



NEGOTIATING RANSOMWARE

Michael Sjøberg, Chief Hostage Negotiator

ABOUT US

- RANSOMWARE NEGOTIATIONS (120+ CASES & COUNTING)
- ACADEMIC & POLICE/MILITARY INTELLIGENCE BACKGROUNDS
- CRISIS EXERCISES, OPERATIONAL CRISIS PLANS, 24/7 RESPONSE





The background of the slide is a black and white photograph. In the center, there is a dark silhouette of a person's head and shoulders, facing away from the camera. In the background, out of focus, are city lights and buildings, suggesting an urban setting at night or dusk.

RANSOMWARE
IS NOT
A CRISIS OF IT!





DELTA CRISIS MANAGEMENT

akira_readme - Notepad

File Edit Format View Help

Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidentally corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - <https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion>.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - <https://www.torproject.org/download/>.
2. Paste this link - <https://akiralkzxxzq2dsrzsrivr2xgbbu2wgsxmryd4csgfameg52n7efvr2id.onion>.
3. Use this code - [REDACTED] - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

CRISIS TRACKS

TECHNICAL

CONTAINMENT
RECOVERY
FORENSICS

COMMS

MEDIA & PRESS
CUSTOMERS
EMPLOYEES

LEGAL

DATA PROTECTION
POLICE
INSURANCE
LAWSUITS

NEGOTIATE

INTELLIGENCE
RISK MITIGATION
DECRYPTION

The background of the slide is a black and white photograph. In the center, there is a dark silhouette of a person's head and shoulders, facing away from the camera. In the background, out of focus, are city lights and buildings, suggesting an urban setting at night or dusk.

NEGOTIATING
DOES **NOT** EQUAL PAYMENT

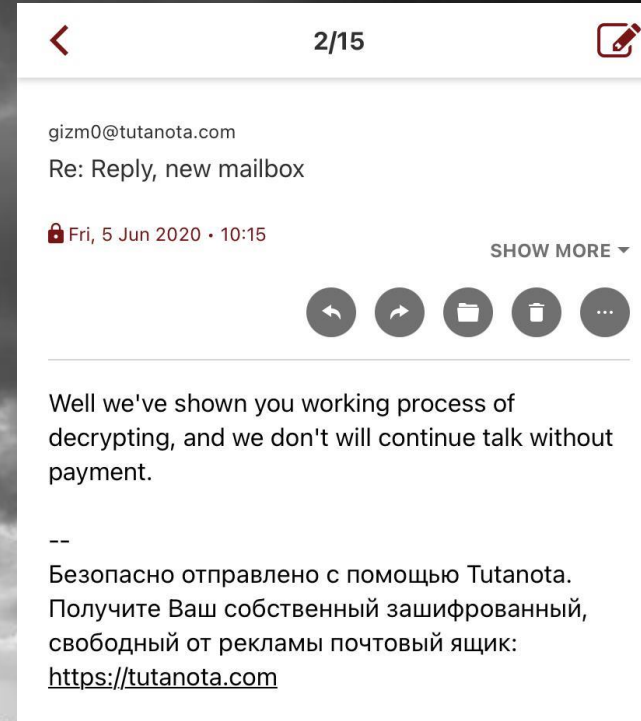


PERPETRATORS

Friday, 25 December 2020, 17.00

You will have nothing. Merry Christmas.

Sent with [ProtonMail](#) Secure Email.



In Monday we start to find customer to your data,
and price will be doubled, stop fuck my brain

09.09.2022 15:15:16 UTC

Hello Peter,
Yes, I don't have any of your files. The threat to leak them to to various data leak sites was a bluff.
But I guarantee that all .aes files can be decrypted.

I can also assist you in recovering lost files if it's possible.

To know if it's possible may I know some details of what happened during the shutdown?:

- 1) How this files looks now? Did they just disappear?
- 2) What exactly was the problem with the file server?
- 3) Do you use your own server or rent someone's server?
- 4) Were the files on HDDs or SSDs?
- 5) What operating system is currently used to access the files?

Please answer these questions as soon as possible, as the possibility of recovery may depend on it.

Best Regards,
N

AKIRA

/sign_out

You

> Hello, I have read your note and I would like to find out if we can find a way to get your assistance. Is it safe to talk here? Best regards Peter

We

> Hello. You've reached Akira support chat. Currently, we are preparing the list of data we took from your network. For now you have to know that dealing with us is the best possible way to settle this quick and cheap. Keep in touch and be patient with us. Do you have a permission to conduct a negotiation on behalf of your organization? Once we get a response you will be provided with all the details.

You

> I don't know how to come up with more money for the wallet. I am sorry.
> It has been the worst weekend ever. Ever. I feel like I am the only one still fighting for this to succeed. All by myself. Even the few people earlier with me seem like they have just given up. I am abandoned by everyone. It is no fun. If something is to happen I have to do it myself, so I have decided to sell my car - just to get a little more for you. We shall see. You need to help me. Please. Lars

We

> I don't know how to help you. You have the amount you need to reach.

You

> But how am I to do this?

We


> Lars, are you here?

You

> Thank you so much. You have helped me a lot, I really, really appreciate it. Personally I think you saved me my job. I have never met people like that before, it is true generosity. Thanks. I wondered: what could happen with the data? Will you delete it? Please. I assure you that we will talk to absolutely noone about this (unless of course you ask me to). Br Lars

We

> Dear Lars, do not worry about the data. It has been deleted as we had no interest to work with it. The deal is over. We wish you all the best!

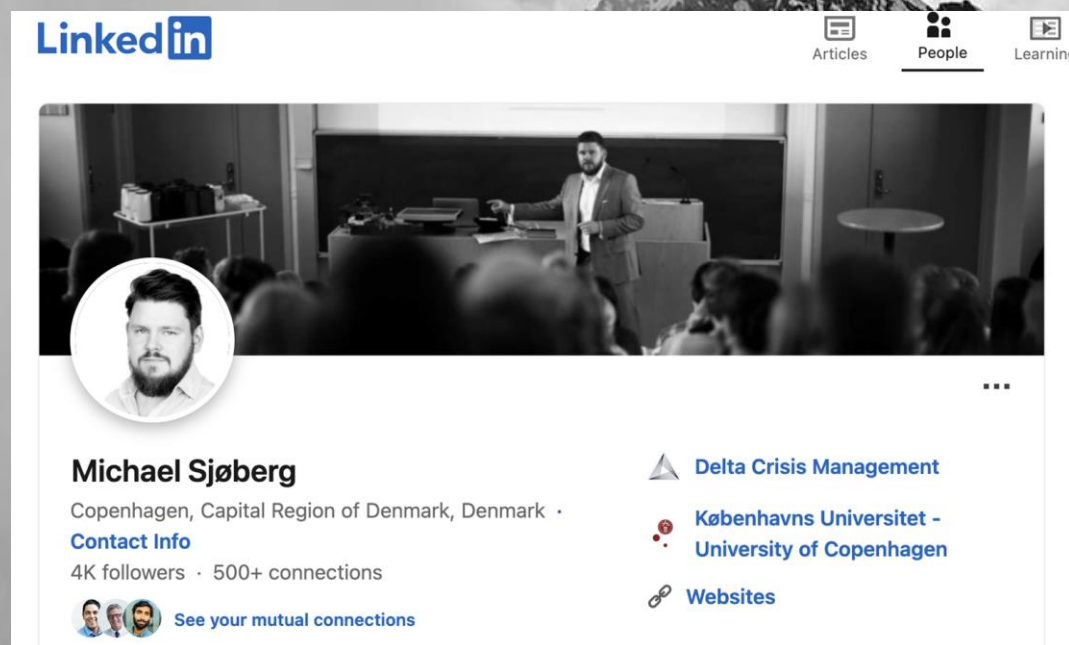
The background of the entire image is a black and white photograph. In the center, there is a dark silhouette of a person's head and shoulders, facing away from the camera. In the background, out of focus, are city lights and buildings, suggesting a night scene. The text is overlaid on this image.

DO YOU HAVE THE
TOOLS, TRAINING & HELP
THAT YOU NEED?





CONTACT



MICHAEL SJØBERG
30256474
MS@DELTACRISIS.COM

