



Wenn nichts mehr geht- Professionelles Krisenmanagement und Lösegeldverhandlung mit Cyber-Erpressern



BISHER KEINE ERPRESSUNG

Deutschlandweite Cyberattacke auf die IHK

Nach einer Cyberattacke auf den IT-Dienstleister der IHK leiden die Kammern bundesweit unter Einschränkungen. Das Ziel des Angriffs scheint Spionage gewesen zu sein.

[Home](#) > [Cyberangriffe](#)

PRODUKTION STEHT STILL

Hipp gehackt

Der Babynahrungshersteller Hipp wurde gehackt. Ein Großteil der Mitarbeiter konnte vorerst nicht arbeiten, die Ermittlungen laufen.

[Massiver Cyberangriff auf die Caritas München und Oberbayern](#)

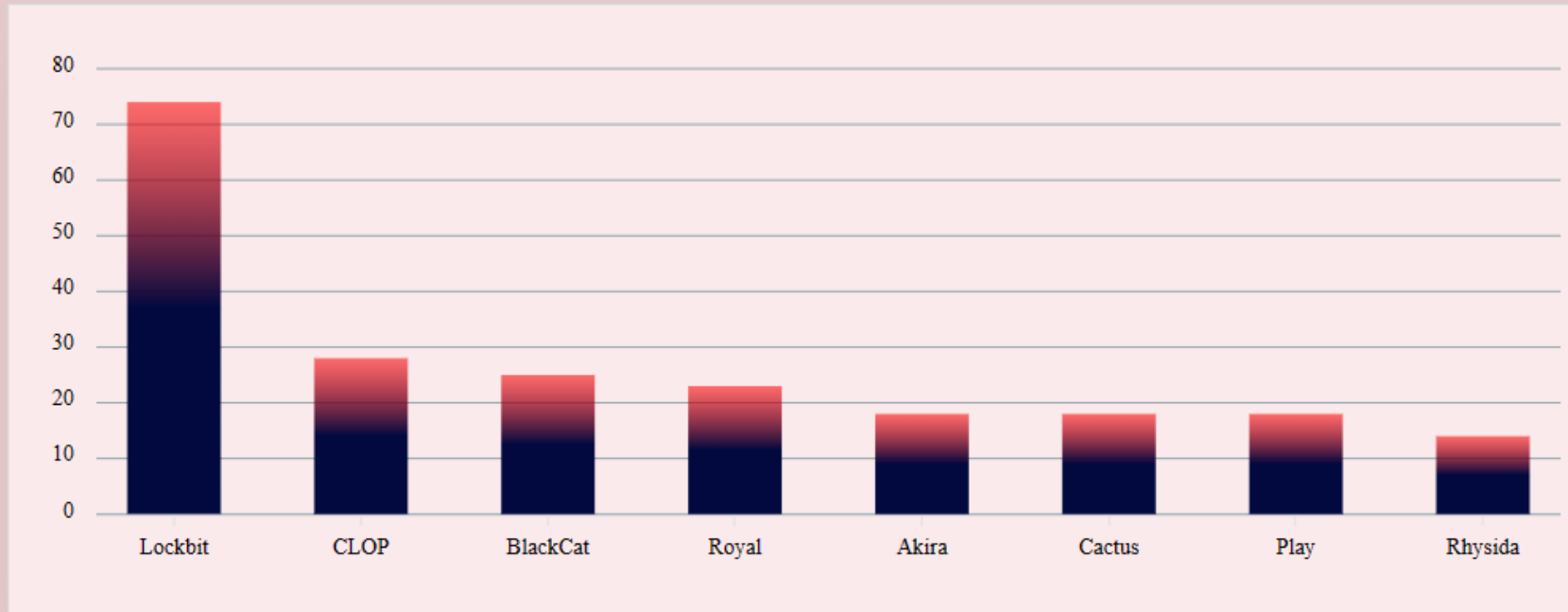
Gnadenlos: Der Cyberangriff auf die Caritas München und Oberbayern

 17. September, 2022  08:36

Total Ransomware Incidents Analyzed

8478

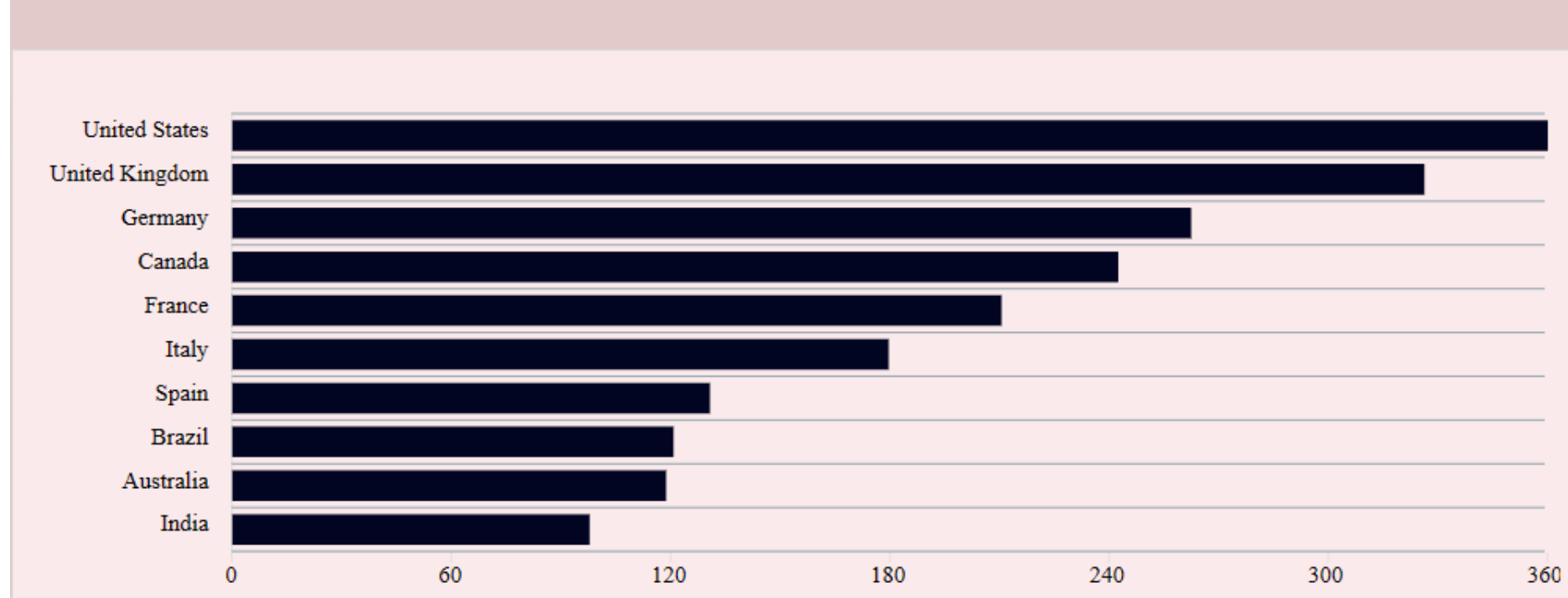
Top Group VPM - Average Victims Per Month



Total Ransomware Incidents Analyzed

8478

Top Targeted Countries



Betriebsunterbrechung
und Wiederherstellungskosten sind die
Hauptursachen für
Ransomware-Verluste

*<https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/agcs-ransomware-trends-risks-and-resilience-de.pdf>

Im Darknet: Cybercrime as a Service

The collage illustrates the 'Cybercrime as a Service' (CaaS) ecosystem in the darknet. It features four distinct screenshots:

- Rent-A-Hacker:** A website where users can hire a hacker. The profile of the hacker, 'hackrentewmxatfh.onion', describes their services and pricing.
- Dream Market:** A marketplace showing search results for 'ransomware'. The interface includes filters for shipping, escrow, category, and cryptocurrency, along with a list of search results.
- Gangst's Paradise:** A forum or marketplace listing various topics and products, including 'ANGELINA' and '+3000 SALES'.
- ChipMixer:** A website featuring a large red circular logo with a white 'C' and a red arrow, symbolizing a cycle or service.

Die 3 gängigsten Einfallstore für Cyber-Kriminelle

1

Infizierte Software eines Providers

2

Social Engineering & Phishing E-Mails

3

Fehlerhafte oder nicht installierte
Sicherheitsupdates



1

Daten inkl. BackUps wurden verschlüsselt

Entschlüsselungssoftware ist nicht bekannt. Täter fordern Lösegeld und stellen Entschlüsselung in Aussicht.

2

Daten inkl. BackUps wurden verschlüsselt und von den Servern gestohlen

Täter drohen mit Veröffentlichung und fordern Lösegeld, stellen Entschlüsselung in Aussicht. Dieses Vorgehen wird Double Extortion genannt und avanciert zum Standard-Modus-Operandi.

3

Mitarbeiter werden unter Druck gesetzt (Triple Extortion)

Die Erpresser nehmen per Email oder Messenger Verbindung mit Mitarbeitern des erpressten Unternehmens auf und konfrontieren sie mit persönlichen Daten wie z.B. Abmahnungen, Arbeitsverträgen o.ä.

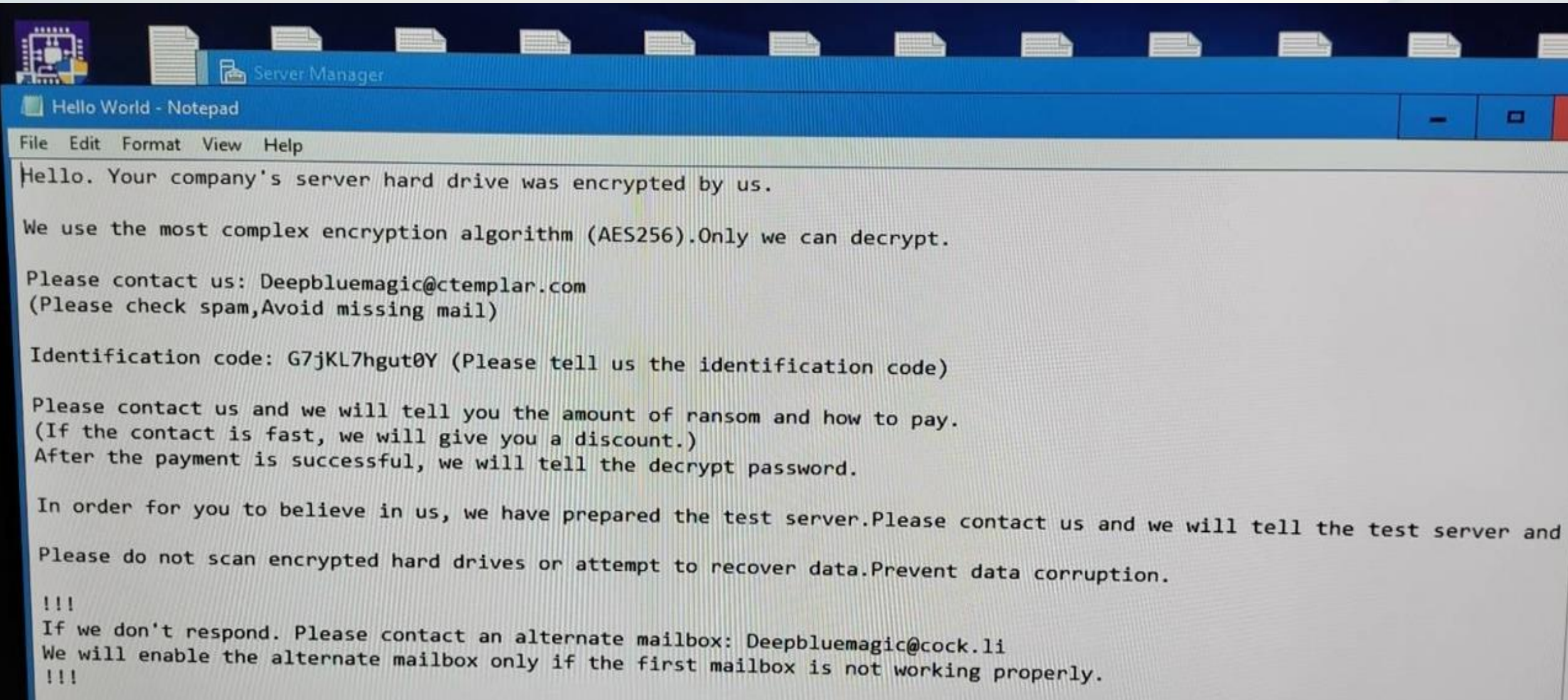
4

Daten werden zerstört, statt verschlüsselt

Dateien werden auf einen externen Server der Erpresser kopiert. Dateien auf den Servern des Unternehmens werden mit Daten aus anderen Files überschrieben und somit unbrauchbar gemacht.

Löschen statt Verschlüsselung als neueste Entwicklung.

Das Ergebnis



Cyber-Krisenstab

? Entscheidungsbefugt?

? Zusammensetzung?

? Aufgaben?

? Abläufe?

? Vorbereitet?

? Einbindung Externer?

? Durchhaltefähig?



Entscheidungsfindung im Krisenstab

1

„Die drei Optionen“

2

Was kostet mich der Ausfall meiner Systeme pro Tag?

3

Was kostet mich der Verlust der Reputation gegenüber meinen Stake Holdern?

4

Was kostet mich die Wiederherstellung der Daten bei Nicht-Zahlung?

5

Was kostet mich die Zahlung von Lösegeld inkl. Berater u. Ausfall der Systeme?

Die Rolle der Polizei

1

Anzeige möglich, aber nicht verpflichtend

2

LKA: Zahlen Sie kein Lösegeld!

3

Ermittlung der Täter vs. Abwendung des wirtschaftlichen Schadens

4

Lösegeldzahlung ist per se nicht verboten!

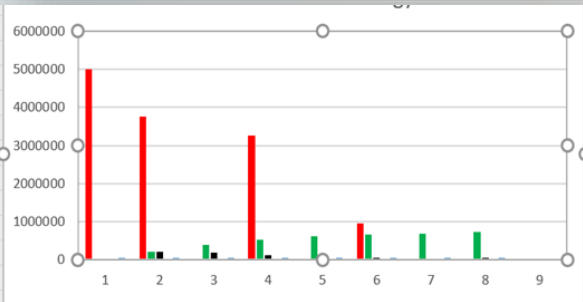
Bestandteile der Verhandlungsstrategie



Signal unsrerseits: Bereitschaft zur Zahlung

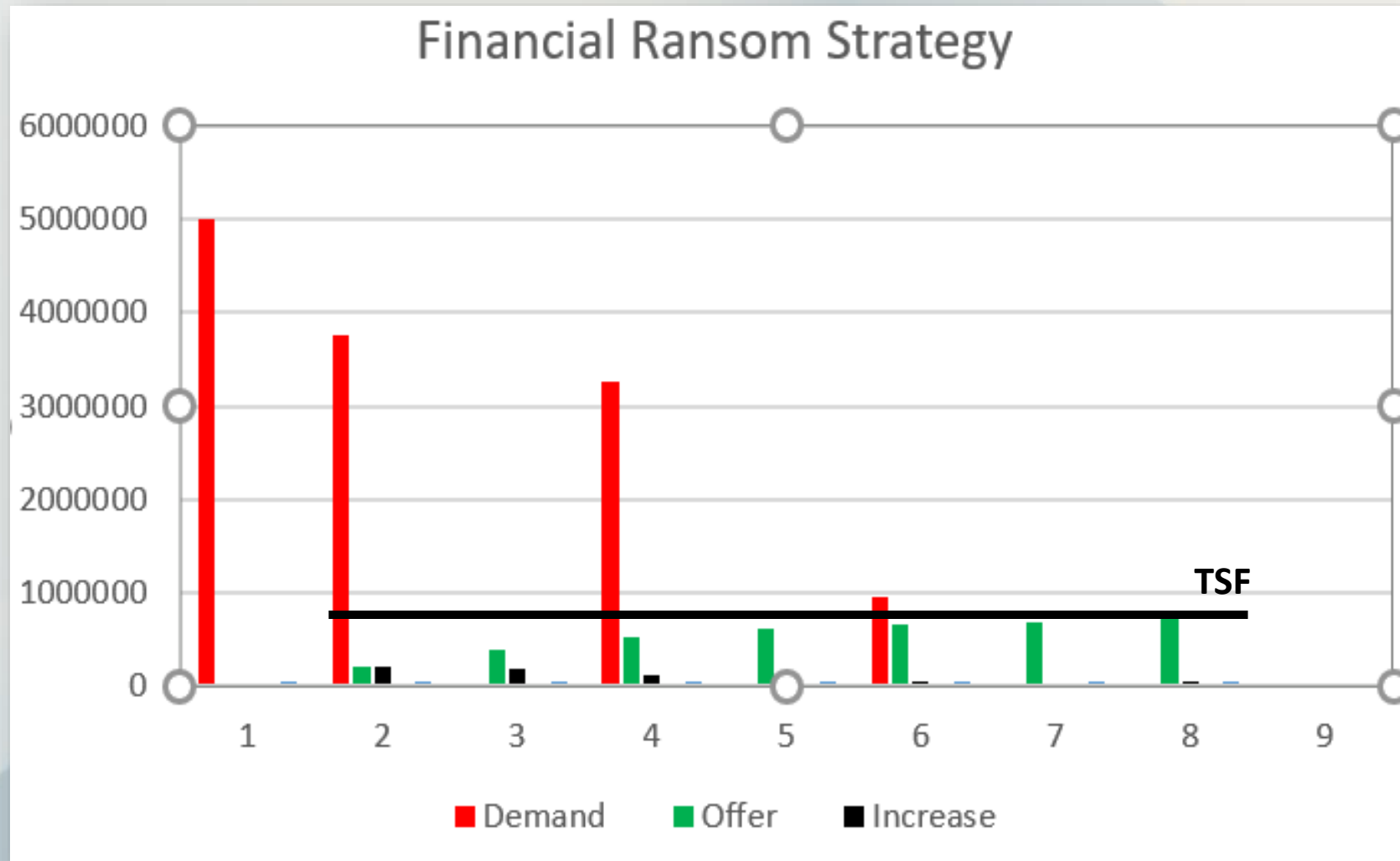


Erst kommt relativ viel, dann immer weniger



Wir orientieren uns nicht an der Forderung, sondern an dem, was wir bereit sind zu zahlen

Bestimmen der Höhe des Lösegelds



Inhalte der Verhandlung

1

Über was genau werden wir verhandeln? (Schlüssel, Security Report, Währung, keine weitere Veröffentlichung)

2

Keine Verhandlung ohne , Proof of Documents'

3

Keine Verhandlung ohne Script

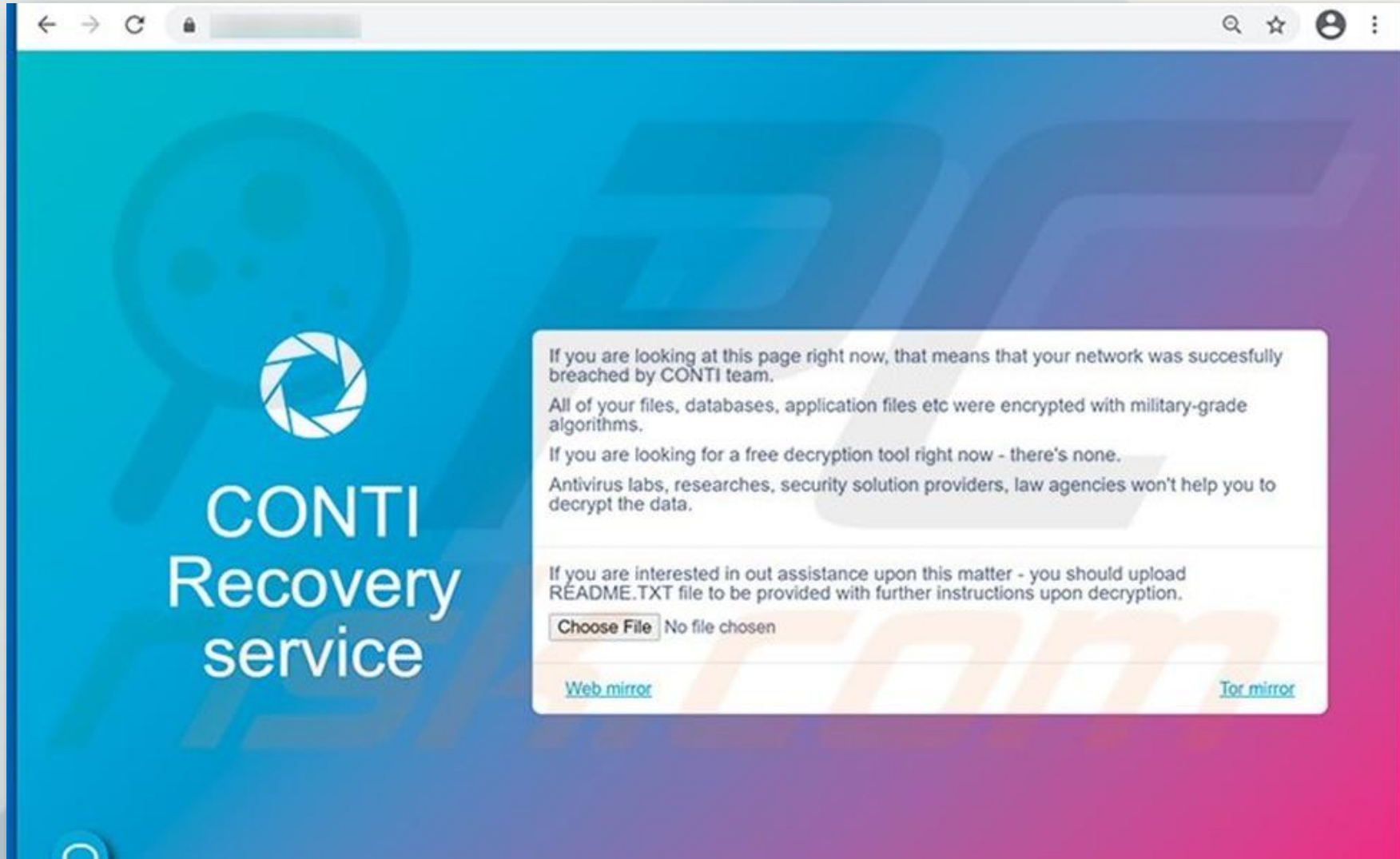
4

Erst Forderung der Erpresser, dann unser Gegenangebot

5

Unser erstes Angebot kauft uns Zeit und zeigt der Gegenseite, dass etwas zu holen ist, Faktor Zeit wird zu „unserem Freund“

Die Verhandlung – Der Chat beginnt



Die Verhandlung – Der Chat beginnt

CONTI Recovery service

Hi There! This is Conti Team.
As you already know, we have infiltrated your networks, researched them, and found critical vulnerabilities which enabled us to access and exfiltrate your inner documentation and encrypt your file servers, SQL servers, subdomains, and local networks.
Due to poor security of your networks, we have downloaded your critical information with a total volume of more than 450 GB. This information includes personal data of your customers, employees, and vendors, as well as your legal, financial HR, IT, audit, and compliance directories (among other files). We obtained personal documents, phone numbers, contact information, consolidated financial statements, payroll, and banking statements.
Fortunately, Conti is here to prevent any further damages!
First, we can provide you with IT support by offering a decryption tool as well as a security report that will address the initial issues with your network security that resulted in this situation.
Secondly, we offer you damage prevention services. At this point, all of your files are about to get public on our blog and will be available for anyone, including darknet criminals who are eager to abuse your information for their own evil purposes like social engineering attacks against your customers and vendors, spamming, and other bad actions.
Your customers, vendors, employees, and investors (lists are available from your inner documentation) will also be notified by us about the breach. This way then can know what to do, since their private data is getting public.
It goes without saying that this privacy violation will lead to long-term legal, regulatory, financial, and reputational damages, including lost contracts and class action lawsuits from those whose info was exposed. However, as a part of our deal we offer a solution to prevent this from happening!
We will first give you a file tree to demonstrate which files we downloaded from your network. Then, you can choose certain file names from this listing and we will provide you with these files to prove that we have them. Then we transfer all the files that we have back to you and delete them from all our hostings and servers, making sure that you are the only one who has access to them. This way, all the above mentioned risks will be prevented!
The price for all of our services is \$5,000,000 USD
As we received this question before, we would like to make a preemptive clarification:
No THERE IS NO WAY that we will not fulfill our promises after you pay. To put it simply - the chances that Hell will freeze are higher than us misleading our customers. We are the most elite group in this market, and our reputation is the absolute foundation of our business and we will never breach our contract obligations.
Please let me know if you have further questions!

Die Verhandlung – Der Vertrag

Hi CONTI team,
As it is usual between business men we should finally write down a contract to what both parties have agreed on.
Contract
Between [REDACTED]
And: Conti team (in the following: Conti)
Terms and conditions
Conti [REDACTED] has agreed on 05.10.2021 on the following terms and conditions:
1) Conti will provide a detailed written IT security report [REDACTED] contains when and how it was possible to breach the IT security systems of [REDACTED] servers were infiltrated and which data exactly was downloaded. The report will be forwarded by Conti directly after the payment was received.
2) Conti confirms hereby that the complete data of the [REDACTED] has not been copied. The one and only original download will be handed over [REDACTED] a cloud server that is only accessible [REDACTED]. The Link to this cloud will be forwarded by Conti directly after the payment was received.
3) Conti confirms hereby that [REDACTED] has not been sold in the past, the present or will be sold in the future to any individual or Conti client.
4) Conti confirms hereby that [REDACTED] has not been published in the past, the present or will be published in the future by Conti or any party that had access [REDACTED] data.
5) Conti [REDACTED] for the services and guarantees above on a payment of 725.000 USD. The payment will be transferred in BITCOIN.
[REDACTED] 05.10.2021, Germany
On behalf of Conti team.

1 hour ago



Operator Kay, speaking on behalf of Conti team, confirms all the abovementioned point of the agreement between the [REDACTED] and Conti Team.
Also we want to add the time frames for the payment. 725.000 USD in BITCOIN must be transferred to address bc1qcrqqt3gv4wwpvnrtgzw8en2ej3k3927nmw9zt in 48 hours from this statement.

39 minutes ago

Mr. Peter, you confirm?

Die Verhandlung-Entschlüsselung und Security Report

Here is your data:

mega.nz
wzvebkxv@pokemail.net
hysuiious65@45fGha!

2 minutes ago

The decryptor is being prepared now.

2 minutes ago

[0Y2bUdHGJV86rTP8Tu27AgfN91oYLnc2GES6JjNUJY6Wy4r1DIzS2E7P7QpX2VVe_decryptor.exe](#)
[\[108kB\]](#)

1 minute ago

Decryptor:

- 1) Launch the decryptor under Administrative rights
- 2) Wait till the decryptor window is closed
- 3) if any of the files haven't changed the extension back to the original - repeat 1 and 2

1 minute ago

We have penetrated your network using email compromise. So, first of all - provide all your employees with strict instructions regarding security measures.

Basic recommendations regarding network:

1. Implement better email filtering policies
2. Implement better password policies
3. Consider blocking some particular attacks like pass-the-hash and pass-the-ticket
4. Update all of your internal systems to the latest versions
5. Review network segmentation and take care about buying hardware firewalls with filtering policies
6. Block kerberoasting attacks
7. Conduct full penetrations tests (both external and internal)
8. Implement better AV/EDR systems
9. Review group policies, remove domain and local admin rights for some users.
10. Implement better DLP software system

51 seconds ago



Tip of the Day

Krisenmanagement-Handout für alle Mitglieder des Krisenstabs – Roles and Responsibilities

Cyber-Krisenübungen lassen Sie in der Krise schneller, besonnener und effektiver entscheiden

Social Engineering Awareness Schulungen sind unverzichtbarer Bestandteil einer ganzheitlichen IT-Security

Darknet Intelligence as a Service als wirksames Frühwarnsystem zum Schutz des Unternehmens. Abgeflossene Credentials, Waren, Informationen, etc. werden so beobachtet; unternehmensbezogene Schadsoftware wird frühzeitig identifiziert

Red Teamings/ Pen-Tests (Partner)

Cyberversicherung inkl. Lösegelddeckung

Kontakt

RiskWorkers GmbH

Konrad-Zuse-Platz 8
81829 München

Telefon: +49 89/20 70 42- 630

Fax: +49 89/20 70 42- 631

Email: office@riskworkers.com

