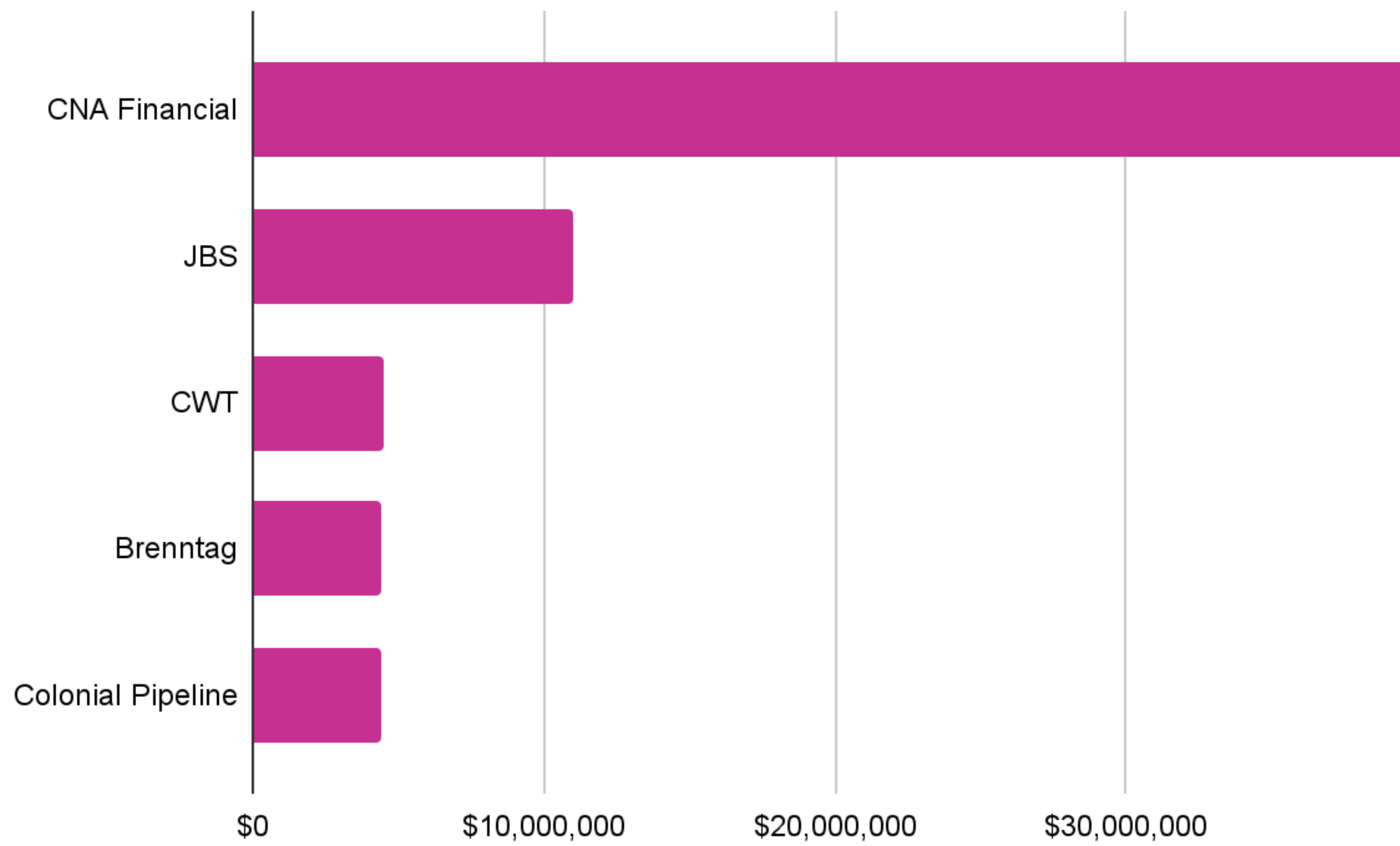
## Top Crypto Ransomware Payments

### Overview

Project	Ransom Payment	Funds Recovery	Ransomware Strain	Cryptocurrency	Origin
<b>CNA Financial</b>	\$40,000,000	N/A	Phoenix	Bitcoin	Russia
<b>JBS</b>	\$11,000,000	N/A	REvil/Sodinokibi	Bitcoin	Russia
<b>CWT</b>	\$4,500,000	N/A	Ragnar Locker	Bitcoin	N/A
<b>Brenntag</b>	\$4,400,000	N/A	DarkSide	Bitcoin	Eastern Europe
<b>Colonial Pipeline</b>	\$4,400,000	\$2,300,000	DarkSide	Bitcoin	Eastern Europe
<b>Travelex</b>	\$2,300,000	N/A	REvil/Sodinokibi	Bitcoin	Russia
<b>UCSF</b>	\$1,140,895	N/A	Netwalker Ransomware	Bitcoin	N/A
<b>BRB Bank</b>	\$957,245	N/A	LockBit	Bitcoin	Eastern Europe
<b>Jackson County, Georgia</b>	\$400,000	N/A	SamSam	Bitcoin	Iran
<b>University of Maastricht</b>	\$218,000	\$218,000*	Clop Ransomware	Bitcoin	Russia

\* When recovered, the total Bitcoin value was worth [\\$510,000](#).

## Top 5 Cases



### CNA Financial

\$40,000,000

### JBS

\$11,000,000

### CWT

\$4,500,000

### Brenntag

\$4,500,000

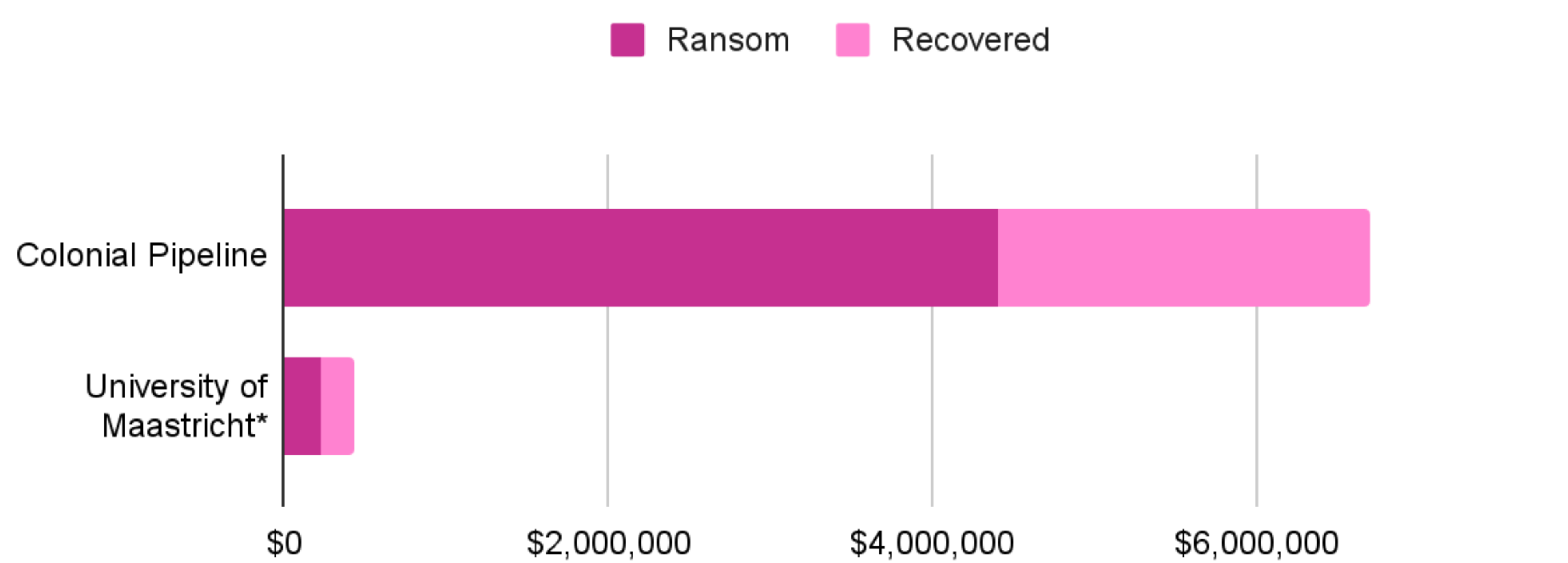
### Colonial Pipeline

\$4,400,000\*

\*Colonial Pipeline recovered [\\$2,300,000](#) from the ransom payment.

## Ransom Recovery

In total, **\$2,518,000** has been recovered from ransom payments in 2 specific situations. This number makes up 3.6% of the top crypto ransomware payments.



### Colonial Pipeline

Ransom **\$4,400,000**

Recovered **\$2,300,000**

### University of Maastricht

Ransom **\$218,000**

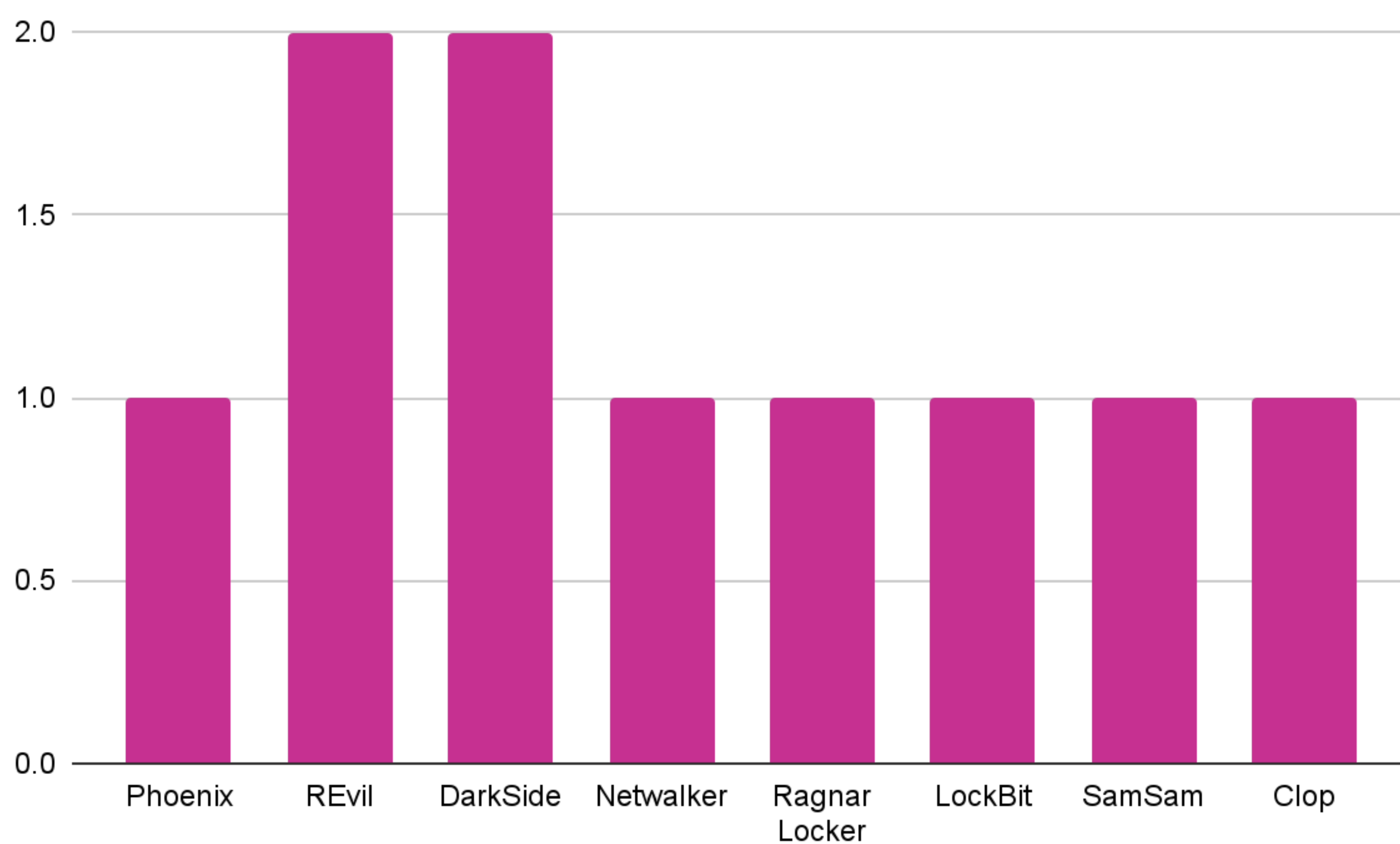
Recovered **\$218,000\***

\* When recovered, the total Bitcoin value was worth **\$510,000**.



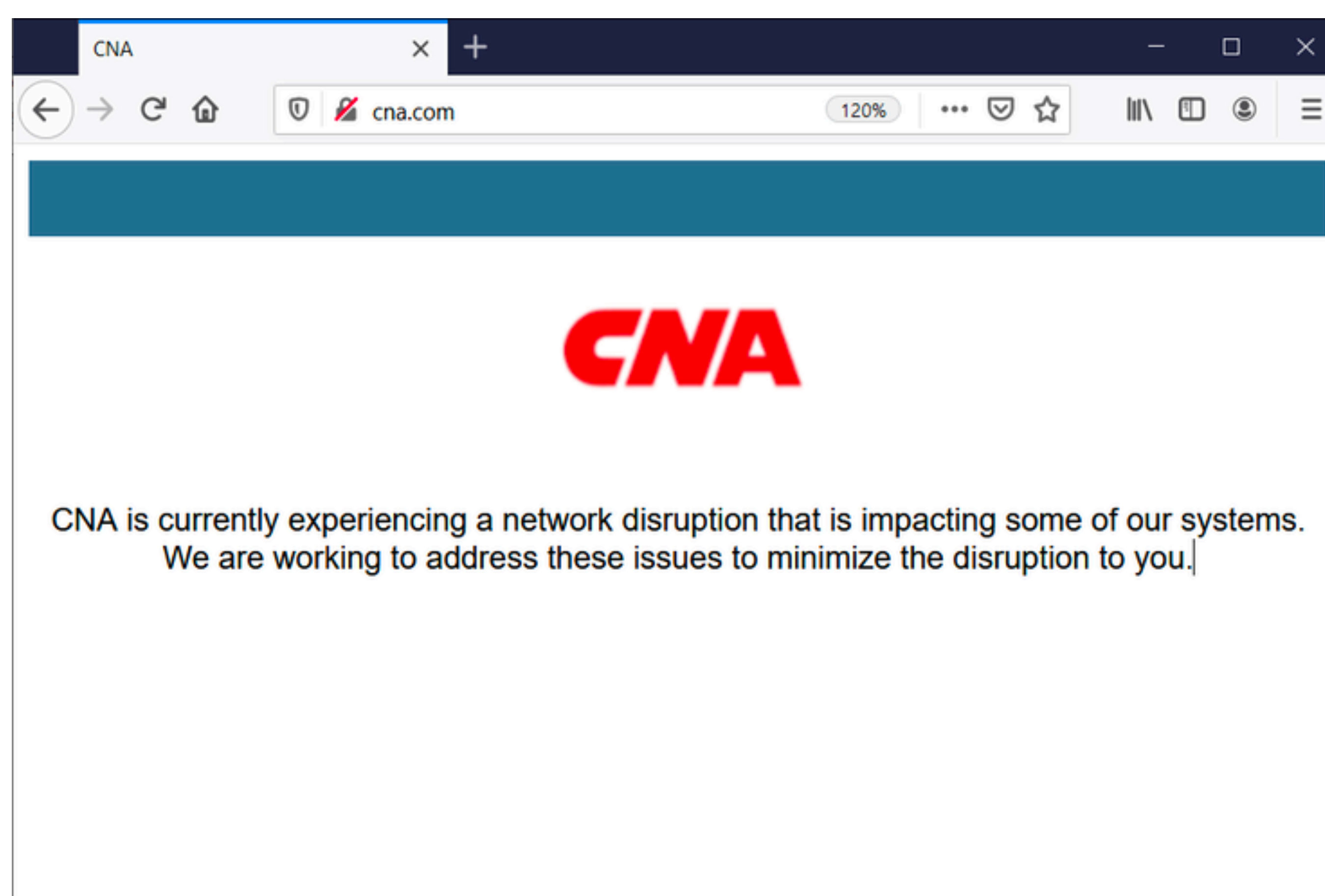
## Detected Ransomware Strains

Researchers have detected 8 specific strains of ransomware connected to the top crypto ransomware payments. REvil/Sodinokibi and DarkSide are key actors based on the total number of attacks, but the Phoenix group had the highest profiting attack.



### Phoenix CryptoLocker

While Phoenix CryptoLocker has been connected to only one of the top crypto ransomware payments cases, it was responsible for the biggest one at **\$40,000,000** (CNA Financial), which represents 57.7% of the top crypto ransomware payments. Phoenix is believed to be a newer variant of the ransomware family released by Evil Corp, a Russian-based cybercriminal group.



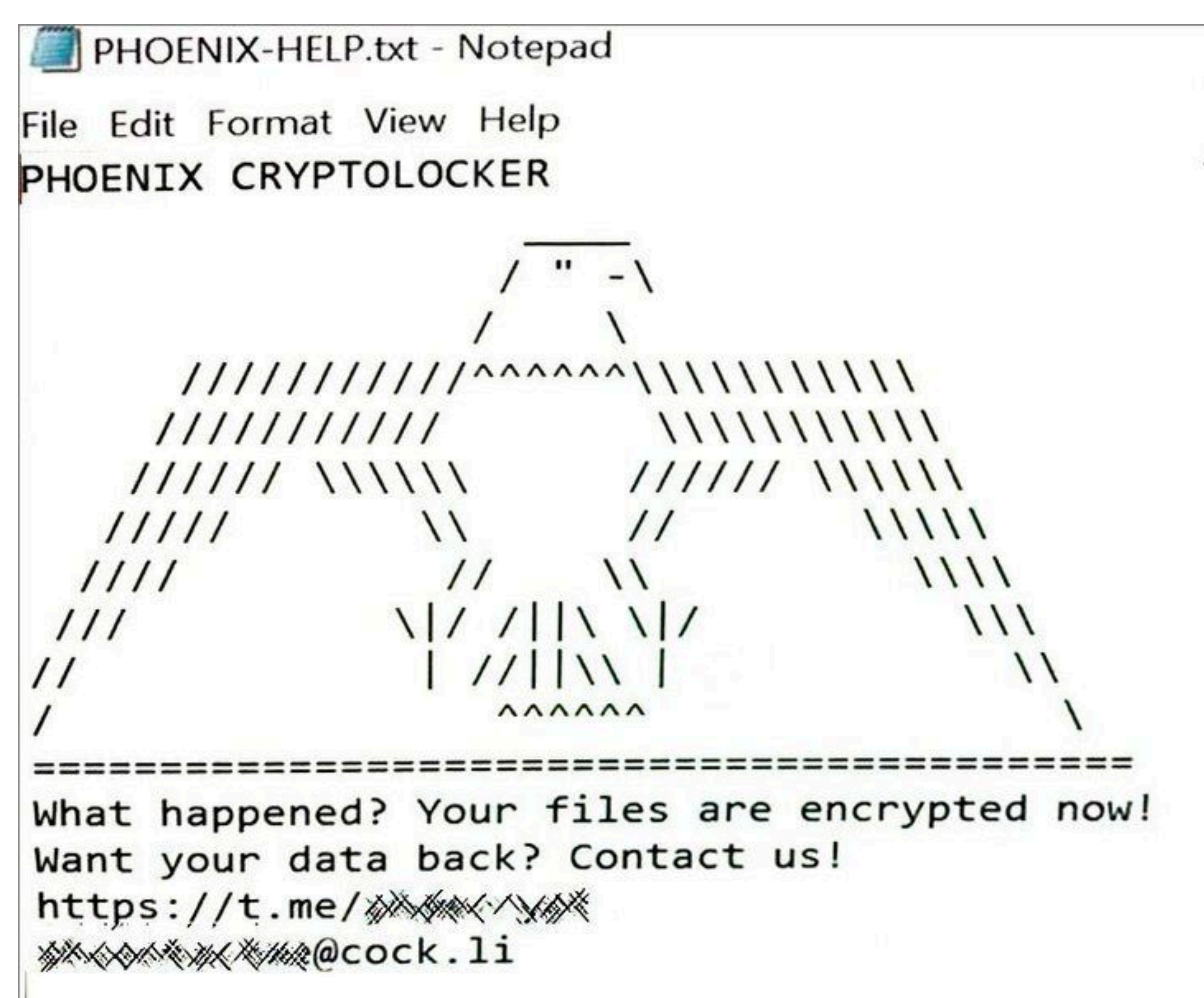
*CNA website shutdown caused by the ransomware attack (Source)*



## Detected Ransomware Strains

### Phoenix CryptoLocker

Evil Corp has allegedly been behind some of the worst hacks of the past decade. Phoenix CryptoLocker entered the list of suspected ransomware variants created by Evil Corp, including DoppelPaymer, Grief, WastedLocker, Hades, and Macaw.



*Phoenix CryptoLocker ransomware message (Source)*

### REvil/Sodinokibi

The group REvil/Sodinokibi, and its malware by the same name, were connected to two attacks: JBS USA Holdings Inc. and Travelex, profiting a total of **\$13,300,000**, which represents 19.2% of the top crypto ransomware payments.

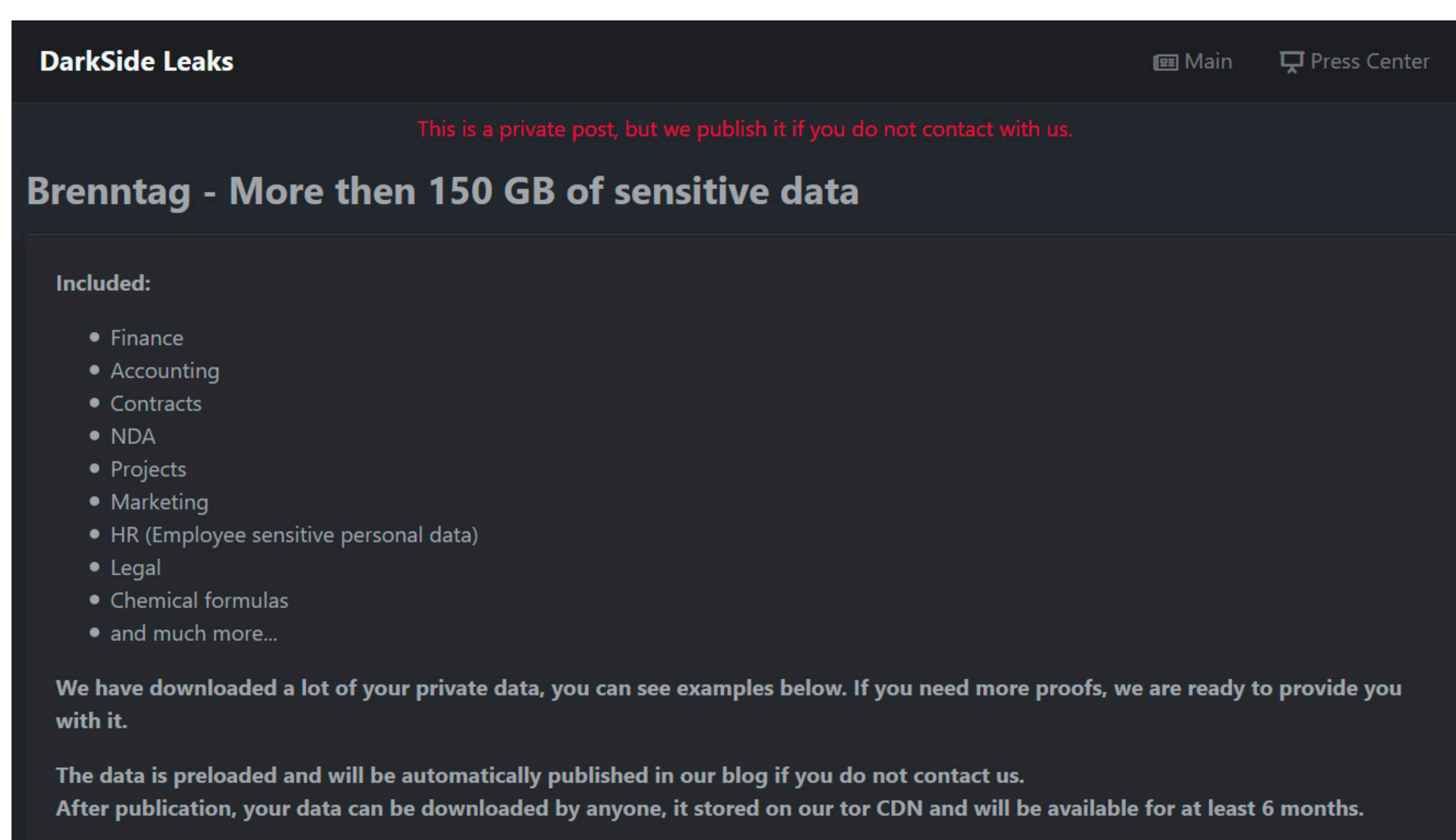
REvil/Sodinokibi ransomware is a Ransomware-as-a-Service (RaaS) operation believed to originate from Russia or Eastern Europe, as reports show the group doesn't target Russian-based organizations. Additionally, the ransomware code verifies that the victims are not located in countries belonging to the Commonwealth of Independent States, a regional intergovernmental organization in Eurasia. REvil/Sodinokibi is likely an offshoot of GandCrab, a now-defunct notorious cybercrime gang, as REvil first became active directly after GandCrab shut down, and the malware share a significant amount of code.



## Detected Ransomware Strains

### DarkSide

DarkSide was connected to two cases. The group was responsible for the attacks on Brenntag and Colonial Pipeline, profiting a total of **\$8,800,000**, which represents 12.7% of the top crypto ransomware payments.



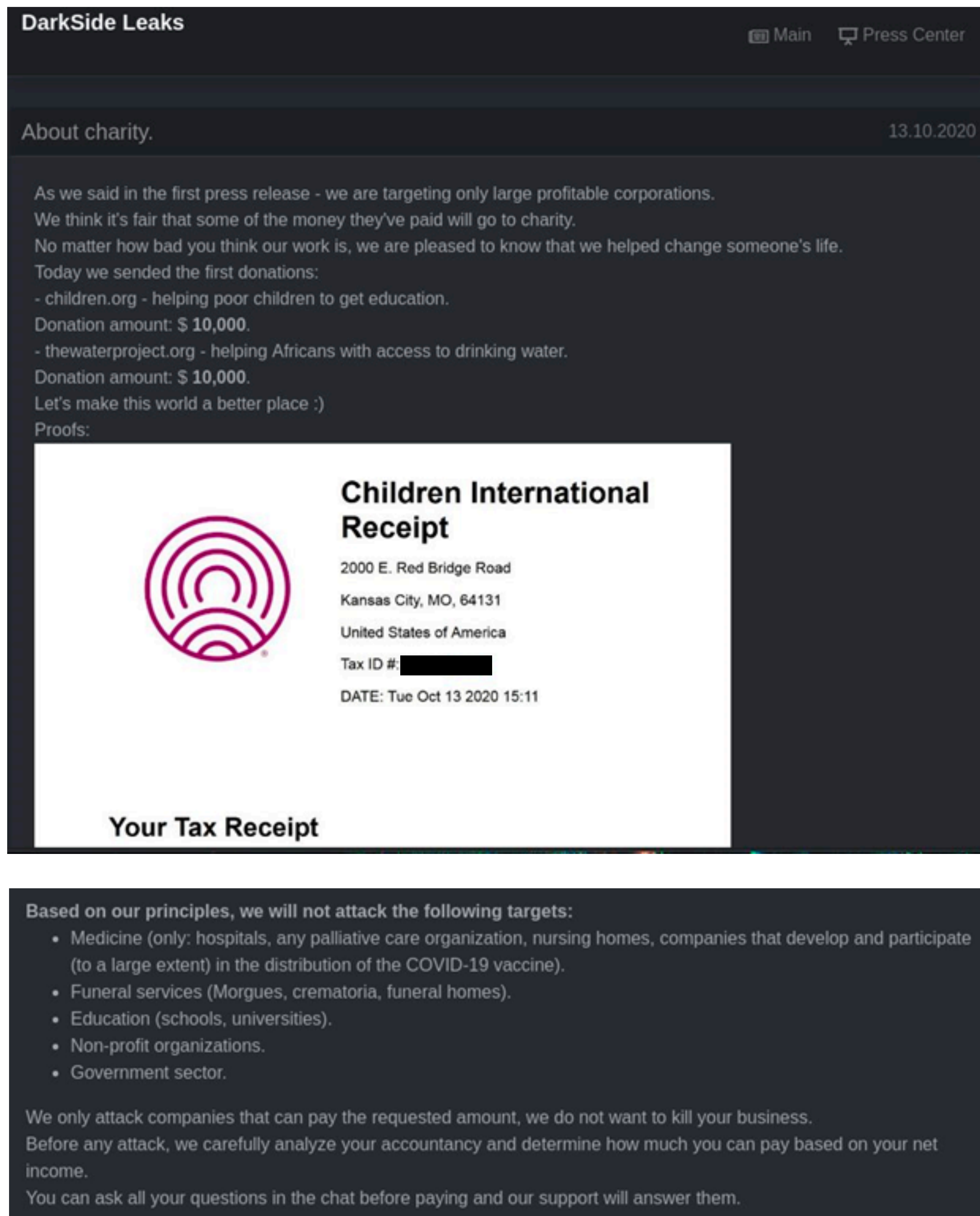
*Private data leak page sent to Brenntag (Source)*

DarkSide is a cybercrime group believed to be based in Eastern Europe that often operates via a Ransomware-as-a-Service (RaaS) model and also employs direct extortion. The group has a history of attempting double ransom payments—in other words, a payment to unlock the affected systems and an additional payment to prevent exfiltrated data from being made public. DarkSide is also known for publishing a code of conduct that lists acceptable targets. These targets are for-profit companies in English-speaking countries. The list of unacceptable targets includes hospitals, hospices, schools, universities, nonprofit organizations, and government agencies. Other protected entities included the Commonwealth of Independent States, a regional intergovernmental organization in Eurasia.



## Detected Ransomware Strains

### DarkSide



**DarkSide Leaks** Main Press Center


About charity. 13.10.2020

As we said in the first press release - we are targeting only large profitable corporations. We think it's fair that some of the money they've paid will go to charity. No matter how bad you think our work is, we are pleased to know that we helped change someone's life. Today we sended the first donations:

- children.org - helping poor children to get education. Donation amount: \$ 10,000.
- thewaterproject.org - helping Africans with access to drinking water. Donation amount: \$ 10,000.

Let's make this world a better place :)

Proofs:



**Children International Receipt**

2000 E. Red Bridge Road  
Kansas City, MO, 64131  
United States of America  
Tax ID #: [REDACTED]  
DATE: Tue Oct 13 2020 15:11

**Your Tax Receipt**

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business. Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income. You can ask all your questions in the chat before paying and our support will answer them.

*DarkSide Leaks: example of charity and targets public posts (Source)*



## Detected Ransomware Strains

### Ragnar Locker

Ragnar Locker was responsible for the CWT attack, the third largest attack on the list, profiting **\$4,500,000**, which represents 6.5% respectively.

Ragnar Locker is the name of the ransomware group and the malware it uses. Similar to DarkSide, Ragnar Locker has been known for the double ransom payment tactic and specifically for regularly changing their obfuscation techniques. The group has often targeted critical infrastructure, such as energy, manufacturing, financial, government, and IT organizations.

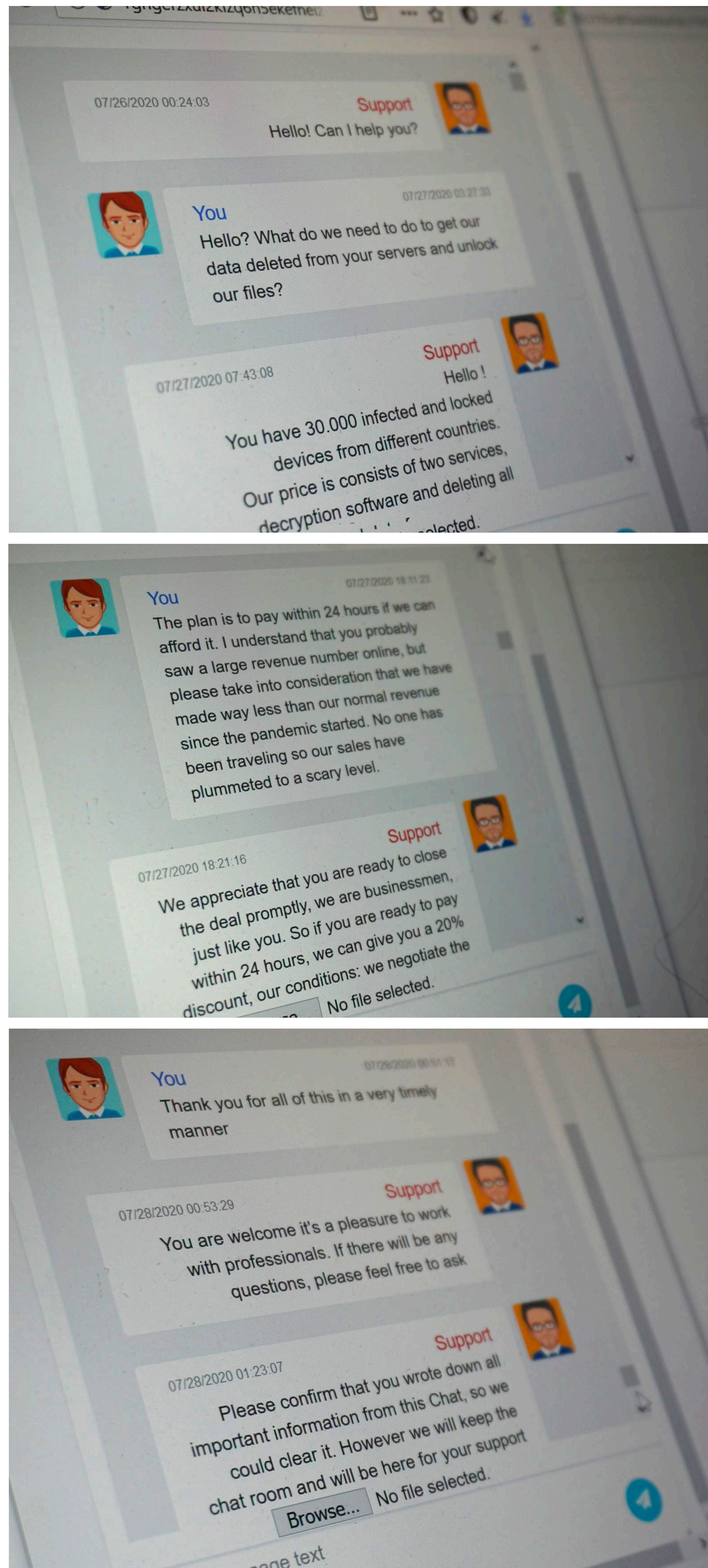
```
1 *****
2
3 If you reading this message, then your net [REDACTED] of your files and data has been ENCRYPTED
4
5 by RAGNAR_LOCKER !
6
7 *****
8
9          !!!!! WARNING !!!!!
10
11 DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
12 DO NOT use any third party or public decryption software, it also may damage files.
13 DO NOT Shutdown or reset your system
14 -----
15
16 There is ONLY ONE possible way to get back your files - contact us and pay for our special decryption key !
17 For your GUARANTEE we will decrypt 2 of your files FOR FREE, as a proof of our capabilities
18
19 Don't waste your TIME, the link for contacting us will be deleted if there is no contact made in closest future
20 and you will never restore your DATA.
21 HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.
22
23 ATTENTION !
24 We had downloaded more than 10TB of data from your fileservers and if you don't contact us for payment, we will
25 publish it or sell to interested parties.
26 Here is just a small part of your files that we have, for a proof (use Tor Browser for open the link) :
27 [REDACTED]
28 We gathered the most sensitive and confidential information about your transactions, billing, contracts,
29 clients and partners. And be assure that if you wouldn't pay,
30 all files and documents would be publicated for everyones view and also we would notify all your clients and
31 partners about this leakage with direct links.
32 So if you want to avoid such a harm for your reputation, better pay the amount that we asking for.
33
34 -----
35 ! HERE IS THE SIMPLE MANUAL HOW TO GET CONTACT WITH US VIA LIVE CHAT !
36 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
37
38 a) Download and install TOR browser from this site : https://torproject.org
39 b) For contact us via LIVE CHAT open our website :
40 [REDACTED]
41
42 d) If Tor is restricted in your area, use VPN [REDACTED]
43
44 When you open LIVE CHAT website follow rules :
45
46 Follow the instructions on the website.
47 At the top you will find CHAT tab.
48 Send your message there and wait for response (we are not online 24/7, so you have to wait for your turn).
49
50
```

*Ragnar Locker Ransomware Message (Source)*



## Detected Ransomware Strains

### Ragnar Locker



CWT Ransomware Attack Payment Negotiations (Source)



## Detected Ransomware Strains

### Netwalker Ransomware

Netwalker ransomware, designed by the Circus Spider group, was responsible for the UCSF attack, profiting a total of **\$1,140,895**, which represents 1.6% of the top crypto ransomware payments.

The Circus Spider group quickly shifted Netwalkers's model to Ransomware-as-a-Service, much like its competitors, to increase its expansion and adoption, allowing them to operate on a larger scale, target more organizations, and increase the size of ransoms. While Netwalker operated like most other ransomware variants, it went further than holding its victim's data hostage. Circus Spider has also been known for immediately leaking parts of the stolen data online at the same time that it demanded the ransom payment. Failure to comply in time meant that Circus Spider would upload the remaining stolen data to the dark web.

### LockBit

The LockBit group, one of the largest international ransomware groups, was responsible for the BRB Bank attack, profiting a total of **\$957,245**, which represents 1.4% respectively.

The group is believed to operate out of Eastern Europe and has developed a sophisticated piece of malware called LockBit, named after itself. The group uses the Ransomware-as-a-Service model and frequently invents new ways to beat its competition.

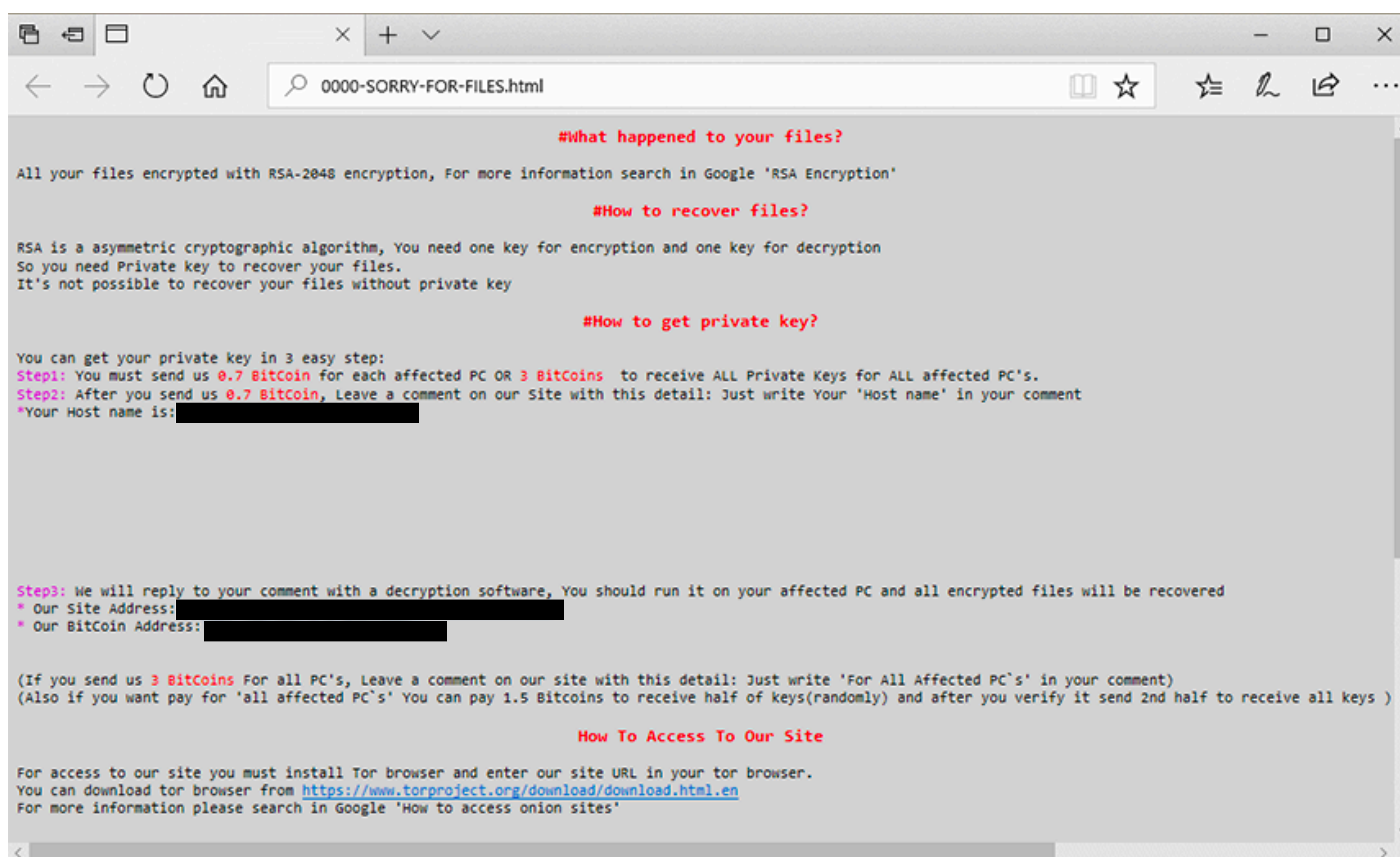
The ransomware is advertised among its community as the fastest and most efficient encryption software and is notable for additional tactics, such as the StealBit malware, which automates data exfiltration. LockBit is used for highly-targeted attacks on corporate and enterprise organizations.



## Detected Ransomware Strains

### SamSam

The SamSam group, responsible for the Jackson County attack, profited a total of **\$400,000**, which represents 0.6% respectively.



*SamSam Ransomware Message (Source)*

SamSam, also known as Samas or SamsamCrypt, is believed to be created, distributed, and operated from [Iran](#). SamSam has specialized in targeted ransomware attacks, breaking into networks, and encrypting multiple computers across an organization before issuing a high-value ransom demand. A trait of the SamSam group has been to thoroughly monitor networks and user activities for an extended period before demanding a ransom payment.

The group has targeted multiple entities across different industries and critical infrastructure to increase its chance of a big payout for data recovery, such as the transportation, education, and health sectors. While most of the attacks targeted organizations in the United States, other attacks have been reported in the UK, France, Portugal, Australia, Canada, Israel, and the Middle East.

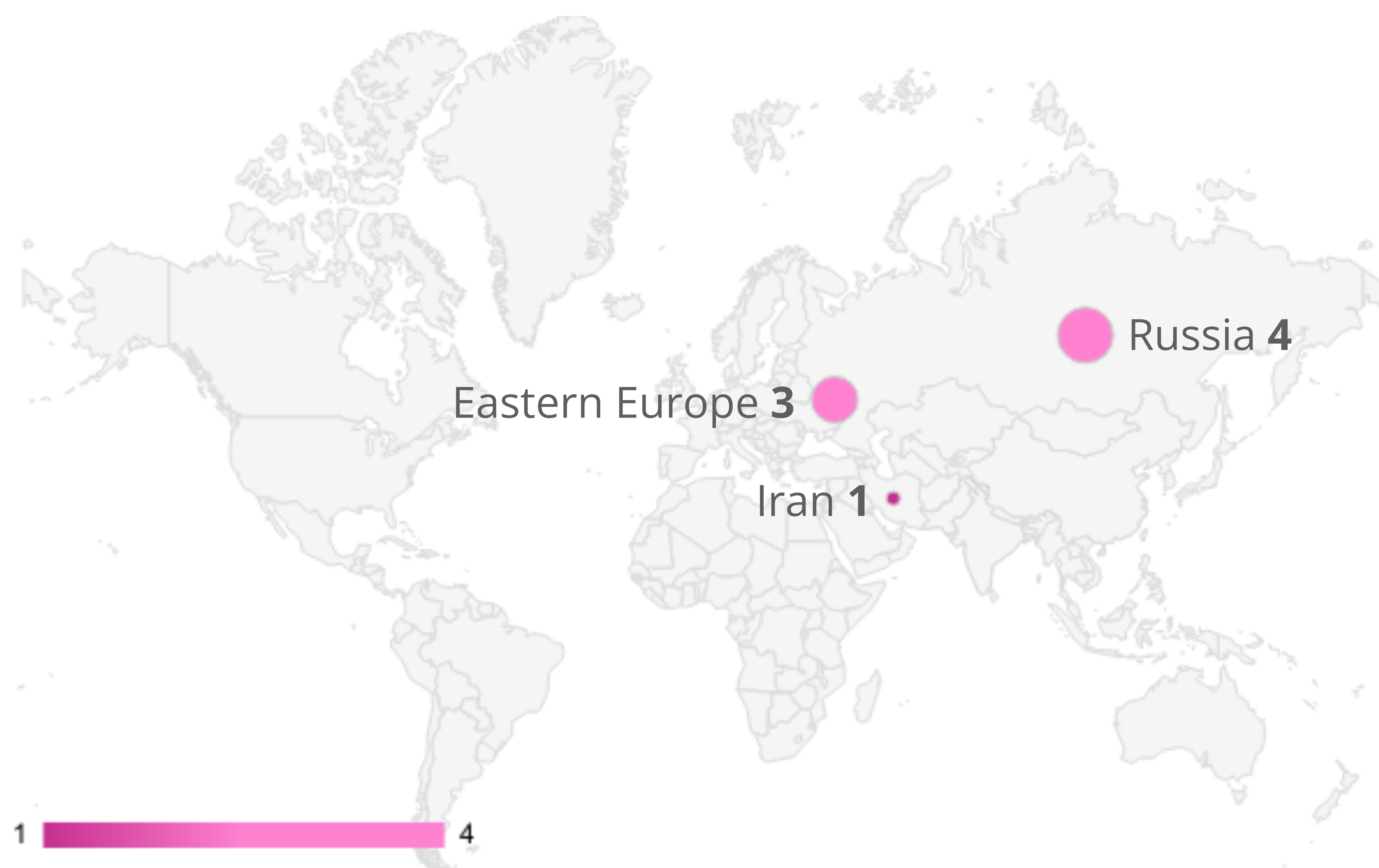


## Detected Ransomware Strains

### Clap Ransomware

The Clap ransomware, distributed by the TA505 group, was responsible for the University of Maastricht attack, profiting **\$218,000**, which represents 0.3% respectively.

The Clap ransomware, named after the Russian word “klop,” which means “bed bug”, is believed to be distributed by the Russian cybercrime group TA505. The group is known for its attacks against financial and public institutions and retail companies using malicious spam campaigns and different kinds of malware. The Clap ransomware encrypts pictures, videos, music, databases, and papers, preventing victims from accessing personal data. Urgent data recovery is often necessary for public institutions, which makes them an appealing target for such attacks.



*Origin of Detected Ransomware Strains*



# BITCOIN AS A RANSOM PAYMENT

## WHY?

All **\$69,316,140** in ransom payments was paid in **Bitcoin**. With several ransom payments in the dozens of millions, it would be challenging to wire such amounts through the legacy banking system without getting caught.

Additionally, it can be difficult even to wire the money in the first place because most of the top ransomware groups operate in high-risk jurisdictions that have tenuous ties with financial systems in Europe and North America.

Lazarus Group, a prolific, North Korea-backed hacking group, has been using Chinese or Malaysian bank accounts to sidestep sanctions. Still, that maneuver would likely only work for smaller amounts rather than upwards of \$40 million.

However, with Bitcoin, the amount of money these groups can receive immediately is vastly larger than ransom payments of \$100,000 or less because of the decentralized nature of the network. It is unsurprising, then, that ransomware groups have turned to cryptocurrencies.

Despite the wide variety of cryptocurrency options available, such as USDC, Ethereum, or even Monero, ransomware groups have relied on Bitcoin for receiving ransom payments. This choice is likely because Bitcoin is the most well-known and easily accessible cryptocurrency for targeted users and organizations.



# TRACING PAYMENTS IS CRYPTOCURRENCY ANONYMOUS AND UNTRACEABLE?

There is now a fast-growing industry of companies that specialize in finding criminals using on-chain data and other techniques, such as Chainalysis, TRM Labs, and Elliptic. Finding criminals is possible because on the Bitcoin network, it's possible to view all addresses that the ransomware recipient address has ever interacted with and potentially trace that chain to the real owner. Everyone leaves a digital trace online.

Clustering is an important technique that aids in unmasking criminals. It works by analyzing Bitcoin blockchain data to find links between addresses and merge them into a group likely to be controlled by the same person or entity.

After the whole blockchain is analyzed, connections appear between the cluster of illicit actors and clusters of services, exchanges, other illicit actors, and personal wallets. This information can then be used to assist in further investigative activities.



# CASHING OUT HOW?

Ransomware groups sometimes use centralized exchanges to convert cryptocurrency into fiat funds. To avoid being caught, they create accounts with fake government IDs purchased on the dark web, but there are pitfalls with that approach discussed below. These groups might also use the crypto directly to buy goods and services like watches, cars, servers, etc.

However, most professional ransomware groups are located in hard-to-reach jurisdictions like Iran, Russia, and North Korea, so they have unique methods of cashing out. For example, ransomware gangs from North Korea are linked to the government and rely on those connections to cash out money through Chinese exchanges. In Russia, it is also possible to cash out dirty money by using the OFAC-sanctioned exchange, Garantex.io, or a lot of other “private” exchanges, which do not care about the source of funds.

## USING EXCHANGES A BREAKTHROUGH FOR TRACING BACK CRIMINALS?

Cybercriminals swap stolen crypto from one blockchain to another, but they are often not cautious enough and use addresses that can lead to their real identities. But most successful investigative cases rely on obtaining information from centralized exchanges. Even when cybercriminals use fake identities on exchanges, they still leave behind clues, such as IP addresses, bank accounts, etc.

As a practical example of how ransomware groups operate, in October 2021, DarkSide moved its Bitcoin funds from one of its wallets in what appeared to be the beginning of a money laundering operation. The group split \$6.8 million into seven separate Bitcoin wallets. This tactic made it more difficult to trace the group as it tried to convert the cryptocurrency into fiat. Small amounts were then transferred to exchanges.



# AVOIDING DETECTION

## WHAT ARE THE STANDARD TECHNIQUES?

To fight back against traceability, ransomware groups have used obfuscation techniques to increase anonymity and avoid detection.

- Ransomware groups frequently use mixers or tumblers to obscure the destination of their illicit Bitcoin ransom gains.
- Ransomware code is sometimes written in the style of another group to throw investigators off the trail.
- Additionally, the operational security of these groups is very complex. They use operating systems built for security, such as Linux Tails, and have several layers of network connections to obscure their origin, such as VPN->VPN->Dedicated server->TOR network->Dedicated server.
- Most importantly, they use their place of operations as a security layer: Iran, Russia, and the DPRK are all jurisdictions that do not cooperate with foreign subpoenas.



# ORGANIZATION PROTECTION WHAT MEASURES TO IMPLEMENT?

Big companies and organizations will always be targets because of their size. However, there are several measures they can take to ensure being targeted doesn't turn into a disastrous ransomware attack.

- First, all organizations should have extensive and regular backups of crucial information, as well as a recovery plan for restoring the data after an attack.
- Second, companies should keep systems and applications up to date to avoid exploitation.
- Third, companies should provide training on common phishing attack vectors and why it's important not to open suspicious email attachments.
- Fourth, companies should use an intrusion detection system and antivirus software.

CDProjekt Red, a videogame development firm based in Poland, is an example of a company that successfully used backups to avoid paying a ransom. In February 2021, the HelloKitty gang [hacked](#) the firm. While the group successfully stole the source code of game projects in development and encrypted devices, CDProjekt did not pay the ransom because it had backups to restore the lost data.





## ImmuneFi

ImmuneFi is the leading bug bounty and security services platform for web3 protecting over \$60 billion in user funds. ImmuneFi features a massive community of whitehat hackers who review projects' blockchain and smart contract code, find and responsibly disclose vulnerabilities, and get paid for making crypto safer. With ImmuneFi, whitehat hackers are rewarded based on the severity of the vulnerability that they discover, creating incentives for as many experts as possible to examine project code for vulnerabilities.

ImmuneFi has pioneered the scaling web3 bug bounties standard, meaning that rewards should be priced accordingly with the severity of an exploit and the volume of funds at risk, which resulted in the company building the largest community of security talent in the web3 space.

## Total bounties paid

ImmuneFi has paid out over **\$65 million** in total bounties, while saving over **\$25 billion** in user funds.

## Total bounties available

ImmuneFi offers over **\$144 million** in available bounty rewards.

## Supported projects

Trusted by established, multi-billion dollar projects like Chainlink, Wormhole, MakerDAO, Compound, Synthetix, and more, ImmuneFi now supports 301 projects across multiple crypto sectors.

## Largest bug bounty payments in the history of software

ImmuneFi has facilitated the largest bug bounty payments in the history of software.

**\$10 million** for a vulnerability discovered in Wormhole, a generic cross-chain messaging protocol.

**\$6 million** for a vulnerability discovered in Aurora, a bridge and a scaling solution for Ethereum.

**\$2.2 million** for a vulnerability discovered in Polygon, a decentralised Ethereum scaling platform that enables developers to build scalable user-friendly dApps.





**The full data sources are available below.**

1. [CNA Financial](#)
2. [JBS](#)
3. [CWT](#)
4. [Brenntag](#)
5. [Colonial Pipeline](#)
6. [Travelex](#)
7. [UCSF](#)
8. [BRB Bank](#)
9. [Jackson County, Georgia](#)
10. [University of Maastricht](#)



If you're a developer thinking about a bug-hunting career in web3, we got you. Check out our [Web3 Security Library](#), and start taking home some of the \$144M in rewards available on ImmuneFi — the leading bug bounty platform for web3.

<https://immunefi.com/>