The Art of Deal Making: Incident Response trifft Ransomware-Verhandlungen

IT-SECX 2025

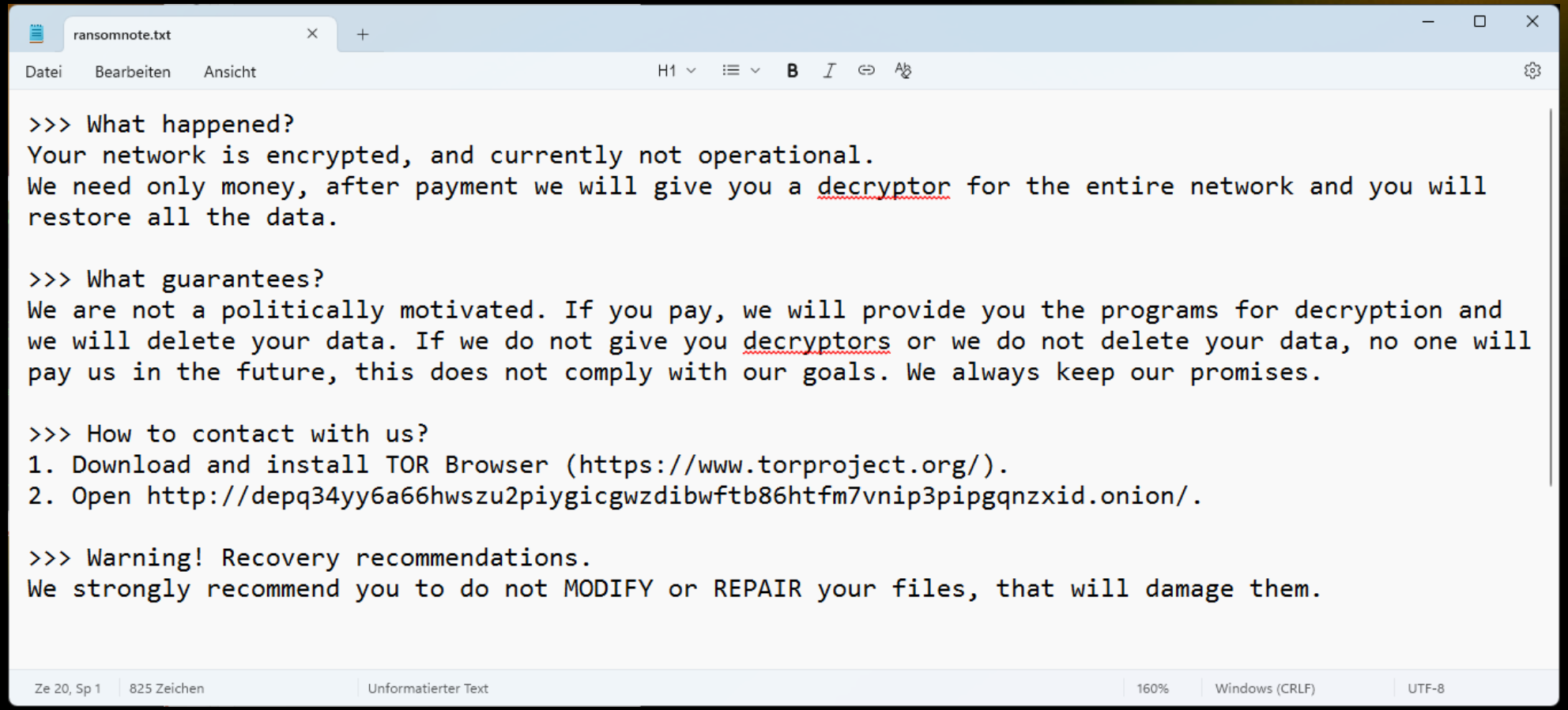
St. Pölten, am 3. Oktober 2025

“

As much as the security person inside me wants to scream “No!” the answer is a little more complex than that.

Allan Liska

Threat Intelligence Analyst at Recorded Future, author of multiple Cyber Security books


ransomnote.txt
Datei
Bearbeiten
Ansicht
H1
>>> What happened?
Your network is encrypted, and currently not operational.
We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.
>>> What guarantees?
We are not a politically motivated. If you pay, we will provide you the programs for decryption and we will delete your data. If we do not give you decryptors or we do not delete your data, no one will pay us in the future, this does not comply with our goals. We always keep our promises.
>>> How to contact with us?
1. Download and install TOR Browser (https://www.torproject.org/).
2. Open http://depq34yy6a66hwszu2piygicgwzdibwftb86htfm7vnip3pipgqnzxid.onion/.
>>> Warning! Recovery recommendations.
We strongly recommend you to do not MODIFY or REPAIR your files, that will damage them.
Ze 20, Sp 1
825 Zeichen
Unformatierter Text
160%
Windows (CRLF)
UTF-8

Was würdest Du tun?

Is anyone here? What do we have to do now?

Hello. In addition to **encrypting** your files, we also **downloaded important data** from your network. We can provide you with a **list of the files** that we took from you. You can also select any 2 files and send them to us and we will decrypt them for you. In order to **avoid disclosure** of your data on our website, get the **decrypt key** and security advice, you must **pay a ransom of $ 3,000,000.**

„Talk Money to Me”

Grundlagen der Kalkulation

- Die erste Lösegeldforderung basiert oft auf:
  - Informationen aus exfiltrierten Finanzdokumenten

    „Public information is fake, the real information is contained in your documents, I have thousands of your documents “
  - Öffentlichen Unternehmensdaten (z. B. Jahresabschluss)
  - „Zufälliger Wert“

Typische Forderungshöhe

- Faustregel: **3–5 % des Jahresumsatzes**
- Forderung kann deutlich darüber oder darunter liegen

Einflussfaktoren

- Bekannt gewordene **Cyber-Versicherungssummen**
- **Globale Umsatzzahlen** oder **Nettoergebnis**

This is a fair price for a company like yours.

You’re a filthy liar, your net profit per month is $3-4 million dollars, that’s just the information I could find now in one of your documents.

We do not ask for what you cannot afford. So, we've gone through your files to define your financial abilities. We've been looking through your bank statements, net income, cyber liability limits, financial audits.

Beispiele Lösegeldforderung

We don't have access to $500,000 today, tomorrow, next week, or any time. We are trying to giving you our best offer that we can here, because anything higher is impossible for us to pay you.

25/08/2021, 16:13:12

Do you remember that we've had access to your network and went through your financial data? We wouldn't ask for anything you are unable to afford.

25/08/2021, 17:18:1

Yes, but if you saw our expenses you would see that our margins are extremely slim. Our industry relies on being the most affordable option, which means accepting slim margins to get work. Revenue may look good, but when we realize only 2% to 4%, you start to see that we are not extremely profitable

https://www.ransomware.live/nego/Conti/20210820

Support: According to the public records your revenue is [more than 30],000,000$, so this price is reasonable. https://www.dnb.com/business-directory/company-profiles.[redacted].html

Also you should remember that the price is much cheaper then you will pay lawsuits, that your clients will send you and government fines, because you have lost so much of their data.

1/8/2021, 5:37:26 PM

[redacted]: We would like to fix this problem but we have been out of service during Covid and do not have this amount o fix and please let me know what we

https://www.ransomware.live/nego/Conti/20210107

I'll talk to the team anyways, will try to get smth better but not sure if my boss agrees.

25/08/2021, 17:26:01

Thank you. I know you guys are looking to make money off of us, but we just want to be realistic with you here regarding what we can actually pay.

25/08/2021, 17:30:23

350k$ today

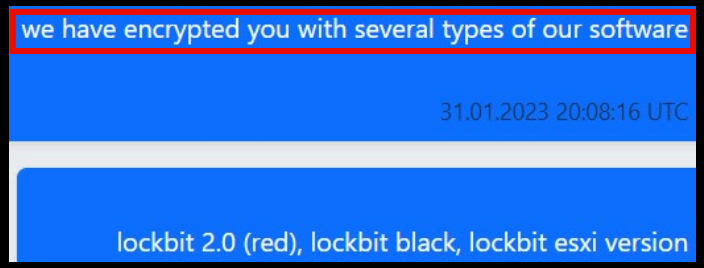
25/08/2021, 17:59:48

Okay, we are working on this

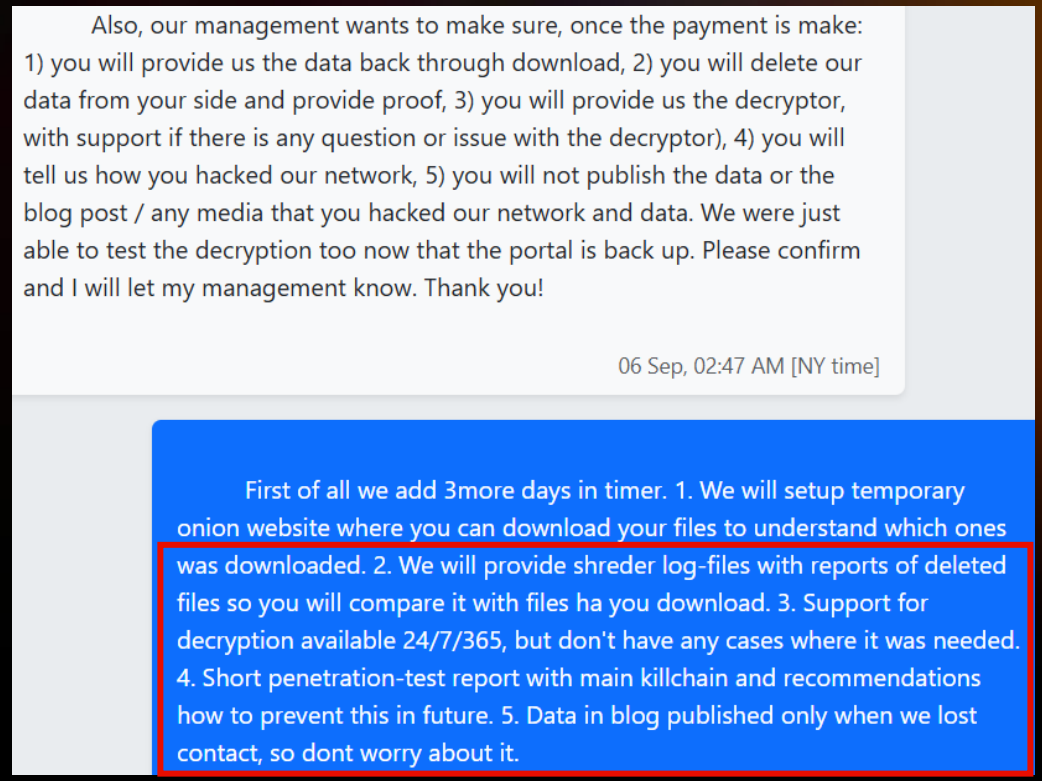
https://www.ransomware.live/nego/Conti/20210820

Zusicherungen der Angreifergruppen

- Bereitstellen des Decryptors zur Entschlüsselung
  - Achtung: Vorher „absichern", dass es der gleiche Decryptor für alle Dateien ist! (Gefahr von **Re-Extortion**)
- Keine Veröffentlichung bzw. kein Verkauf der exfiltrierten Daten
- Pentesting Report bzw. initiale Zugriffsvektor
  - Meist nur allgemein / fehlende Qualität
- Proof of Deletion
- „optional": Support bei der Wiederherstellung



https://www.ransomware.live/nego/lockbit3.0/myerspower_com



https://www.ransomware.live/nego/BlackMatter/20210829

Einschüchterung als Bestandteil der Taktik

- Angreifergruppen kontaktieren gezielt Personen im Unternehmen oder Kunden/Lieferanten
  - Ziel: psychologischen Druck aufbauen, Angst erzeugen, schnelle Zahlung erzwingen

Die Uhr tickt: Zeitdruck als Teil der Erpressung

https://www.the74million.org/wp-content/uploads/2023/03/minnesota-schools-hack-countdown_b.gif

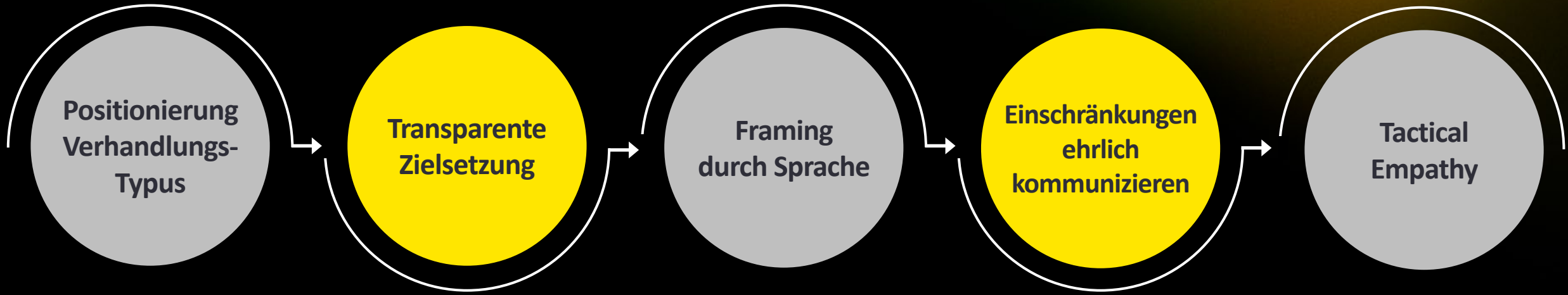
Zähe Verhandlungen? - Kann, muss aber nicht!

But we don‘t have that much money. And how can we trust you? We don‘t know that even if we pay we get what you promise us.

Check us out on the internet. We are a serious group and we respect the money of our victims. Talked to my boss: we can give you a 10% discount if you pay by tomorrow.

You have 24 hours to give us your decision regarding this deal. If you stay silent, we will announce the breach on our blog.

Taktiken & Sprache



Festlegen, welche „Rolle" eingenommen wird:

- *Der/Die informierte Profi*
- *Der/Die persönliche Stratege/Strategin*
- *Der/Die naive Vermittler/Vermittlerin*

Relevant, je nach Größe/Professionalität der Angreifergruppen

Von Anfang an klare Ziele festsetzen und kommunizieren.

„Our goal is to resolve this with minimal damage to both sides."

„we", „together", „resolve", „move forward"

Vermeiden: „attack", „criminal", „ransom", „threat"

„Maybe other companies have investors to help them. We don't – so let's try to find something realistic."

Die Perspektive der Angreifergruppe verstehen, ohne sie zu rechtfertigen.

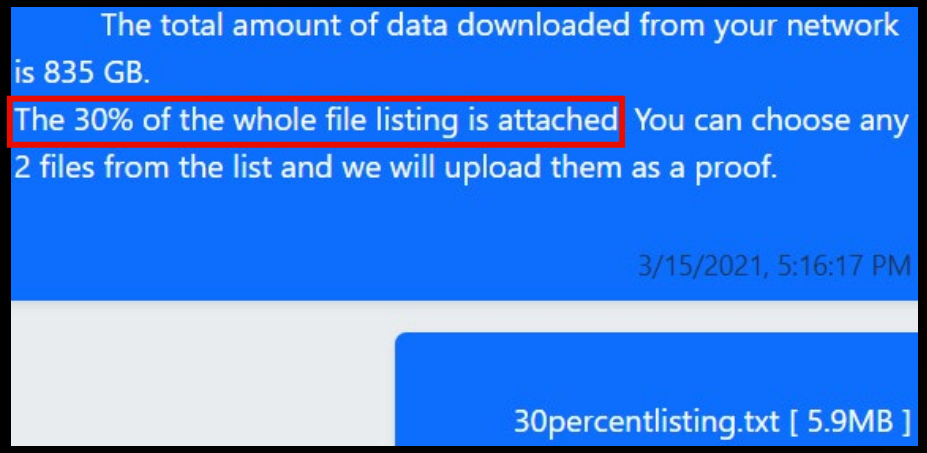
„We understand your time is valuable – we're trying to move things along, too."

„Proof of Life”: Nachweis der Exfiltration

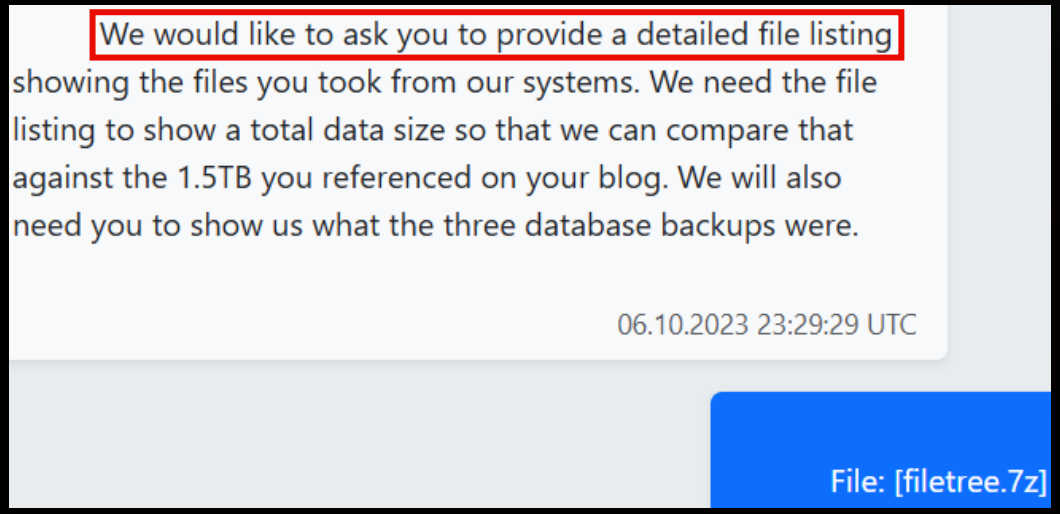
Ein File Tree dient als Nachweis des tatsächlichen Systemzugriffs und der Datenexfiltration.

Bevor überhaupt Lösegeld bezahlt wird, MUSS unbedingt verifiziert werden, ob die Entschlüsselung tatsächlich funktioniert/funktionieren würde!

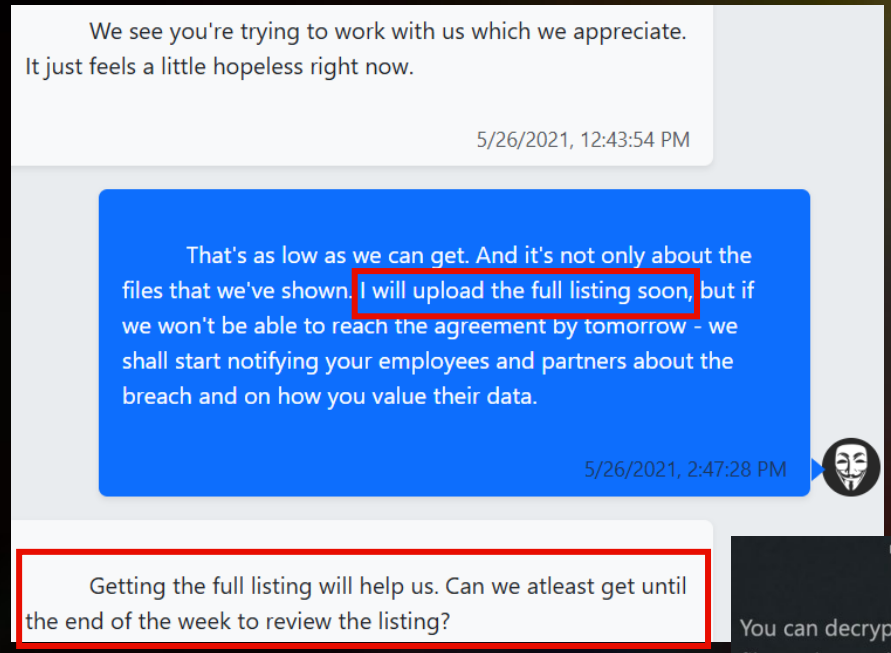
Beispiele File Tree



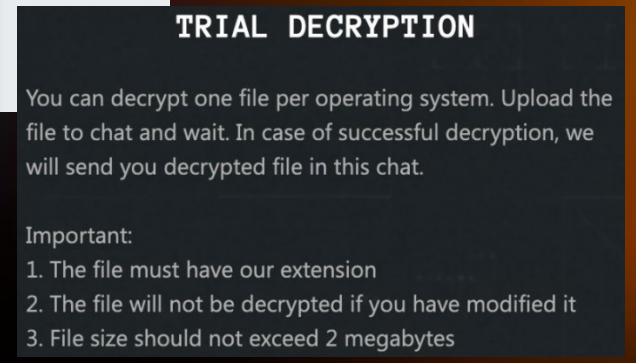
https://www.ransomware.live/nego/Conti/20210315

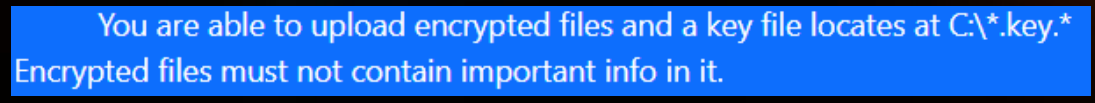


https://www.ransomware.live/nego/lockbit3.0/sirva_com

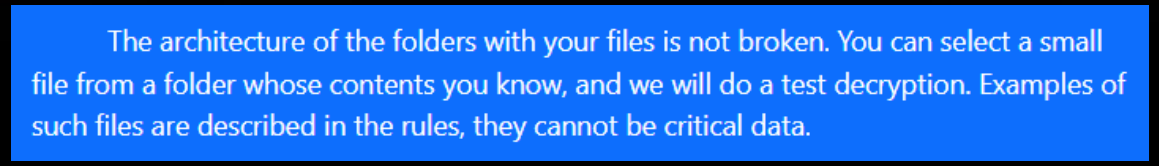


https://www.ransomware.live/nego/Conti/20211205t





https://www.ransomware.live/nego/Hive/20211004



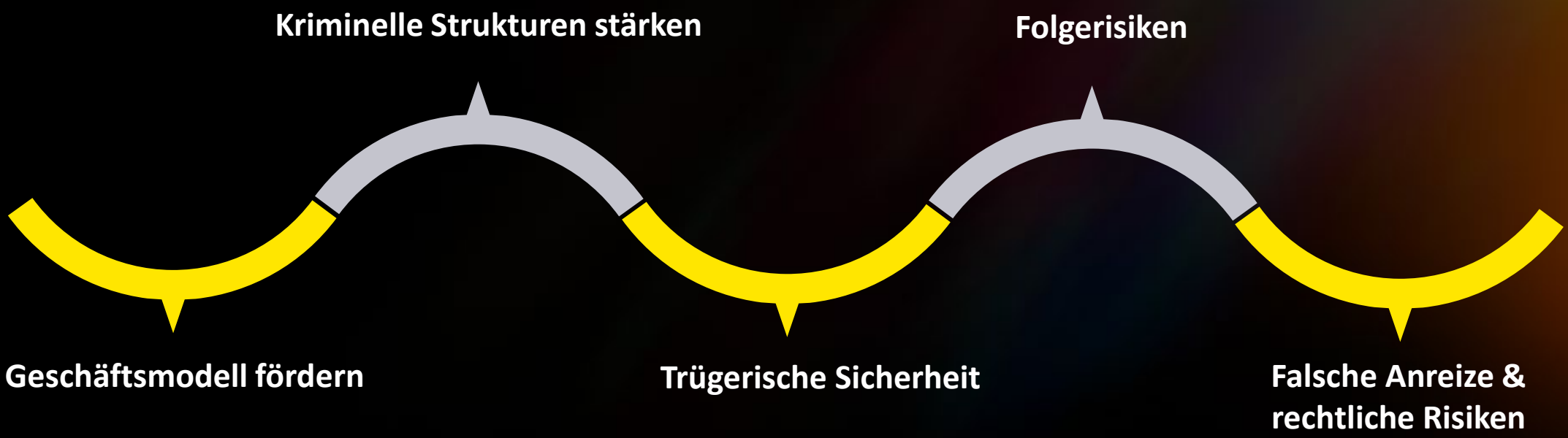
https://www.ransomware.live/nego/Dragonforce/C7CD31EAAF9DE9AC

Wenn doch gezahlt wird

The leadership has decided to accept $500,000 and let you be. Here is our BTC wallet [redacted]. Let us know when you are ready to make payment.

We are ready to send the Bitcoin. We have the loan from the bank. Are you online and ready to receive.

Aspekte wenn gezahlt wird



Do’s

- ✓ Preisangebot der Angreifergruppe abwarten
  (wenn nicht schon bekannt)
- ✓ Immer respektvoll und professionell kommunizieren
- ✓ Motivation/Lage der Angreifergruppe nachvollziehen
  (Tactical Empathy)
- ✓ Als entscheidungsfähiger Gesprächspartner auftreten
- ✓ Informationen zur Angreifergruppe einholen
- ✓ Beweise anfordern *(File Tree, Decryptor)*

Dont’s

- x Nicht im Alleingang handeln
  - Expert:innen / ggfs. Behörden hinzuziehen
- x Keine sensiblen Informationen teilen
- x Versicherungen nicht erwähnen
  - Kann den Preis signifikant erhöhen
- x Keine Drohungen oder Provokationen
  - Erschweren die Verhandlung oder führen zum Abbruch der Kommunikation

Fragen?

Consultant Forensic & Integrity Services (w/m/d)

Schwerpunkte:
Cyber Incident Response, eDiscovery

Standort: Wien
Stundenausmaß: Vollzeit, ab sofort

Christoph Wiedner
Forensic & Integrity Services

+43 664 60003 1851
christoph.wiedner@at.ey.com

Sabine Kölly
Forensic & Integrity Services

+43 664 60003 7032
sabine.koelly@at.ey.com

EY | Building a better working world

EY setzt sich für eine besser funktionierende Welt ein, indem wir neuen Wert für Kund:innen, Mitarbeitende, die Gesellschaft und den Planeten schaffen und gleichzeitig das Vertrauen in die Kapitalmärkte stärken.

Mithilfe von Daten, KI und fortschrittlicher Technologie helfen wir unseren Kund:innen, die Zukunft mit Zuversicht zu gestalten und Lösungen für die drängendsten Herausforderungen von heute und morgen zu entwickeln.

Unsere EY-Teams betreuen das volle Spektrum an Services in der Wirtschaftsprüfung, Unternehmensberatung, Steuerberatung sowie Strategie- und Transaktionsberatung. Angetrieben von branchenspezifischen Erkenntnissen, einem global vernetzten, multidisziplinären Netzwerk und vielfältigen Ökosystempartner:innen, erbringen wir Dienstleistungen in mehr als 150 Ländern und Gebieten.

Das internationale Netzwerk von EY Law, in Österreich vertreten durch die Pelzmann Gall Größ Rechtsanwälte GmbH, komplettiert mit umfassender Rechtsberatung das ganzheitliche Serviceportfolio von EY.

All in to shape the future with confidence.

SK 2510-056
ED None

ey.com/at