GUIDEPOINT SECURITY

# Anatomy of Ransomware

Secure Delaware - October 2023

GUIDEPOINT
SECURITY

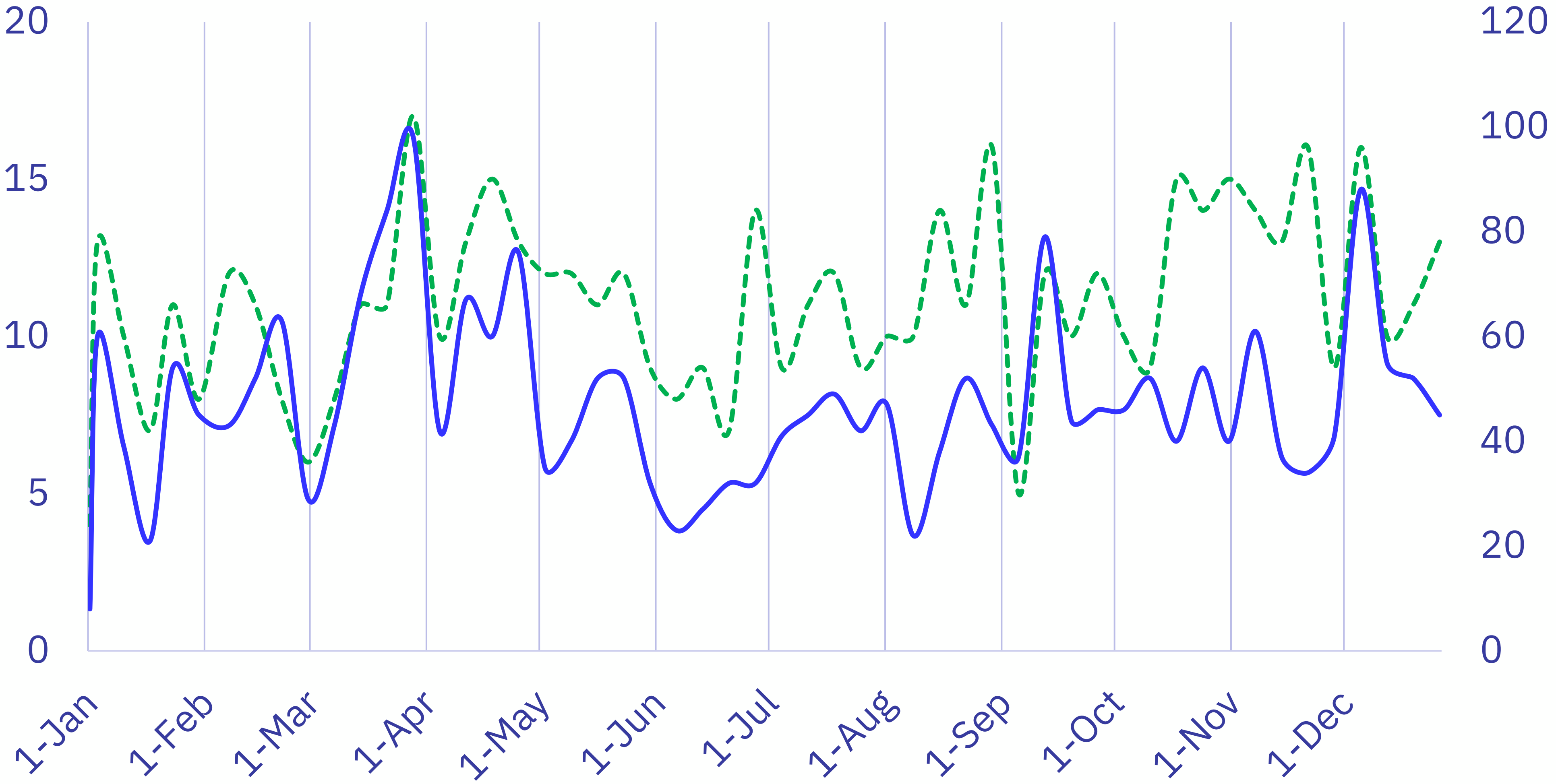
WHY RANSOMWARE?

# Increasingly prevalent in today's threat landscape

**Ransomware** is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

- Can impact organizations regardless of vertical, size or other factors
- 3 Usual Options: Restore, Accept Loss, Pay
- Largely Successful for Criminals
  - Simple Attack Vectors (Phishing, RDP, Vulns)
  - Continued evolution of criminal threats
- Potential for heavy impact
  - Operations
  - Brand
  - Disclosure
  - Costs
- Variety of considerations
- Double/Triple Extortion (Data Theft/DDOS)

# Rate of Publicly Posted Ransomware Victims (2022)



● Total Posts **2507**

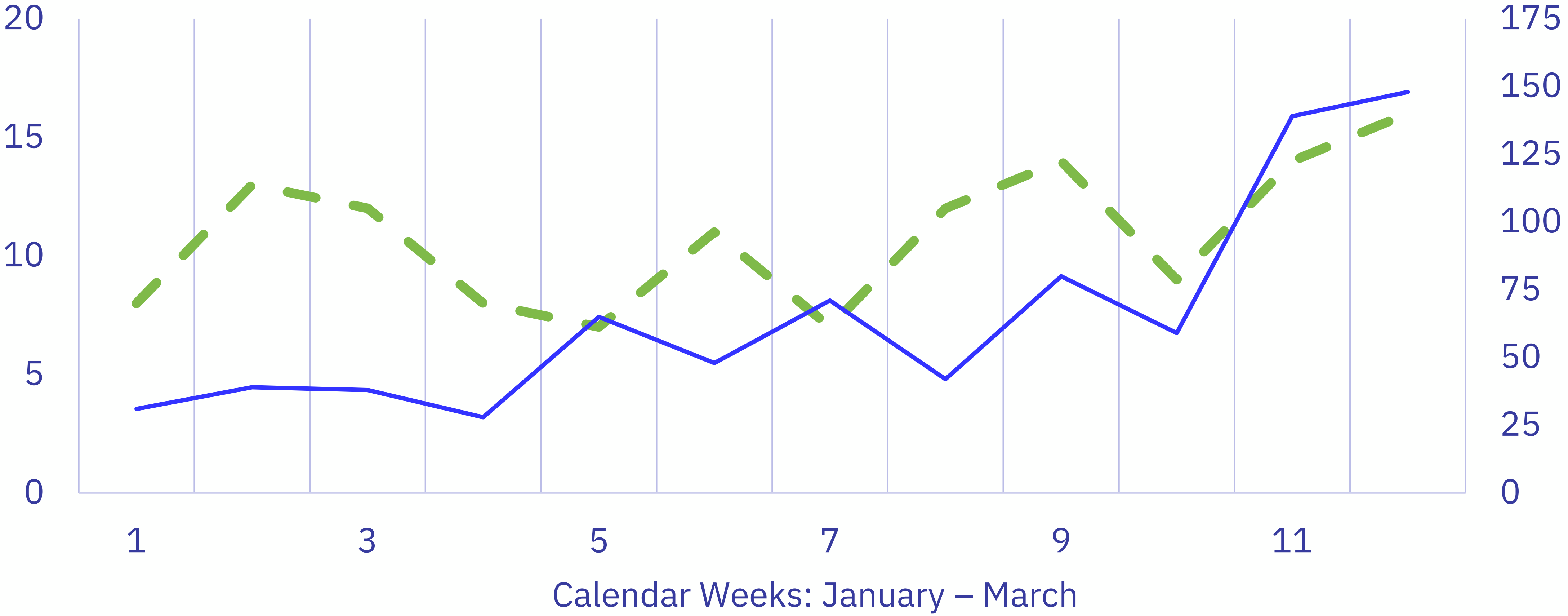
● Total Groups **54**

Average Posts per Week **48.1**

Average Groups per Week **11.2**

GUIDEPOINT SECURITY

# Rate of Publicly Posted Ransomware Victims (Q1 2023)



● Total Posts **849**

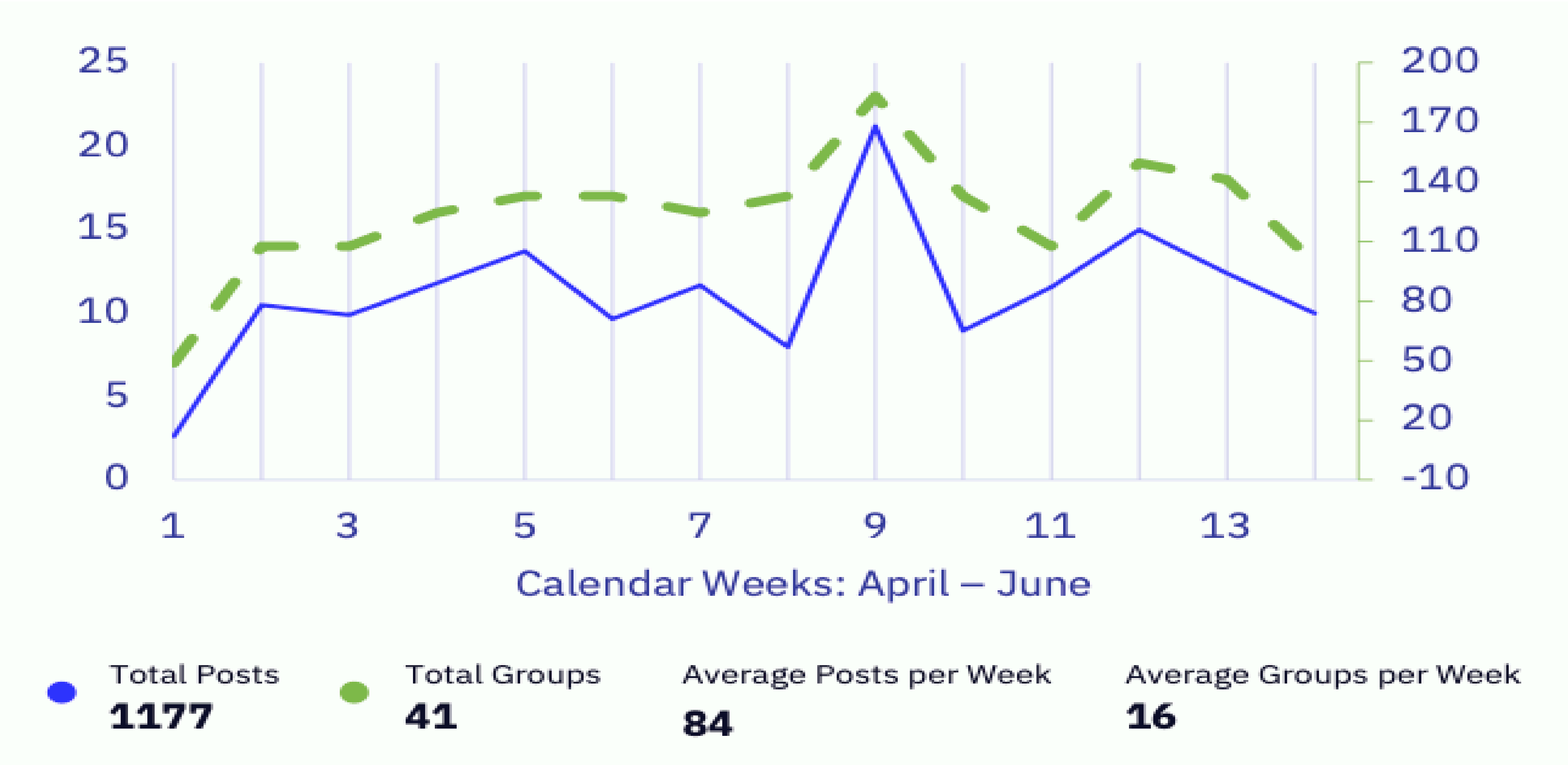
● Total Groups **29**

Average Posts per Week **65**

Average Groups per Week **11**

GUIDEPOINT SECURITY

# Rate of Publicly Posted Ransomware Victims (Q2 2023)



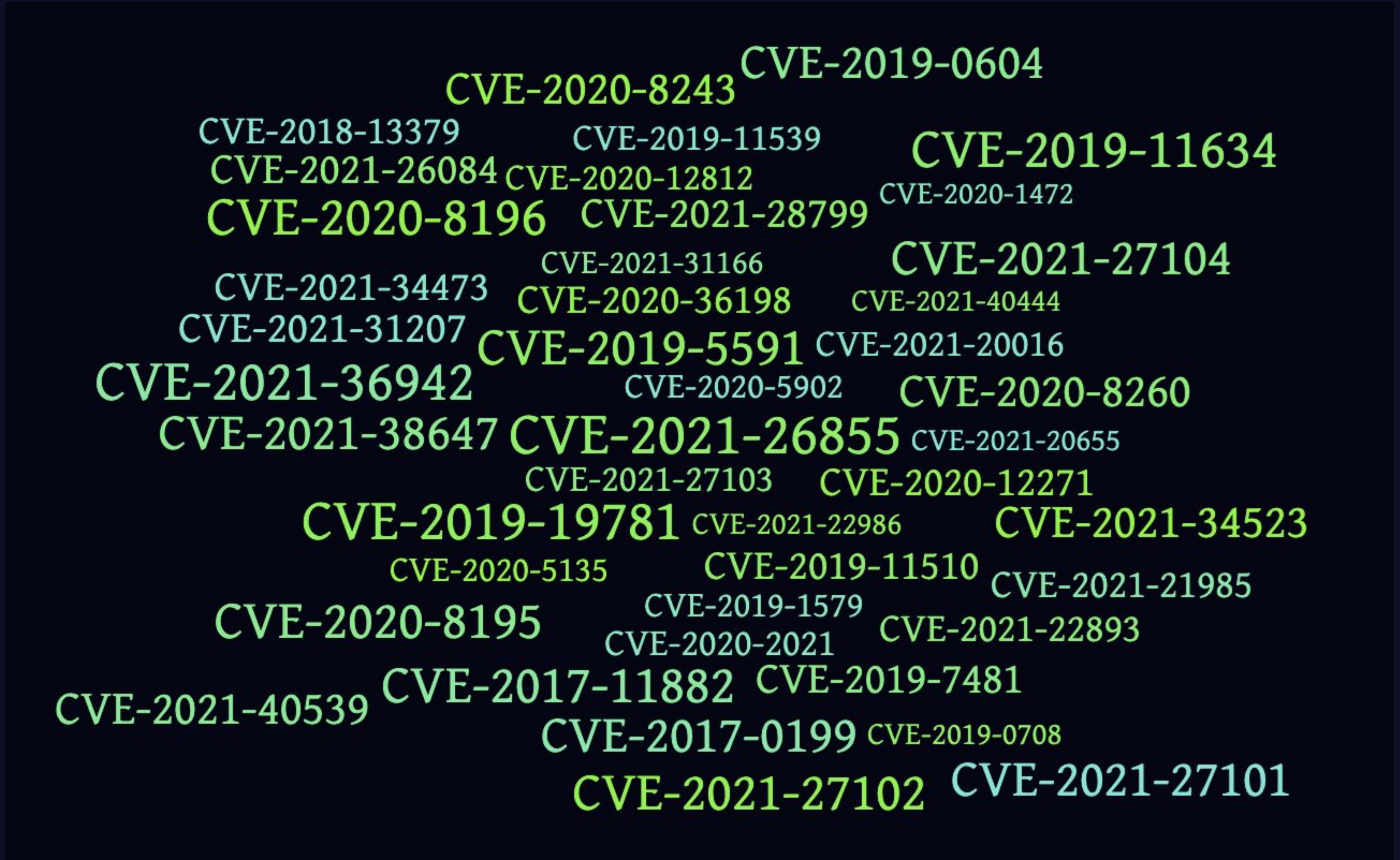
# Ransomware H1 | 2023

- Increased Volume
- MSPs
- Rebranding
- Encrypting ESX
- Legitimate Tools Usage
- No encryption
- Coercive Tactics
- Mass Exploitation

# Vulnerabilities Exploited by Ransomware Groups

## Platforms:

- Exchange
- Microsoft Office
- Windows
- F5
- Accellion
- vCenter
- FileZen
- Azure
- Zoho Corp.
- Atlassian
- Palo Alto
- Sophos
- QNAP
- SharePoint
- SonicWall
- Fortinet
- Citrix

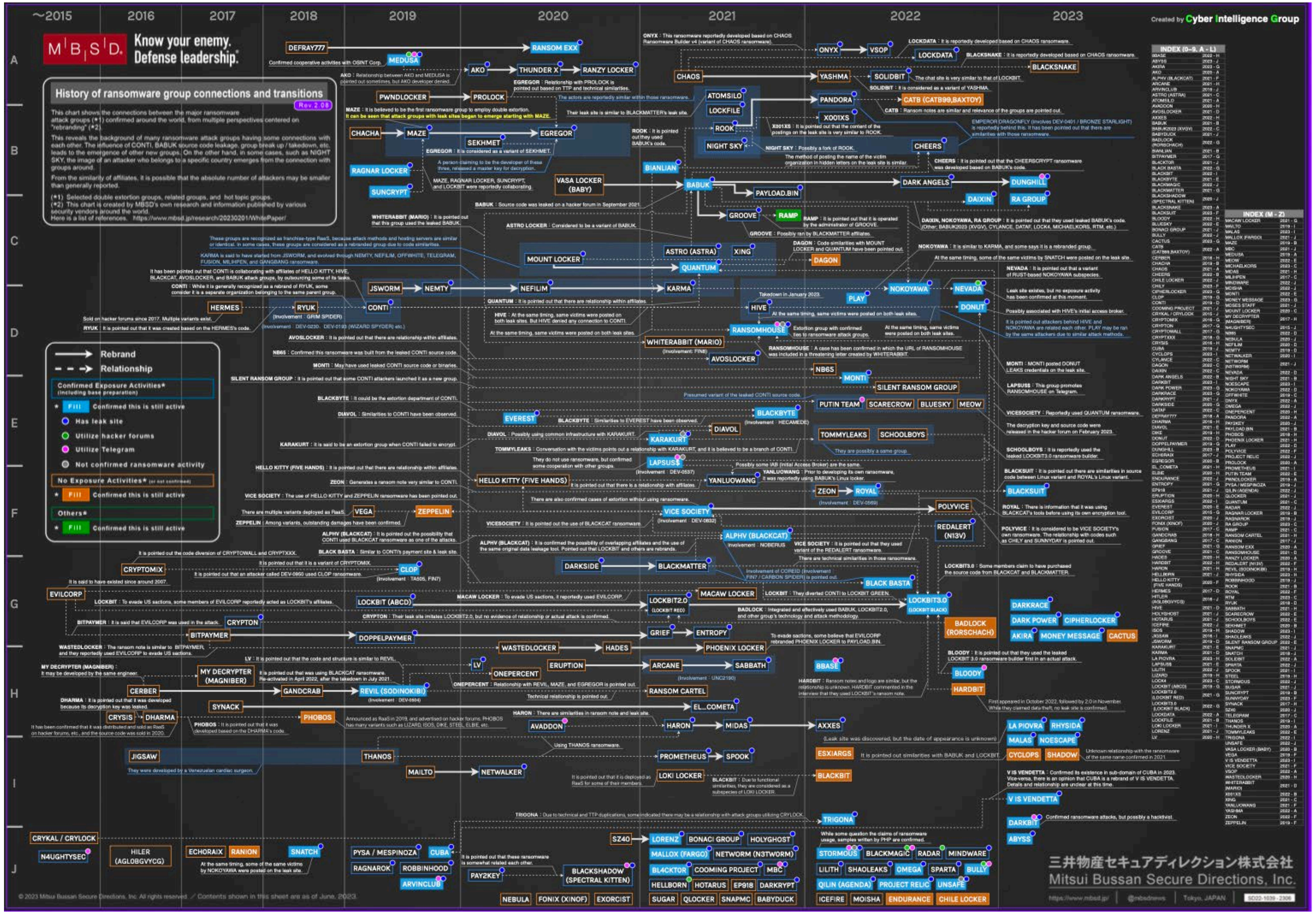


# Tracking Ransomware

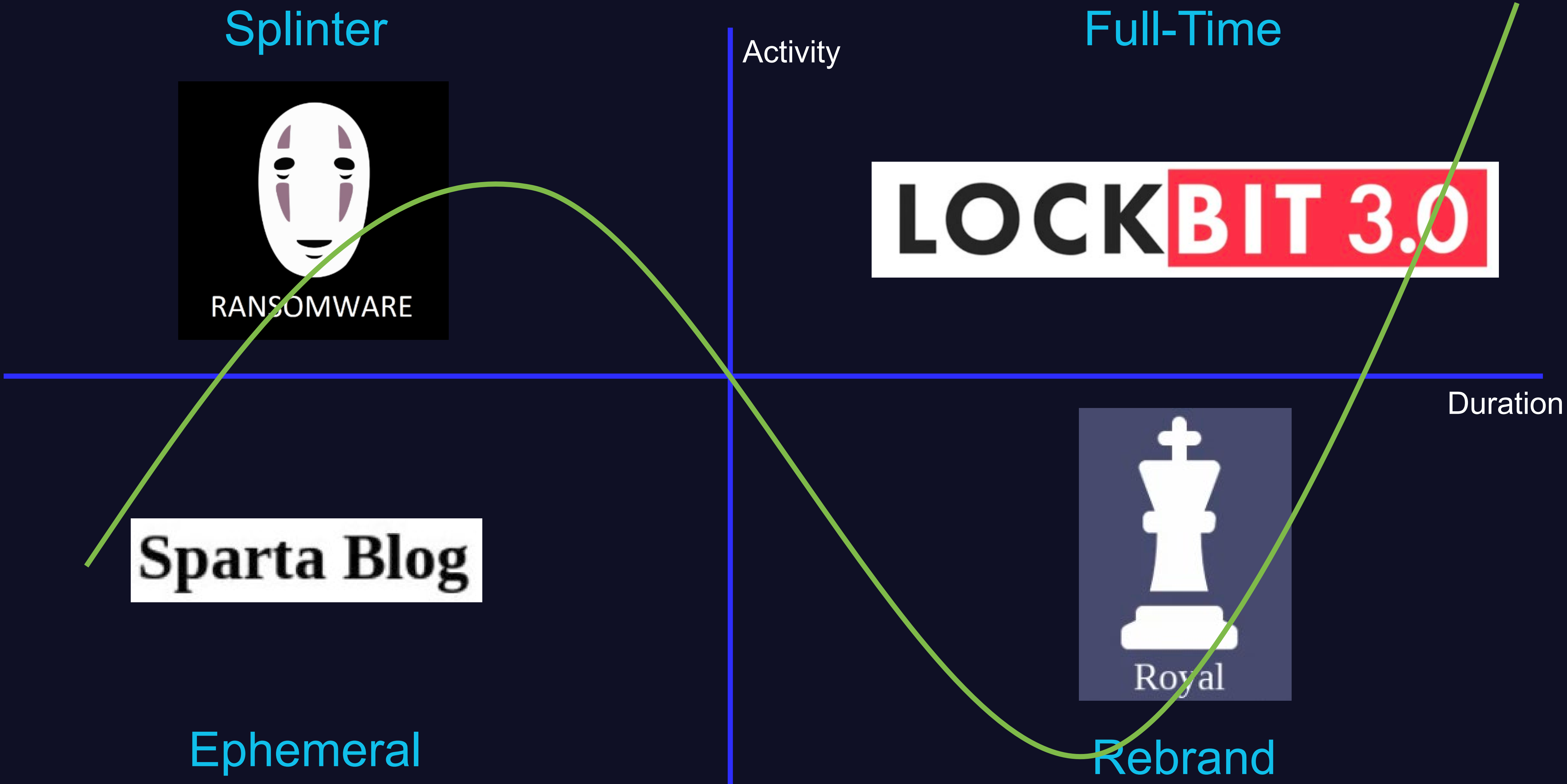
REVIL
Defray777
Darkside
Black Basta
Hive Ransomware
E
Egregor
EVIL CORP
MACAW LOCKER
RYUK
AvosLocker
CONTI
payload.bin
Grief
BLACK Matter
WastedLocker
Bitpaymer
BLACKBYTE
Hades
ransomware.
Maze Ransomware
GANDCRAB RANSOMWARE
MOUNT LOCKER
PHOENIX CRYPTOLOCKER
RANSOMEXX

GUIDEPOINT SECURITY

# A brief history of Ransomware Groups



# A Taxonomy for Ransomware Rebranding



Splinter

Full-Time

Activity

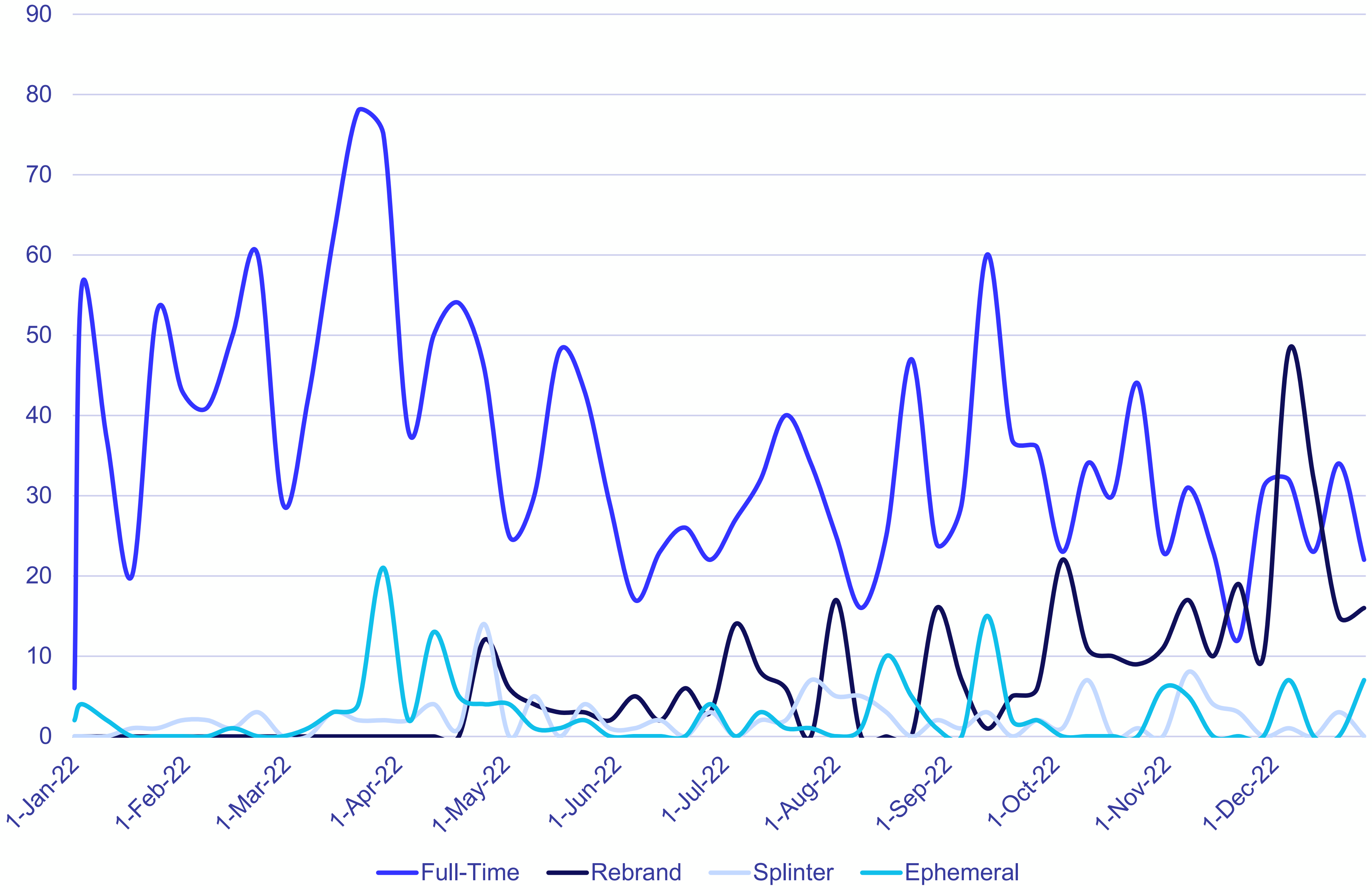
Duration

Ephemeral

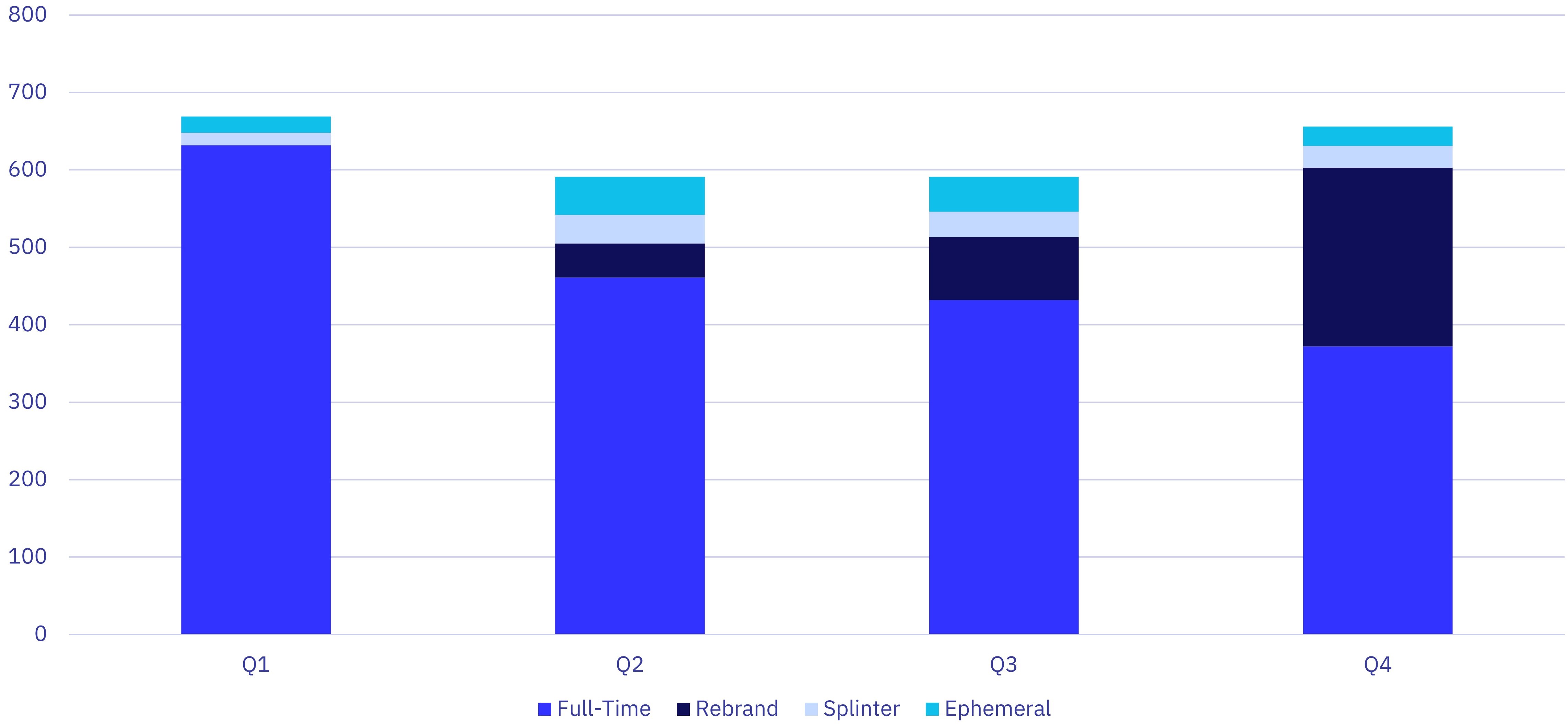
Rebrand

GUIDEPOINT
SECURITY

# Rate of Publicly Posted Ransomware Victims by Group Type (2022)



# Post Rates per Quarter

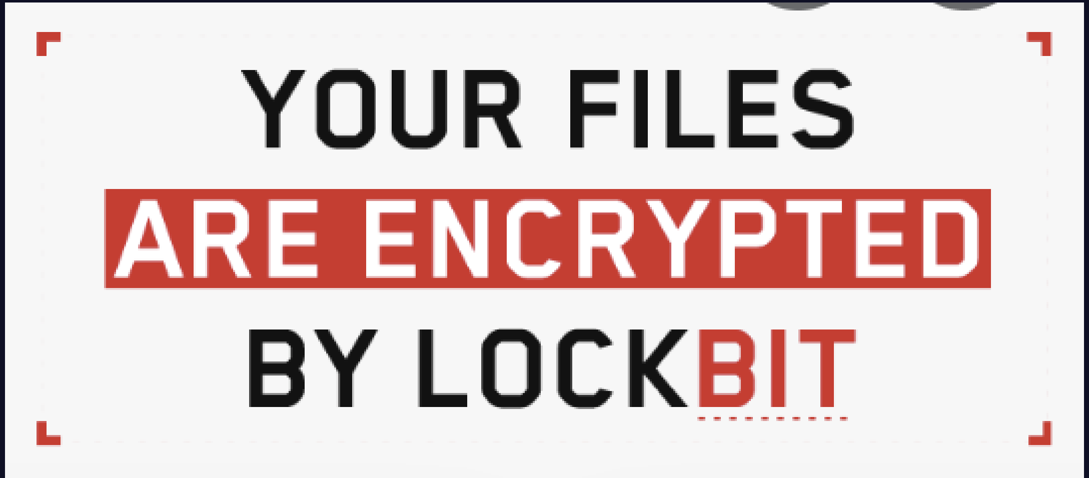


GUIDEPOINT
SECURITY

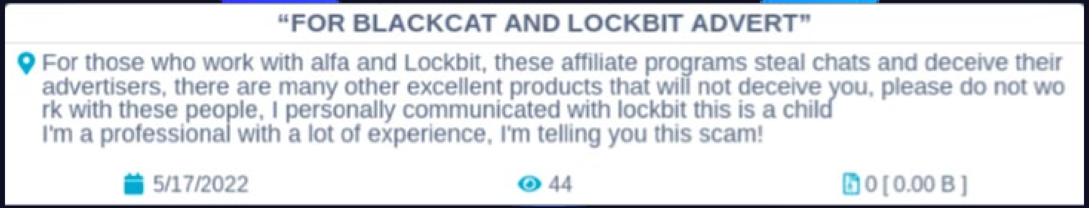
# Ransomware as a Service

## (Affiliate Program/Model)

- Allows for a core group of developers and operators to create the core tooling (ransomware) and administrative platforms used for tracking victims and negotiation.
- If selected to be an affiliate, the individual receives access to the administrative platform, ransomware builder, and other tooling used during ransomware operations.
- It is the affiliate's responsibility to infiltrate the victim environment, steal sensitive data, and encrypt files.
- In many cases, affiliates also perform the negotiation process. If a ransom is paid, the affiliate and ransomware group split the ransom amount.
- Affiliate programs have grown significantly over the last three years which has introduced competition between ransomware groups for the most capable individuals.



YOUR FILES
ARE ENCRYPTED
BY LOCKBIT

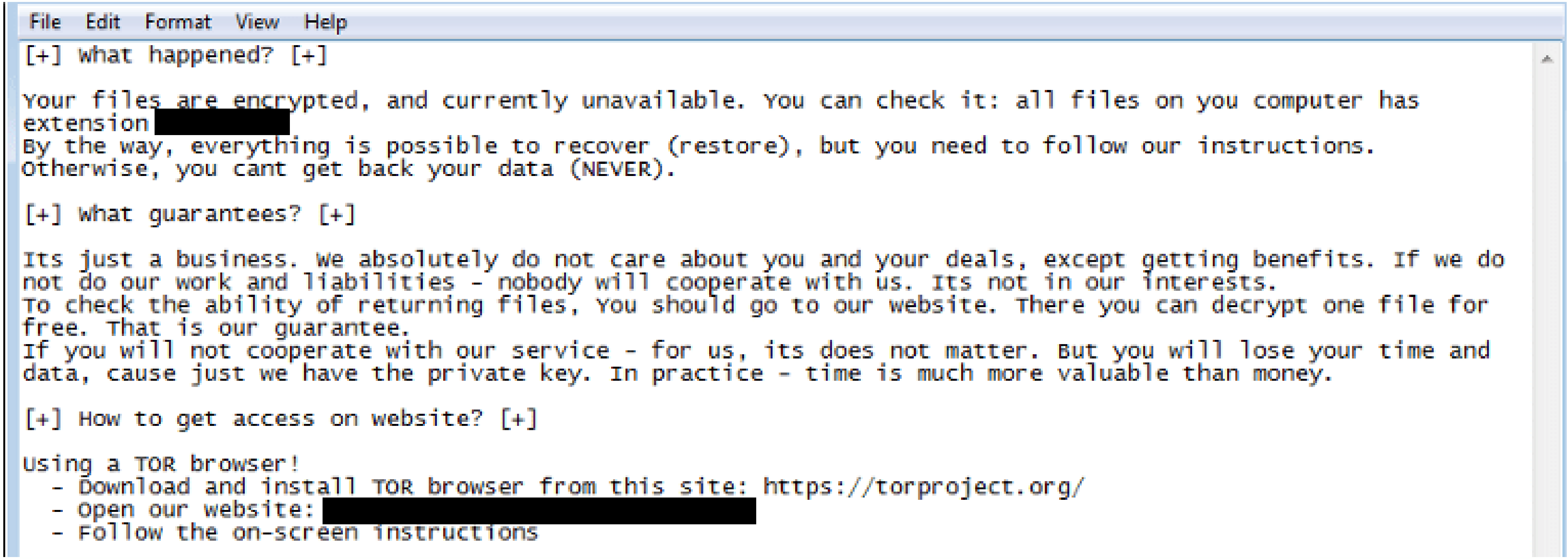


"FOR BLACKCAT AND LOCKBIT ADVERT"

For those who work with alfa and Lockbit, these affiliate programs steal chats and deceive their advertisers, there are many other excellent products that will not deceive you, please do not wo
rk with these people, I personally communicated with lockbit this is a child
I'm a professional with a lot of experience, I'm telling you this scam!

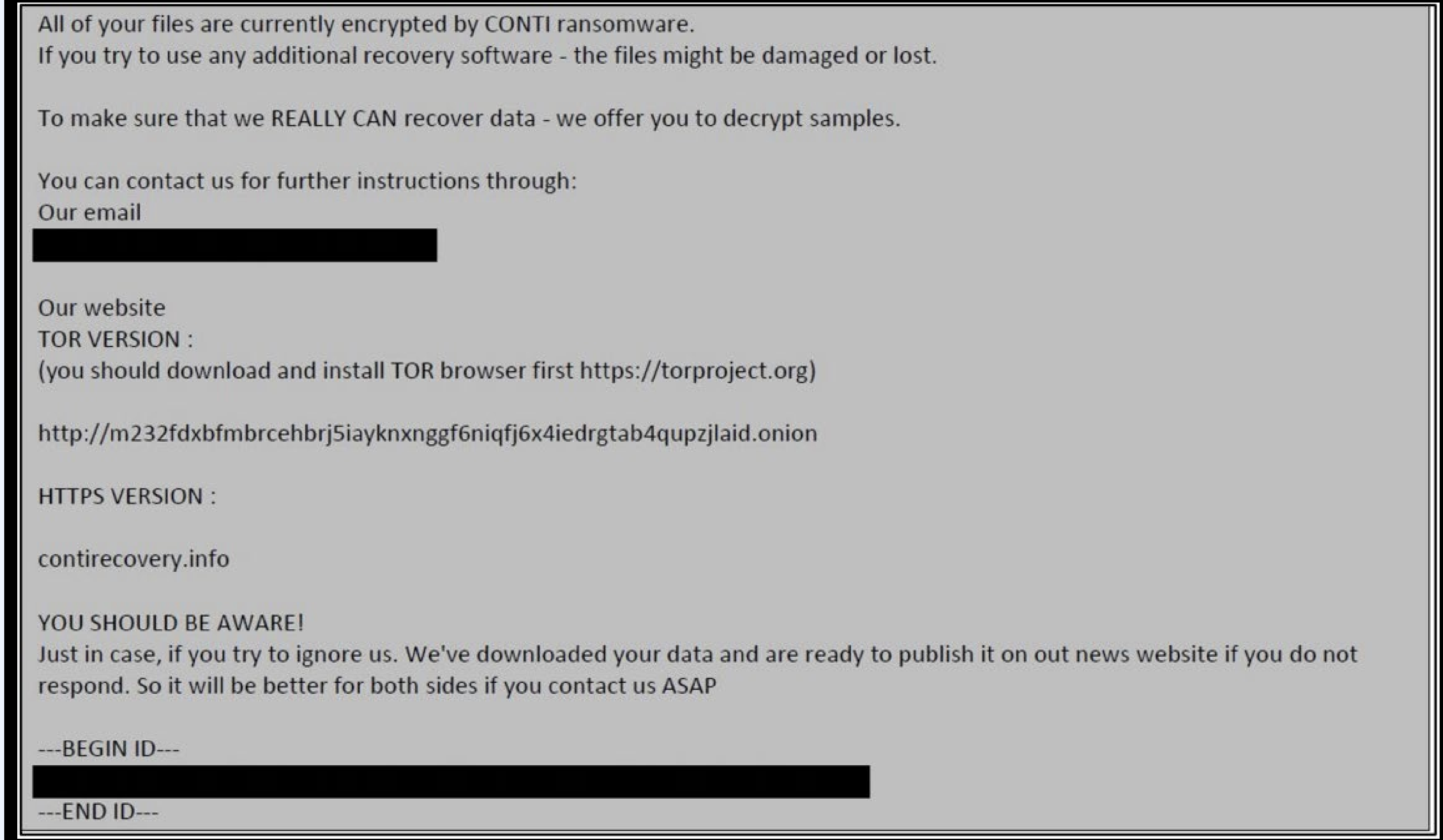
5/17/2022 44 0 [ 0.00 B ]

# Ransom Note Example (Hades)



```
[+] what happened? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has
extension [redacted]
By the way, everything is possible to recover (restore), but you need to follow our instructions.
Otherwise, you cant get back your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do
not do our work and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for
free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and
data, cause just we have the private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]

Using a TOR browser!
  - Download and install TOR browser from this site: https://torproject.org/
  - Open our website: [redacted]
  - Follow the on-screen instructions
```

# Conti Ransomware Note



All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.

To make sure that we REALLY CAN recover data - we offer you to decrypt samples.

You can contact us for further instructions through:
Our email
[redacted]

Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid.onion

HTTPS VERSION :

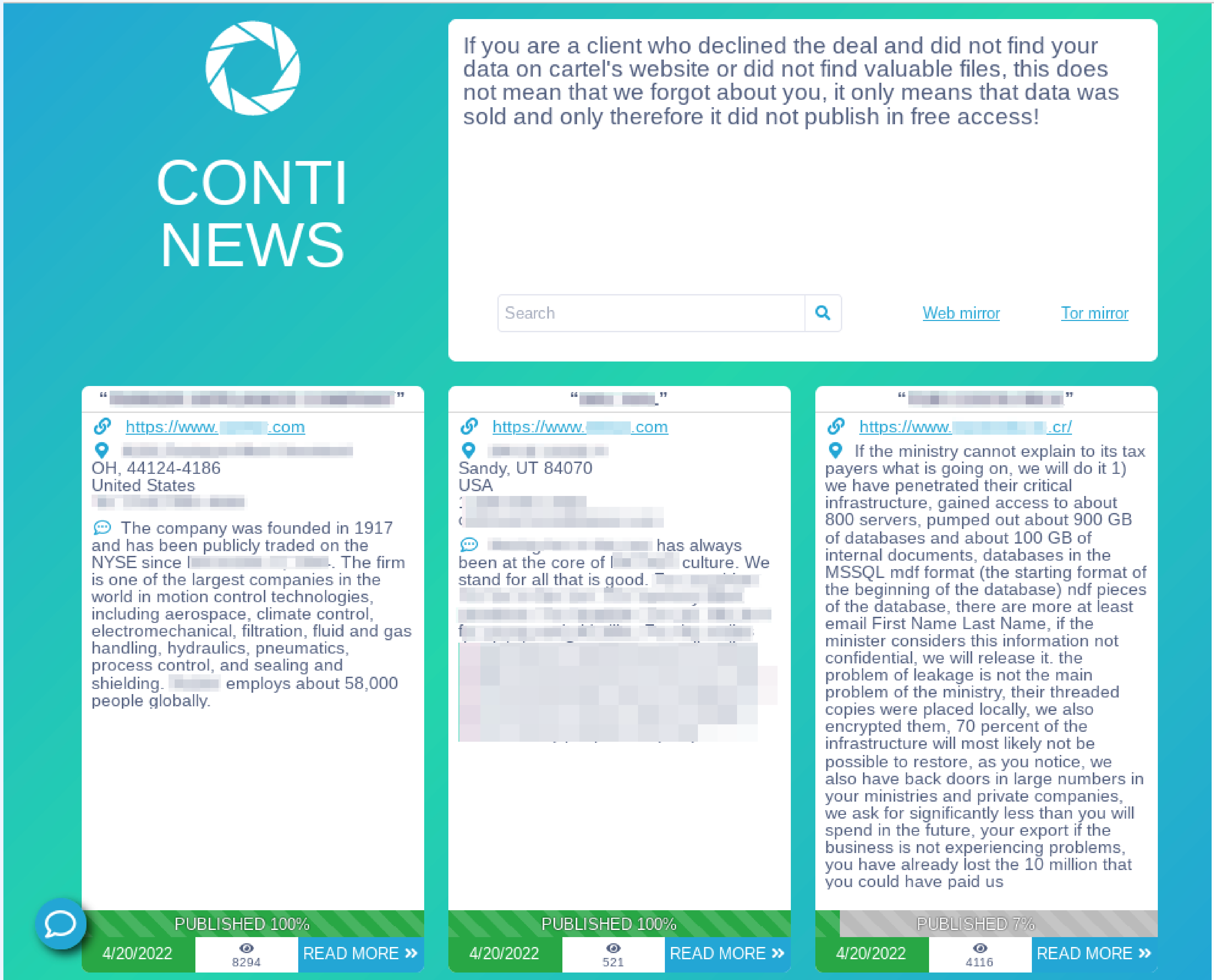
contirecovery.info

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us ASAP

---BEGIN ID---
[redacted]
---END ID---

GUIDEPOINT SECURITY

# Conti News Ransomware Site



If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

"[redacted]"

https://www.[redacted].com

[redacted]
OH, 44124-4186
United States
[redacted]

The company was founded in 1917 and has been publicly traded on the NYSE since [redacted]. The firm is one of the largest companies in the world in motion control technologies, including aerospace, climate control, electromechanical, filtration, fluid and gas handling, hydraulics, pneumatics, process control, and sealing and shielding. [redacted] employs about 58,000 people globally.

PUBLISHED 100%

4/20/2022 | 8294 | READ MORE »

"[redacted]"

https://www.[redacted].com

[redacted]
Sandy, UT 84070
USA
[redacted]

[redacted] has always been at the core of [redacted] culture. We stand for all that is good. [redacted]

[redacted]

PUBLISHED 100%

4/20/2022 | 521 | READ MORE »

"[redacted]"

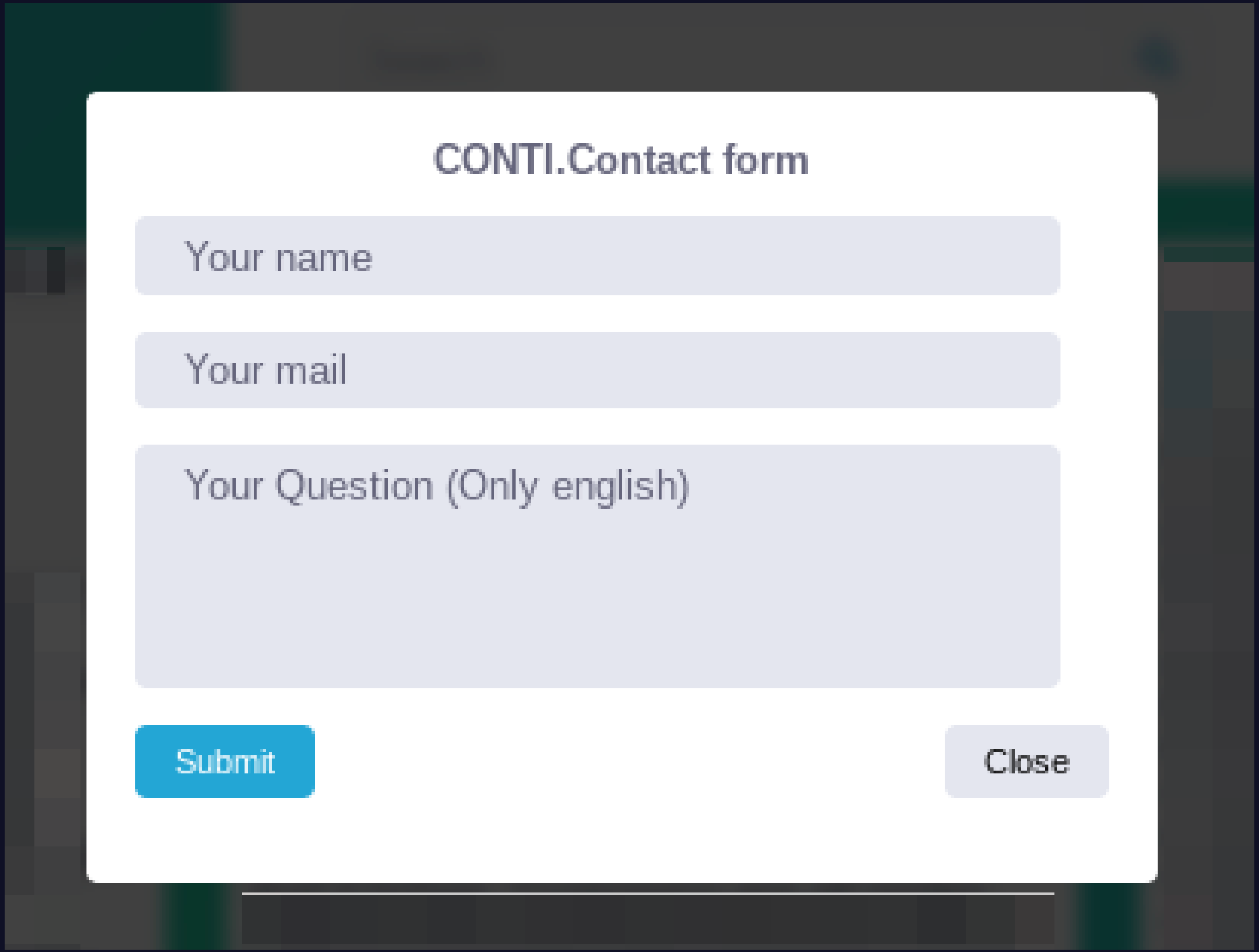
https://www.[redacted].cr/

If the ministry cannot explain to its tax payers what is going on, we will do it 1) we have penetrated their critical infrastructure, gained access to about 800 servers, pumped out about 900 GB of databases and about 100 GB of internal documents, databases in the MSSQL mdf format (the starting format of the beginning of the database) ndf pieces of the database, there are more at least email First Name Last Name, if the minister considers this information not confidential, we will release it. the problem of leakage is not the main problem of the ministry, their threaded copies were placed locally, we also encrypted them, 70 percent of the infrastructure will most likely not be possible to restore, as you notice, we also have back doors in large numbers in your ministries and private companies, we ask for significantly less than you will spend in the future, your export if the business is not experiencing problems, you have already lost the 10 million that you could have paid us

PUBLISHED 7%

4/20/2022 | 4116 | READ MORE »

# Conti's Contact Form



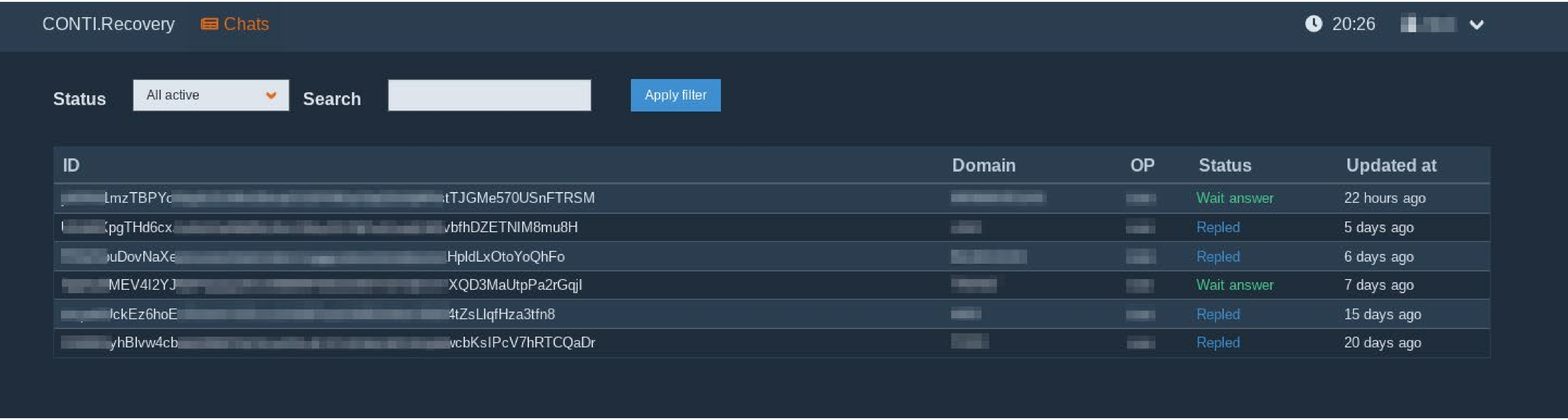
CONTI.Contact form

Your name

Your mail

Your Question (Only english)

# Conti's "Customer" Queue

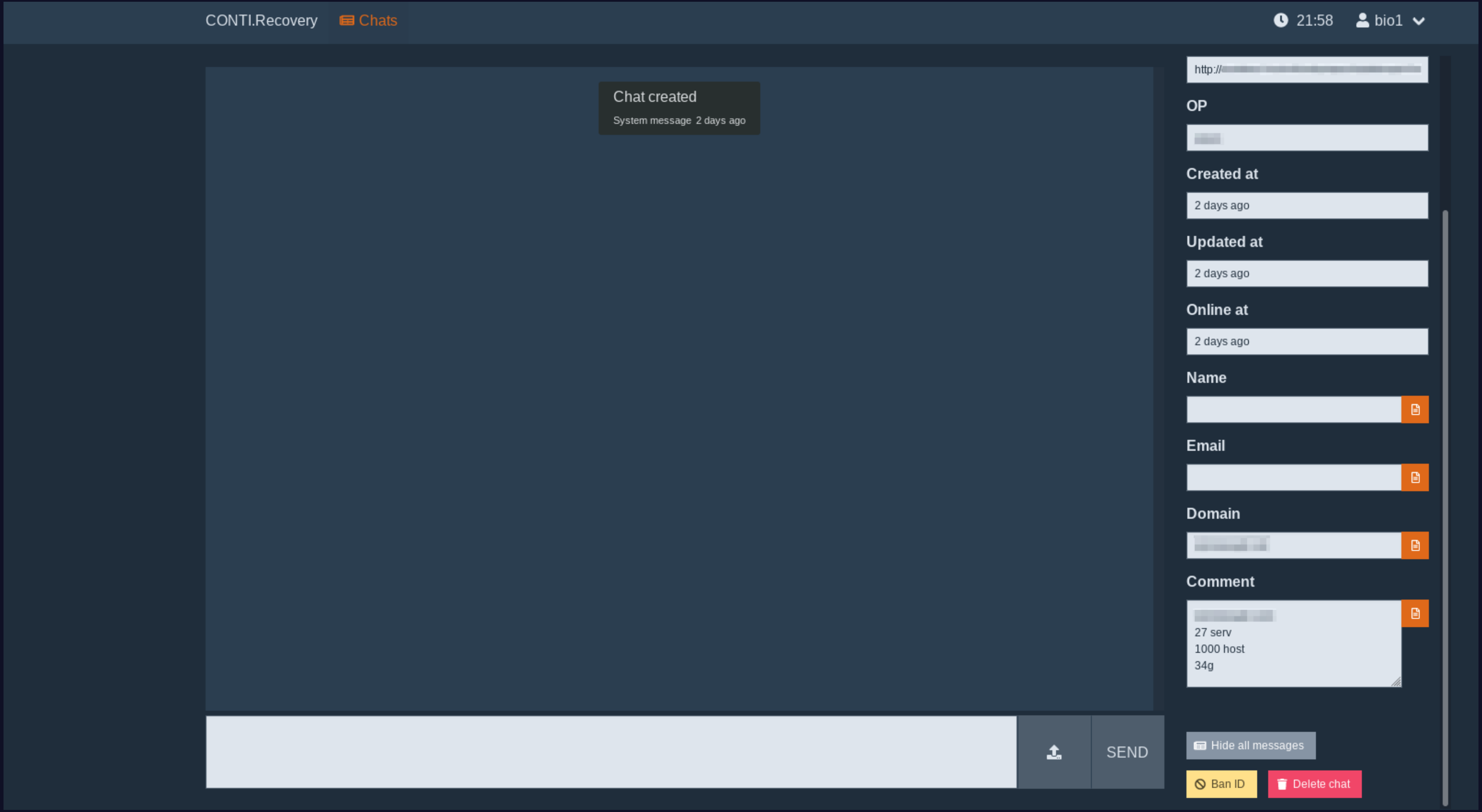


[redacted]

| ID | Domain | OP | Status | Updated at |
|---|---|---|---|---|
| [redacted]lmzTBPYc[redacted]tTJGMe570USnFTRSM | [redacted] | [redacted] | Wait answer | 22 hours ago |
| [redacted]pgTHd6cx[redacted]vbfhDZETNIM8mu8H | [redacted] | [redacted] | Repled | 5 days ago |
| [redacted]uDovNaXe[redacted]HpldLxOtoYoQhFo | [redacted] | [redacted] | Repled | 6 days ago |
| [redacted]MEV4I2YJ[redacted]XQD3MaUtpPa2rGqjl | [redacted] | [redacted] | Wait answer | 7 days ago |
| [redacted]lckEz6hoE[redacted]4tZsLlqfHza3tfn8 | [redacted] | [redacted] | Repled | 15 days ago |
| [redacted]yhBlvw4cb[redacted]wcbKsIPcV7hRTCQaDr | [redacted] | [redacted] | Repled | 20 days ago |

GUIDEPOINT SECURITY

# Conti’s Real-Time Chat Capability



Chat created
System message 2 days ago

http://[redacted]

OP
[redacted]

Created at
2 days ago

Updated at
2 days ago

Online at
2 days ago

Name

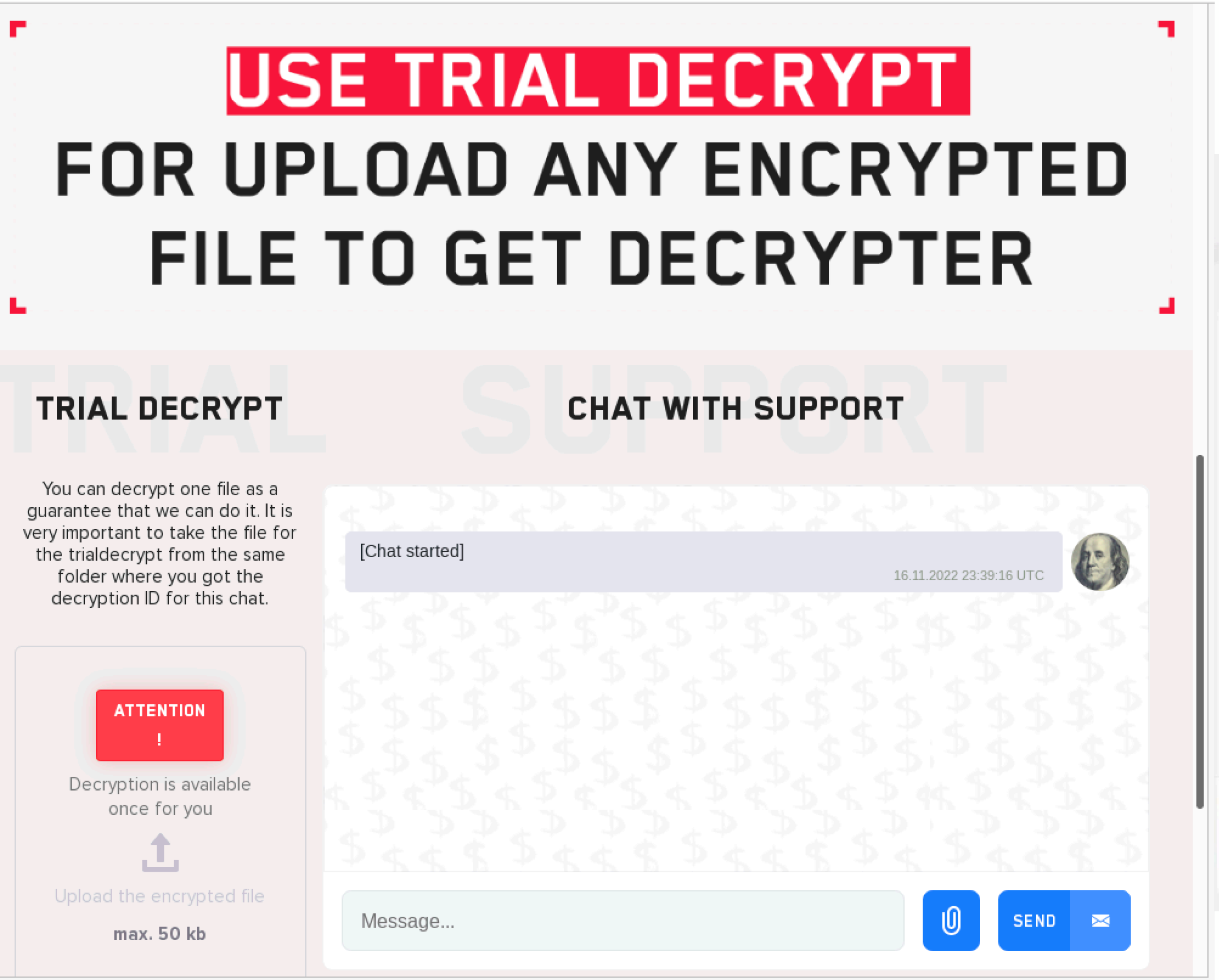
Email

Domain
[redacted]

Comment
[redacted]
27 serv
1000 host
34g

GUIDEPOINT SECURITY

# Lockbit Chat



USE TRIAL DECRYPT

FOR UPLOAD ANY ENCRYPTED FILE TO GET DECRYPTER

TRIAL DECRYPT

You can decrypt one file as a guarantee that we can do it. It is very important to take the file for the trialdecrypt from the same folder where you got the decryption ID for this chat.

ATTENTION !

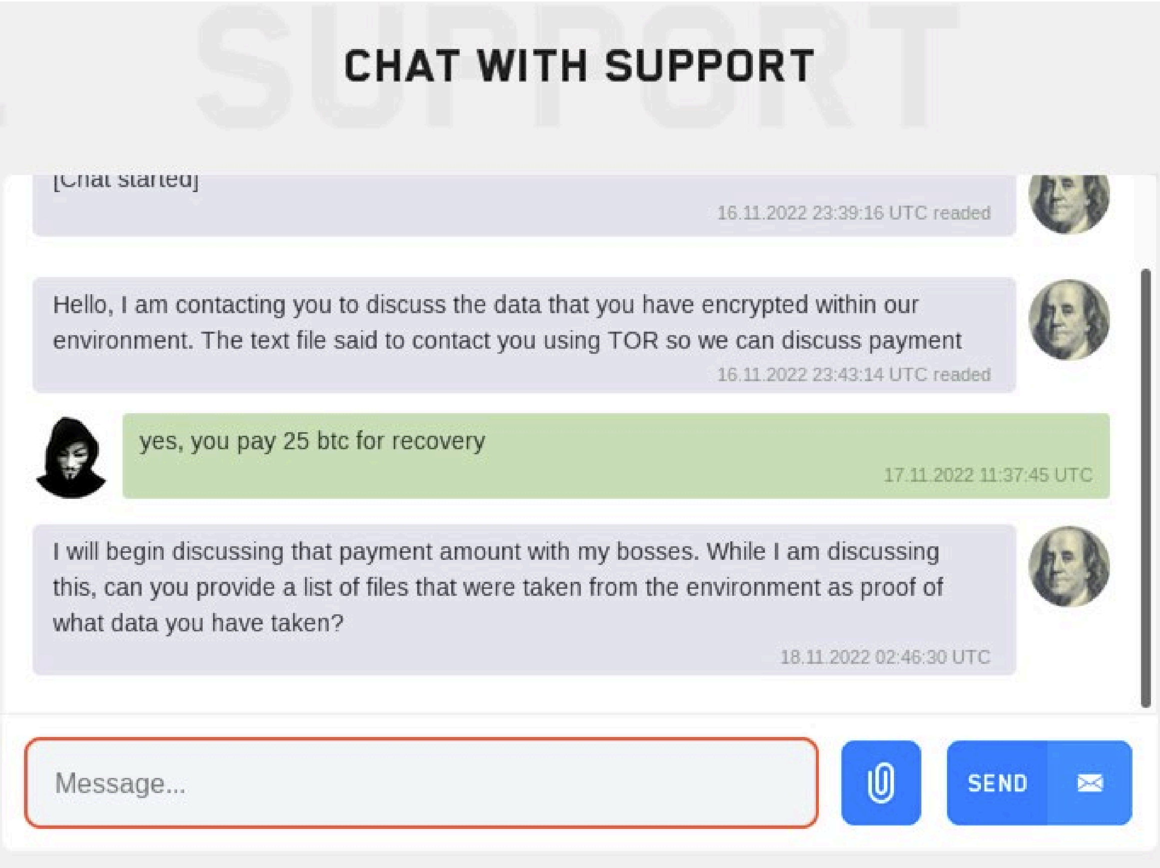
Decryption is available once for you

Upload the encrypted file

max. 50 kb

CHAT WITH SUPPORT

[Chat started]
16.11.2022 23:39:16 UTC



CHAT WITH SUPPORT

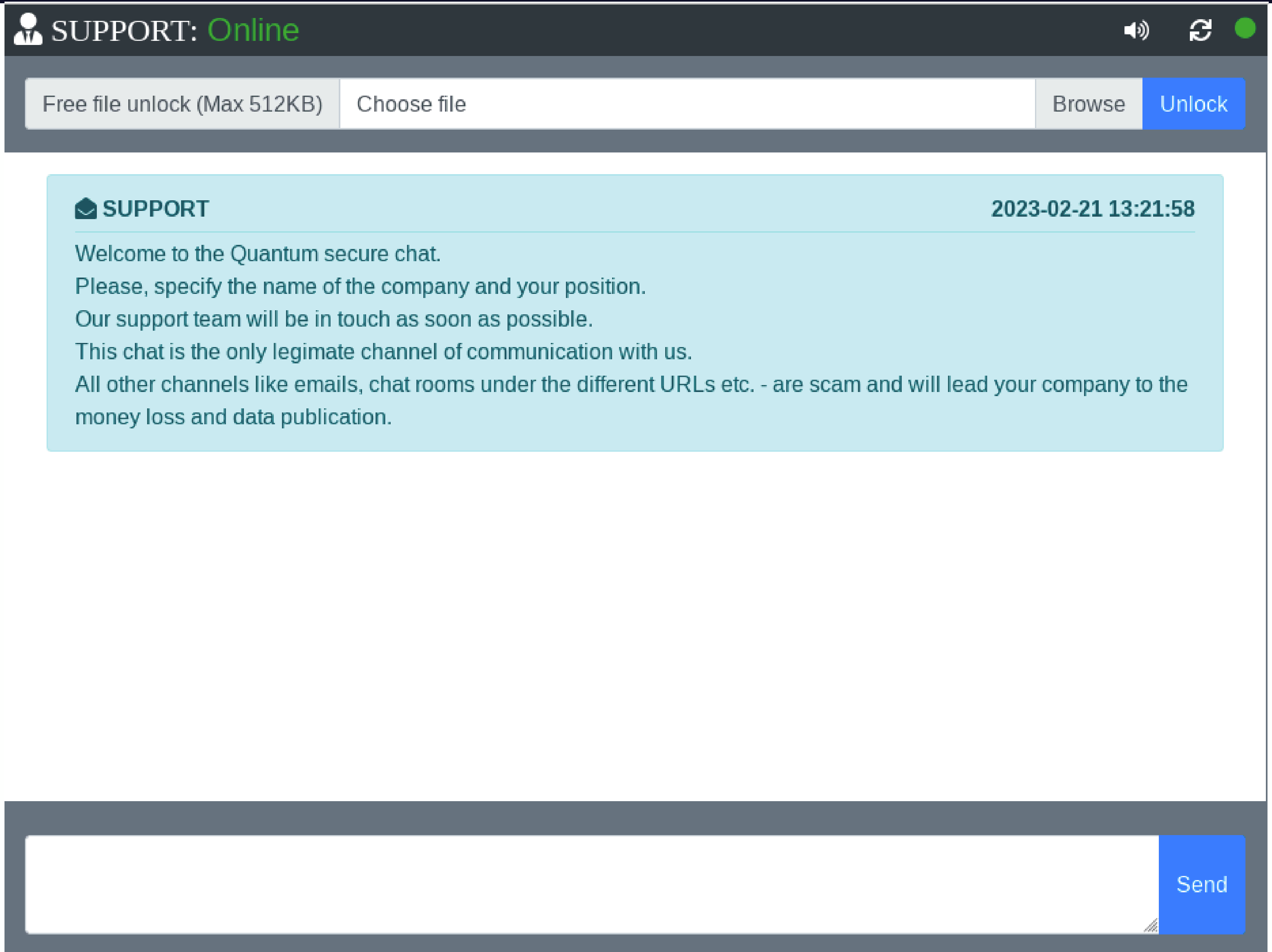
[Chat started]
16.11.2022 23:39:16 UTC readed

Hello, I am contacting you to discuss the data that you have encrypted within our environment. The text file said to contact you using TOR so we can discuss payment
16.11.2022 23:43:14 UTC readed

yes, you pay 25 btc for recovery
17.11.2022 11:37:45 UTC

I will begin discussing that payment amount with my bosses. While I am discussing this, can you provide a list of files that were taken from the environment as proof of what data you have taken?
18.11.2022 02:46:30 UTC

# Quantum Chat

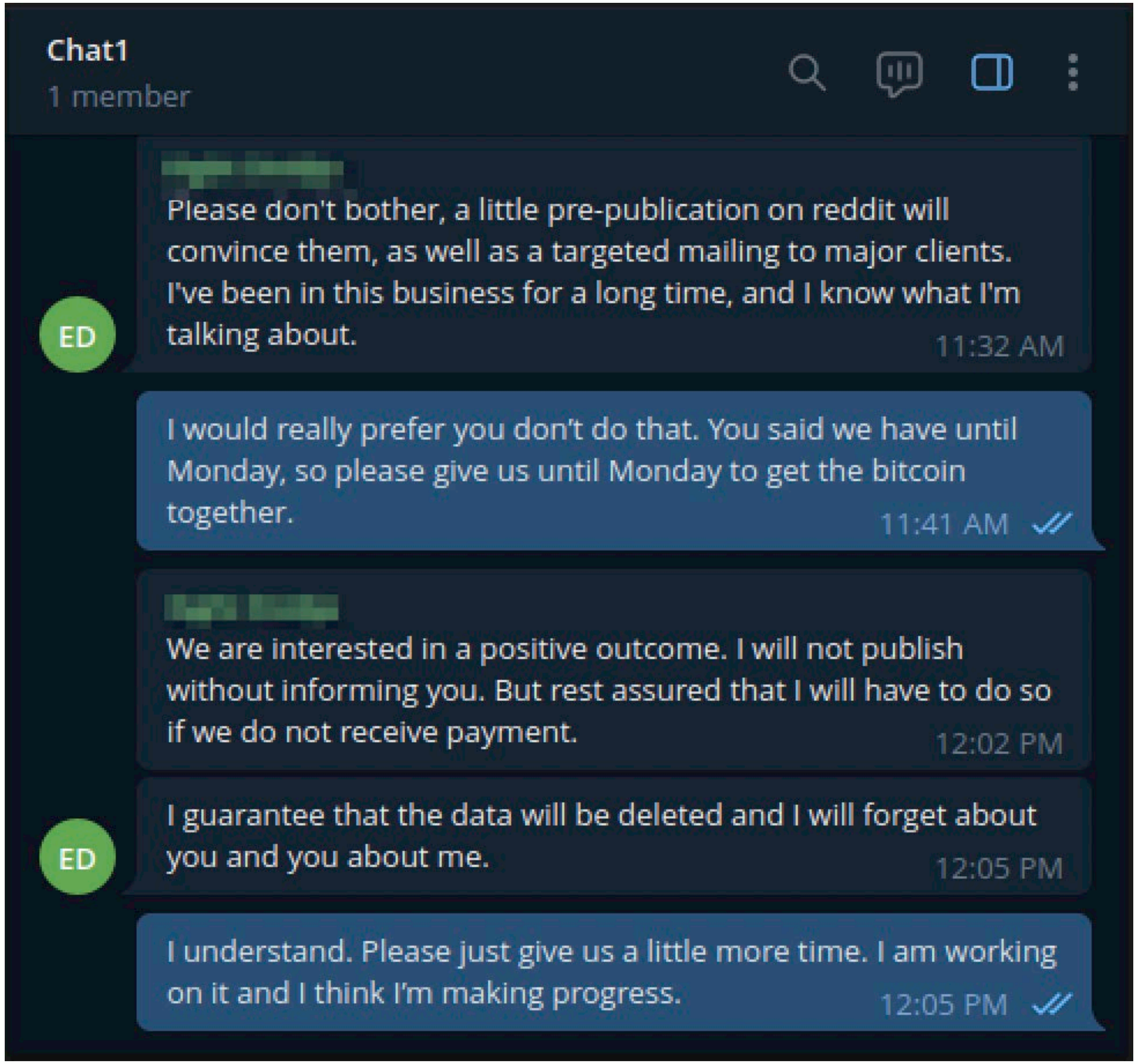


**SUPPORT** 2023-02-21 13:21:58

Welcome to the Quantum secure chat.
Please, specify the name of the company and your position.
Our support team will be in touch as soon as possible.
This chat is the only legimate channel of communication with us.
All other channels like emails, chat rooms under the different URLs etc. - are scam and will lead your company to the money loss and data publication.

GUIDEPOINT SECURITY

# Telegram Chat (Suspected Bianlian Affiliate)



Chat1

1 member

[redacted]

ED: Please don't bother, a little pre-publication on reddit will convince them, as well as a targeted mailing to major clients. I've been in this business for a long time, and I know what I'm talking about. 11:32 AM

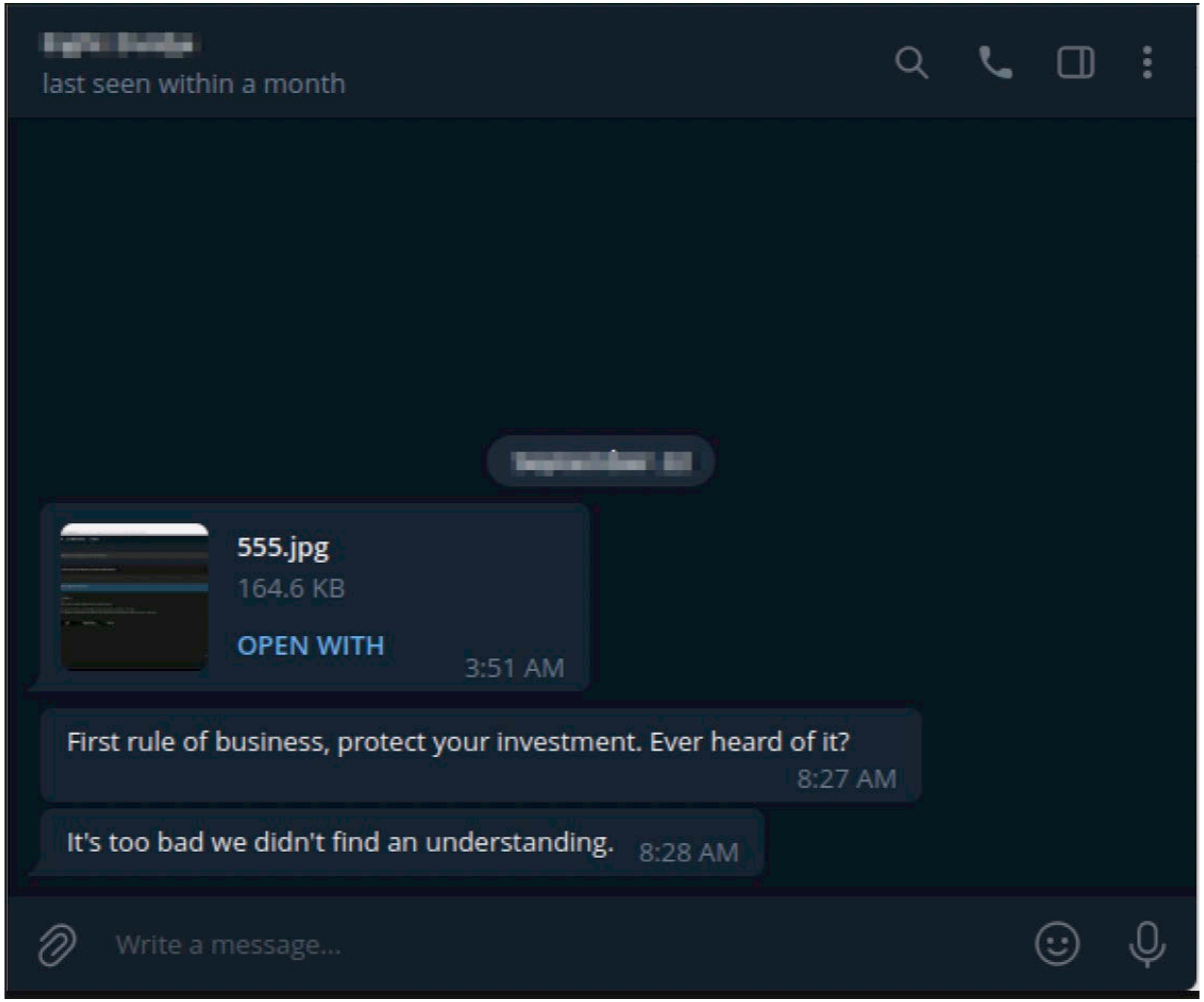
I would really prefer you don't do that. You said we have until Monday, so please give us until Monday to get the bitcoin together. 11:41 AM

[redacted]

We are interested in a positive outcome. I will not publish without informing you. But rest assured that I will have to do so if we do not receive payment. 12:02 PM

ED: I guarantee that the data will be deleted and I will forget about you and you about me. 12:05 PM

I understand. Please just give us a little more time. I am working on it and I think I'm making progress. 12:05 PM



[redacted]

last seen within a month

[redacted]

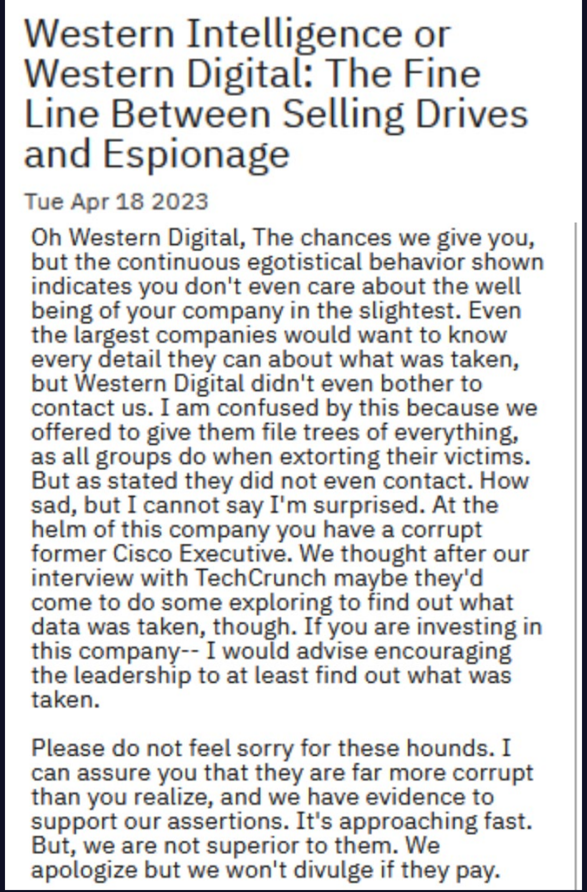
555.jpg
164.6 KB
OPEN WITH 3:51 AM

First rule of business, protect your investment. Ever heard of it? 8:27 AM

It's too bad we didn't find an understanding. 8:28 AM

GUIDEPOINT SECURITY

# Continued Escalation of Coercive Tactics - AlphV

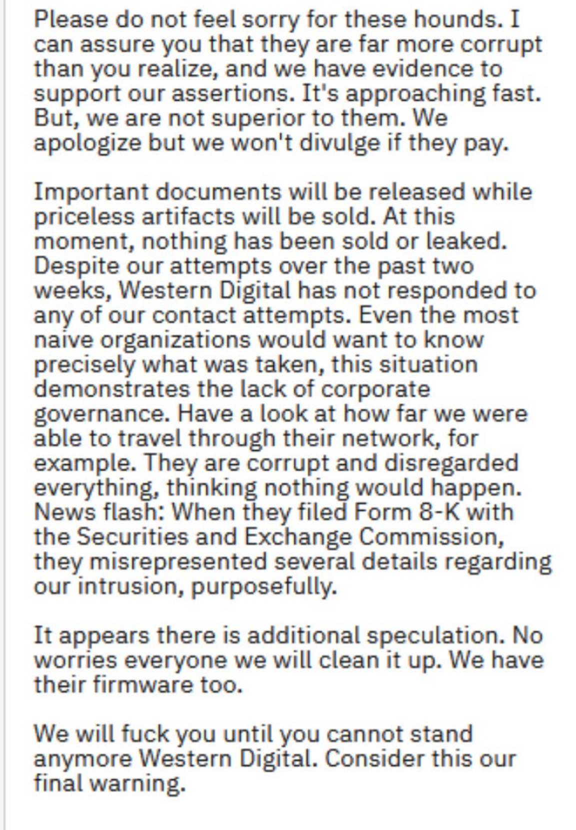


## Western Intelligence or Western Digital: The Fine Line Between Selling Drives and Espionage

Tue Apr 18 2023

Oh Western Digital, The chances we give you, but the continuous egotistical behavior shown indicates you don't even care about the well being of your company in the slightest. Even the largest companies would want to know every detail they can about what was taken, but Western Digital didn't even bother to contact us. I am confused by this because we offered to give them file trees of everything, as all groups do when extorting their victims. But as stated they did not even contact. How sad, but I cannot say I'm surprised. At the helm of this company you have a corrupt former Cisco Executive. We thought after our interview with TechCrunch maybe they'd come to do some exploring to find out what data was taken, though. If you are investing in this company-- I would advise encouraging the leadership to at least find out what was taken.

Please do not feel sorry for these hounds. I can assure you that they are far more corrupt than you realize, and we have evidence to support our assertions. It's approaching fast. But, we are not superior to them. We apologize but we won't divulge if they pay.

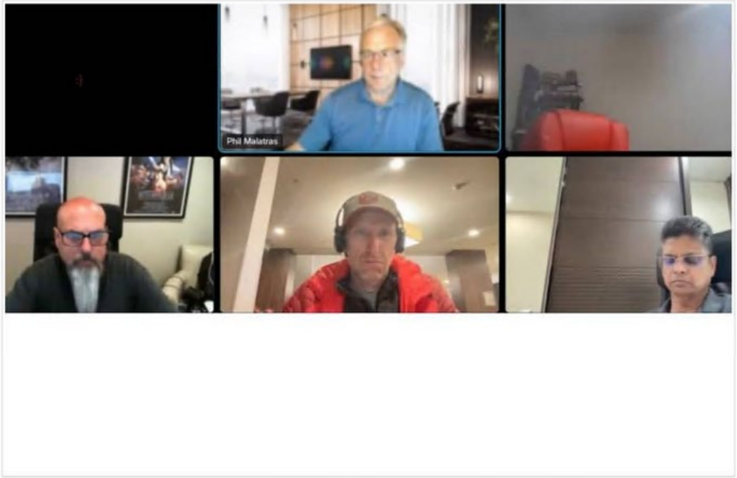


Please do not feel sorry for these hounds. I can assure you that they are far more corrupt than you realize, and we have evidence to support our assertions. It's approaching fast. But, we are not superior to them. We apologize but we won't divulge if they pay.

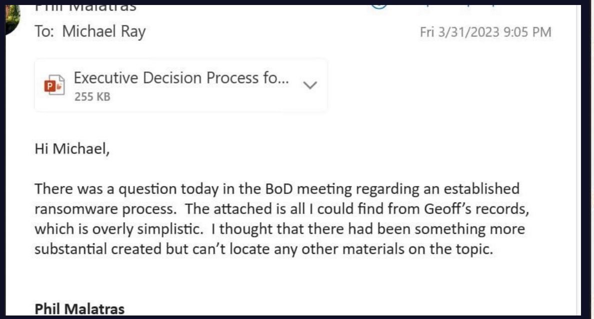
Important documents will be released while priceless artifacts will be sold. At this moment, nothing has been sold or leaked. Despite our attempts over the past two weeks, Western Digital has not responded to any of our contact attempts. Even the most naive organizations would want to know precisely what was taken, this situation demonstrates the lack of corporate governance. Have a look at how far we were able to travel through their network, for example. They are corrupt and disregarded everything, thinking nothing would happen. News flash: When they filed Form 8-K with the Securities and Exchange Commission, they misrepresented several details regarding our intrusion, purposefully.

It appears there is additional speculation. No worries everyone we will clean it up. We have their firmware too.

We will fuck you until you cannot stand anymore Western Digital. Consider this our final warning.



An early morning session with the finest threat hunters Western Digital has to offer.



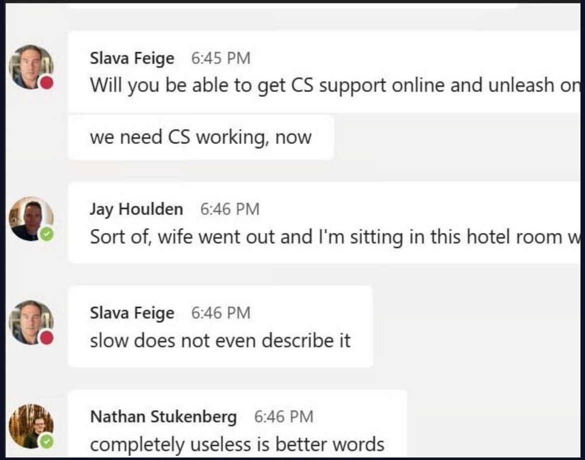
Phil Malatras
To: Michael Ray
Fri 3/31/2023 9:05 PM

Executive Decision Process fo...
255 KB

Hi Michael,

There was a question today in the BoD meeting regarding an established ransomware process. The attached is all I could find from Geoff's records, which is overly simplistic. I thought that there had been something more substantial created but can't locate any other materials on the topic.

**Phil Malatras**



**Slava Feige** 6:45 PM
Will you be able to get CS support online and unleash on

we need CS working, now

**Jay Houlden** 6:46 PM
Sort of, wife went out and I'm sitting in this hotel room w

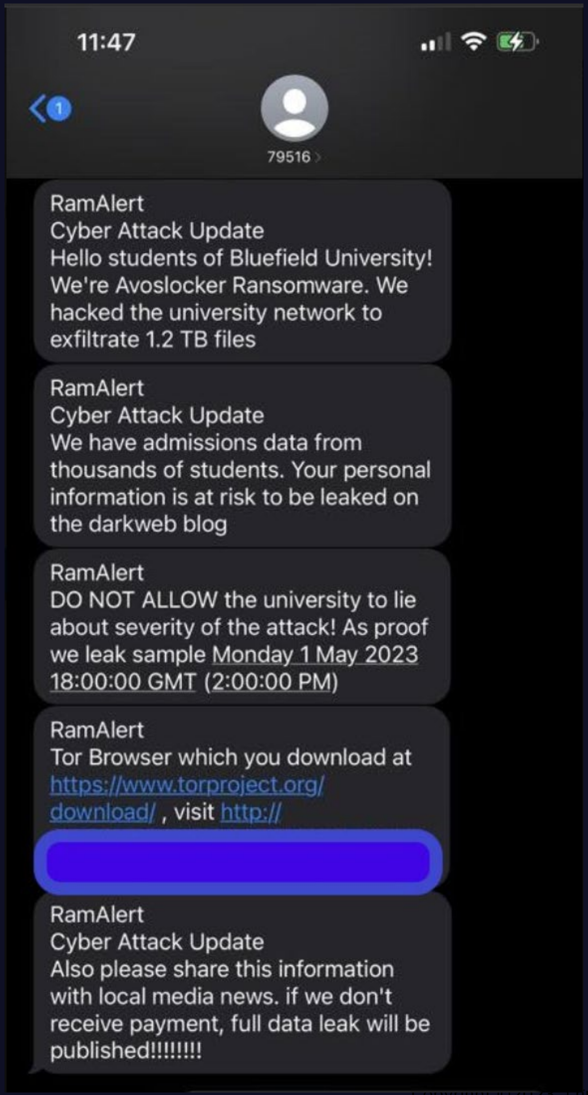
**Slava Feige** 6:46 PM
slow does not even describe it

**Nathan Stukenberg** 6:46 PM
completely useless is better words

# Continued Escalation of Coercive Tactics - Avoslocker

- Bluefield University compromised by Avoslocker
- TA contacted students via emergency alert system
- https://www.wvva.com/2023/05/01/ransomware-cyberattack-continues-bluefield-university/

BLUEFIELD
UNIVERSITY



RamAlert
Cyber Attack Update
Hello students of Bluefield University! We're Avoslocker Ransomware. We hacked the university network to exfiltrate 1.2 TB files

RamAlert
Cyber Attack Update
We have admissions data from thousands of students. Your personal information is at risk to be leaked on the darkweb blog

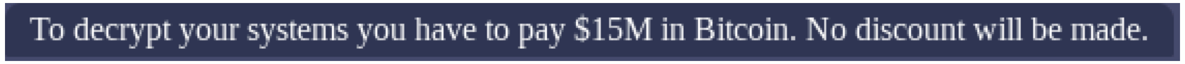
RamAlert
DO NOT ALLOW the university to lie about severity of the attack! As proof we leak sample Monday 1 May 2023 18:00:00 GMT (2:00:00 PM)

RamAlert
Tor Browser which you download at https://www.torproject.org/download/ , visit http://

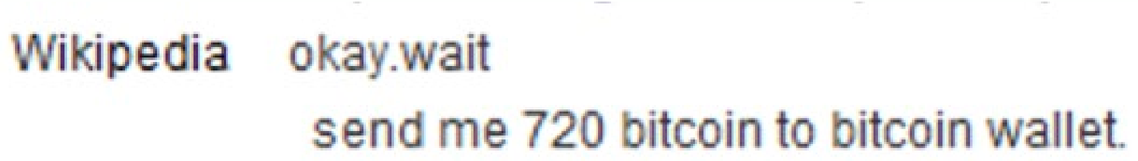
[redacted]

RamAlert
Cyber Attack Update
Also please share this information with local media news. if we don't receive payment, full data leak will be published!!!!!!!!

# Decryption Process

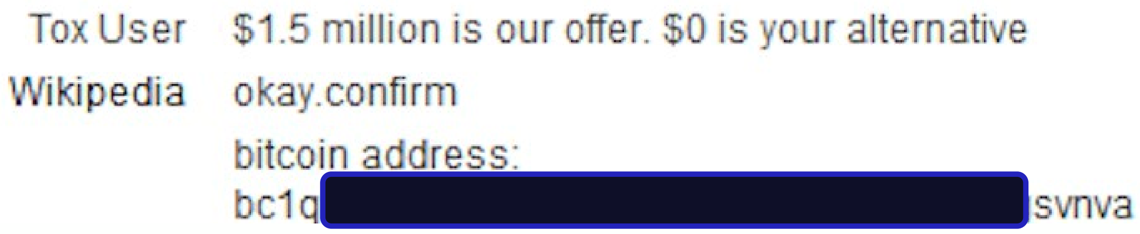


To decrypt your systems you have to pay $15M in Bitcoin. No discount will be made.



Wikipedia okay.wait

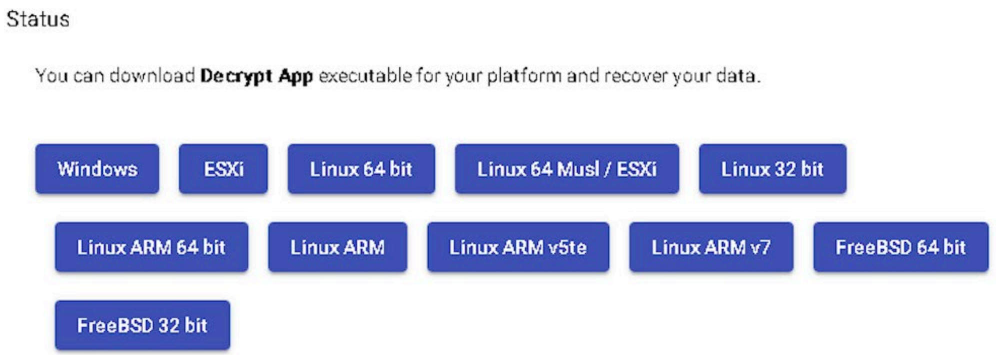
send me 720 bitcoin to bitcoin wallet.



Tox User $1.5 million is our offer. $0 is your alternative

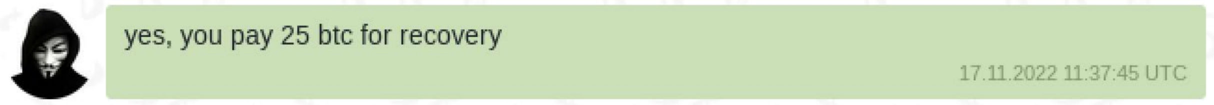
Wikipedia okay.confirm

bitcoin address:
bc1q[redacted]svnva



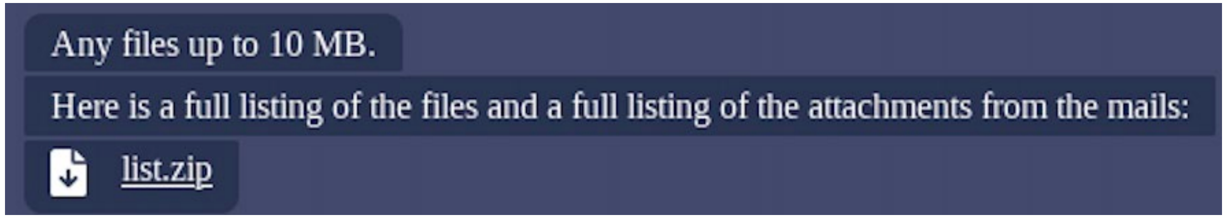
Status

You can download **Decrypt App** executable for your platform and recover your data.



yes, you pay 25 btc for recovery

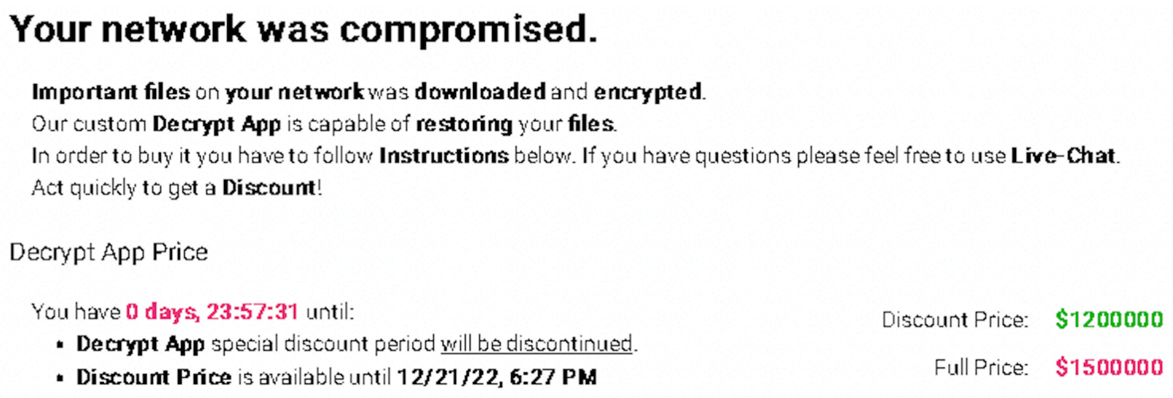
17.11.2022 11:37:45 UTC



Any files up to 10 MB.

Here is a full listing of the files and a full listing of the attachments from the mails:

list.zip



## Your network was compromised.

**Important files** on **your network** was **downloaded** and **encrypted**.
Our custom **Decrypt App** is capable of **restoring** your **files**.
In order to buy it you have to follow **Instructions** below. If you have questions please feel free to use **Live-Chat**.
Act quickly to get a **Discount**!

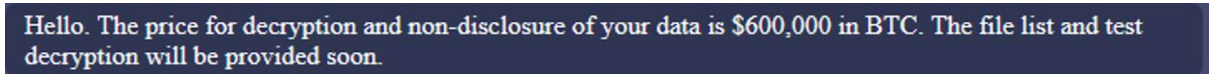
Decrypt App Price

You have **0 days, 23:57:31** until:

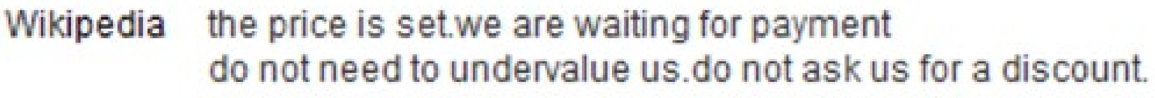
- **Decrypt App** special discount period will be discontinued.
- **Discount Price** is available until **12/21/22, 6:27 PM**

Discount Price: **$1200000**

Full Price: **$1500000**



Hello. The price for decryption and non-disclosure of your data is $600,000 in BTC. The file list and test decryption will be provided soon.



Wikipedia the price is set.we are waiting for payment
do not need to undervalue us.do not ask us for a discount.

# AlphV Ransomware Investigation

## Sector: Oil and Gas
## Ransomware Group: AlphV

- Encrypted Systems:
  - Servers
  - Workstations
  - Hyper-V Servers (Virtualization Platform)
  - NAS
- Exfiltrated Data: 1.4 TB
  - Employee Sensitive Data
  - Client Contracts and Proprietary Information
  - HR Documentation
- Ransom Payment:
  - $850K
  - Removal from Leak Site
  - Proof of Deletion
  - No DDoS
- Downtime
  - Not Able to Operate: 3 days
  - Limited operations: 21 days

GUIDEPOINT
SECURITY

THREAT DETAILS

# Key Takeaways

- Initial Access: Compromised Credentials Used to Access VPN (No MFA in place)
    - Credentials belonged to a Network Administrator
    - Escalated to the domain admin account (Mimikatz)
- Post Exploitation Framework: Cobalt Strike
- PowerShell used to disable Windows Defender via Registry
- SCCM Server used to deploy ransomware
- Exfiltration Tools: PowerShell (Collection), 7za (staging), and Proprietary Tool (Exfil)

# The Upsides Despite the Doom and Gloom

- Focusing on cyber security fundamentals mitigates many exploitation scenarios commonly used by ransomware threat groups
- Threat intelligence teams bridge the gap between emerging attacker trends and detection/prevention capabilities
- Having knowledge of assets, applications, and emerging vulnerabilities helps to keep your attack surface as resilient and protected as possible
- Having a plan for ransomware that covers administrative and technical response measures ensures you’re prepared to respond if necessary

GUIDEPOINT SECURITY

THREAT DETAILS

# Key Information

- Initial Impact commonly bad hygiene or user practices; also vulnerabilities
- For Ransomware, number of encrypted systems does not determine scale of the incident
  - Removal of encrypted systems and restoration from backups does not mean you’re safe
  - Most recent engagements also include Data Loss, Publicly disclosed if unpaid
- Living off the LAN and Persistence
- Need to determine root cause and identify persistence mechanisms
- Incidents are High Impact

INSIGHTS FROM THE FIELD

# Focus Areas

- At least have the Basics
- Includes People, Process, and Technology
- Most Impactful Areas and Solutions
  - Multi-Factor Authentication (Remote and Privileged Access)
  - Endpoint Detection and Response (EDR)
  - Privileged Account Management (PAM)
  - Centralized Logging (SIEM)
  - Vetted Backup Solution
  - Updated Incident Response Plan
  - Threat-specific Playbooks (Ransomware, BEC)
  - Periodic IR Tabletop Exercises (Technical, Executive)
  - User Awareness Training/Testing

# Know the Roles

## Incident Response

- Role: IR Service Provider
- Responsibilities:
  - Response Methodology
  - Incident Investigation
  - Actor Awareness
  - 24/7 Threat Monitoring
  - Root Cause Analysis
  - Remediation Strategy
  - Negotiation/Brokerage

## Cyber Insurance

- Roles: Insurance Carrier, Claims Adjuster
- Responsibilities:
  - Determine what’s covered
  - Pay the bills

## External Counsel

- Role: External Legal Counsel
- Responsibilities:
  - Receive facts from IR and counsel customer

## Other Roles:

### Recovery/Restoration

- Role: IT Assistance
- Responsibilities: Assist customer with hand-on keyboard assistance

### Breach Management

- Role: Logistical support for Impacted
- Responsibilities: Credit monitoring, Call Centers, Communications

### More…

- Data Analysis/Review, Public Relations, Breach Management Services

# Preparation is Critical

## Prepare and Practice

- IR Retainer
  - Provide SLA’s to Responses
- Incident Response Plan
  - Ensures awareness to Roles and Responsibilities
  - Establishes Incident Response process
- Playbooks & Runbooks
  - Add-On to IR Plan
  - Playbooks define workflows
  - Runbooks document tool specific procedures

- Tabletop Exercise
  - Walk Through of IR Plan
  - Find Gaps in Processes, Communication
- Purple Team Simulation
  - Live Fire of a Scenario
  - Test out Controls & Responses
- Readiness Assessments
  - General or Threat specific
  - Review Detection, Containment, and Remediation action

GUIDEPOINT
SECURITY

QUESTIONS?

# Thank You!

IR@guidepointsecurity.com