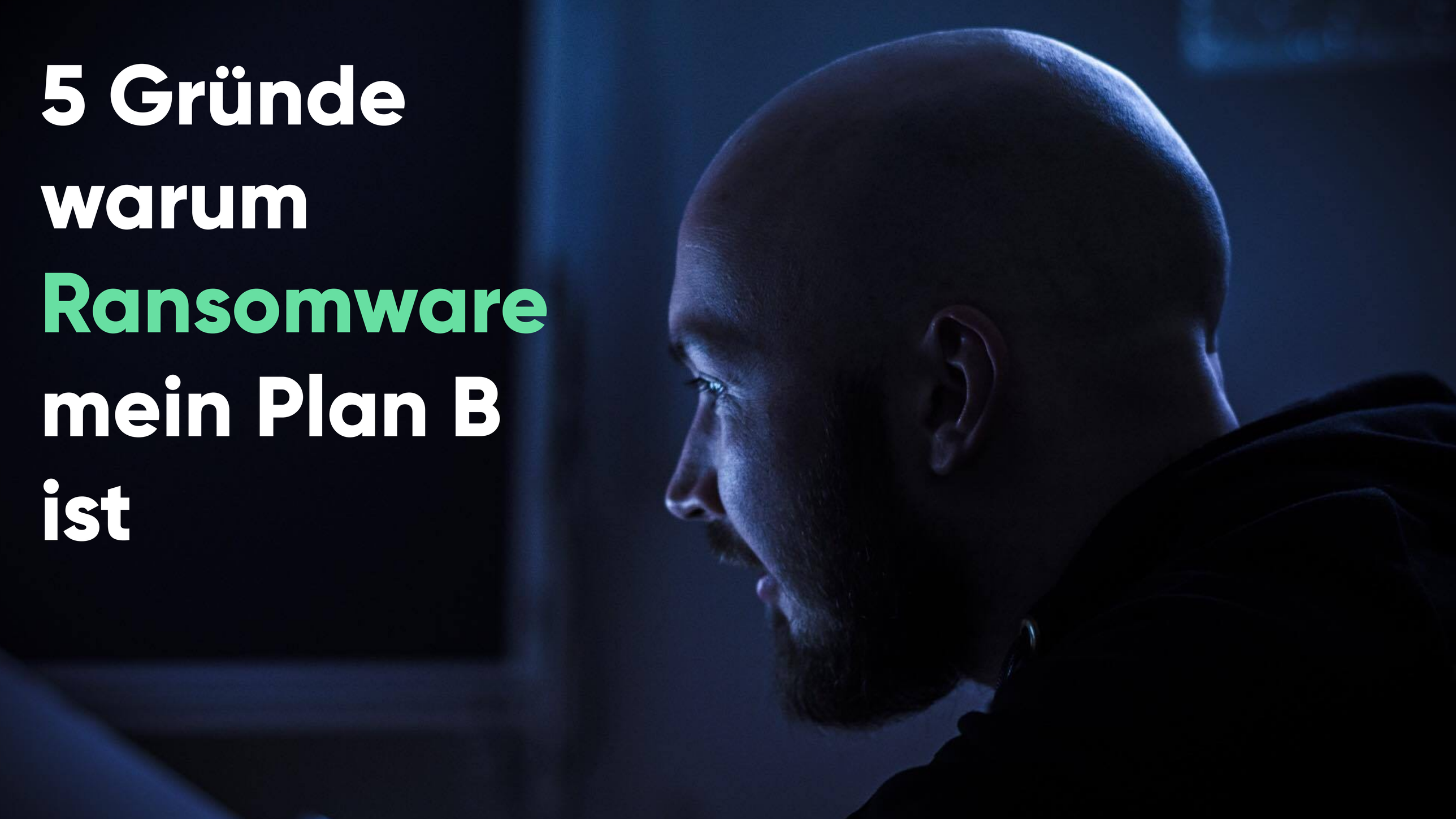
5 Gründe warum Ransomware mein Plan B ist



Disclaimer: Nicht wirklich.

MARTIN HAUNSCHMID

- Datenbankentwicklung
- Business-Software
- Ausflug in die Kommunikation
- Web-Development
- Tech-Blog martinhaunschmid.com

IT-SECURITY

- Offensive Security Certified Professional (OSCP)
- Penetration Testing
- hack-mi.net Bootcamp
- LinkedIn Top Voice 2020

Ablauf

\ [0] = Die Branche boomt

\ [1] = Weil Digitalisierung vorgelebt wird

\ [2] = Weil die Versicherungen noch ahnungslos sind

\ [3] = Weil einem nix passiert

\ [4] = Weil die Unternehmen (größtenteils) schlecht vorbereitet sind

[0] Die Branche boomt


Das Internet, 2021

Cyberangriff auf Anhalt-Bitterfeld: Suche nach Lücken, Stellungnahme des CCC

Manuel Atug vom CCC stellt klar: Es gibt etliche Sicherheitslücken in kommunalen Systemen. IT-Sicherheit müsse viel mehr in den Fokus geraten.

Lesezeit: **3 Min.** In Pocket speichern 72

CHRONIK

Cyberangriff: Palfinger zahlte Lösegeld

Nur mit der Zahlung von Lösegeld hat der Salzburger Kranhersteller Palfinger Ende Jänner eine Cyberattacke abwehren können, das hat das Unternehmen jetzt eingestanden. Durch den Hacker-Angriff wurden die meisten der weltweit 35 Werke für rund zwei Wochen lahm gelegt.

Colonial Pipeline attack: Everything you need to know

Updated: DarkSide has claimed responsibility for the catastrophic ransomware outbreak.

WIRTSCHAFT

Salzburg Milch produziert wieder nach Hacker-Angriff

Acht Tage nach dem Hackerangriff auf die EDV der Salzburg Milch hat die Molkerei in Salzburg und Lamprechtshausen (Flachgau) den Normalbetrieb wieder aufgenommen. Das teilte der drittgrößte Milchverarbeiter Österreichs am Donnerstag mit. Auf die Frage, ob Geld an die kriminellen Hacker bezahlt wurde, sagte ein Manager: „Dazu darf und kann ich nichts sagen."

JBS: FBI says Russia-linked group hacked meat supplier

Kaseya CEO at Center of Massive Ransomware Attack Says 'It Totally Sucks'

“We all have to take a step back and realize this is the world we live in.”

RD By Radhamely De Leon

20 Mrd.

Schaden durch Ransomware 2021

Cybereason: True Cost of Ransomware, 2021

alle 11s

Erfolgt ein Ransomware-Angriff

Cybereason: True Cost of Ransomware, 2021

66% hatten Umsatzeinbußen

42% Versicherung deckte nicht alle Kosten

25% mussten laufenden Betrieb einstellen

29% mussten Stellen abbauen

46% haben nach Bezahlung nicht alle Daten wieder

80% der Unternehmen die bezahlten, wurden wieder angegriffen.

Cybereasen: True Cost of Ransomware, 2021

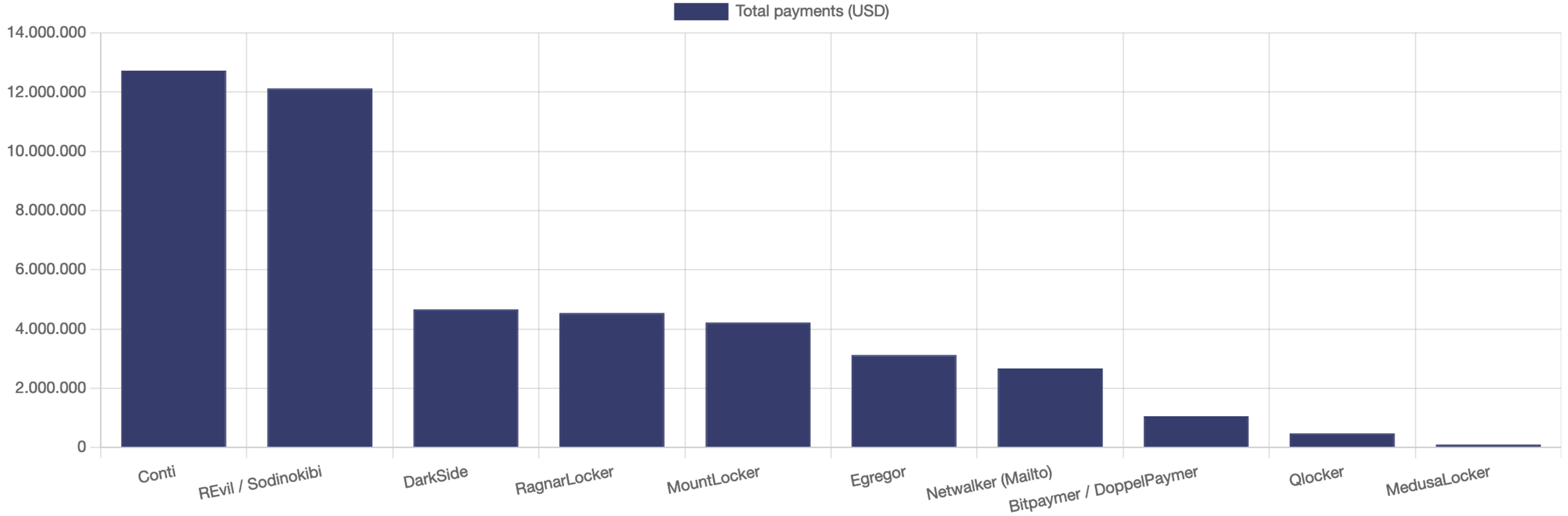
Haben Ransomware-Gruppen CRMs?

Random Corporation

hat bezahlt **Stammkunde**

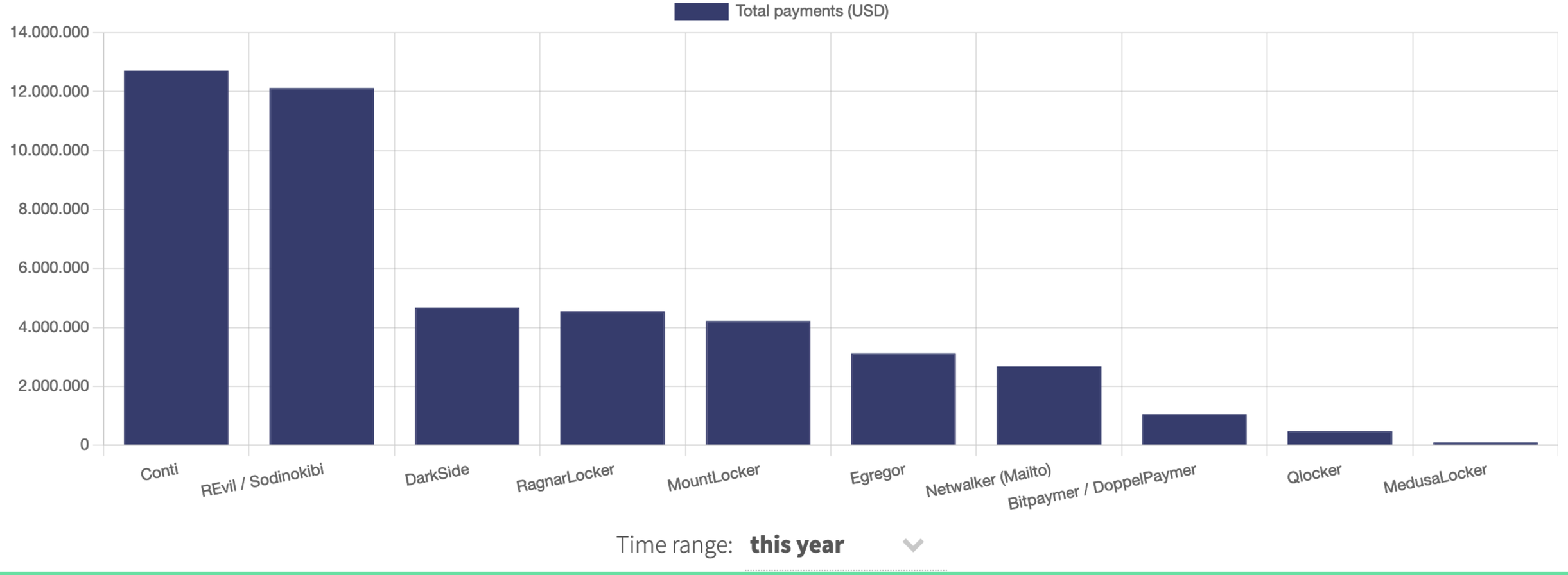
‘I scrounged through the trash heaps... now I’m a millionaire:’ An interview with REvil’s Unknown

https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/



https://ransomwhe.re/

Juli 2021



Das sind nur selbst-reportede Zahlen

https://ransomwhe.re/

Juli 2021

[1] Weil Digitalisierung vorgelebt wird

“Once you only had to deal with encryption and decryption,” he explains. “Now we’re talking about maintaining a data leak site, having someone take care of the press releases, having someone who takes care of the graphics, someone who takes care of managing when and how that data is uploaded to the site.”

Arbeitsteilung

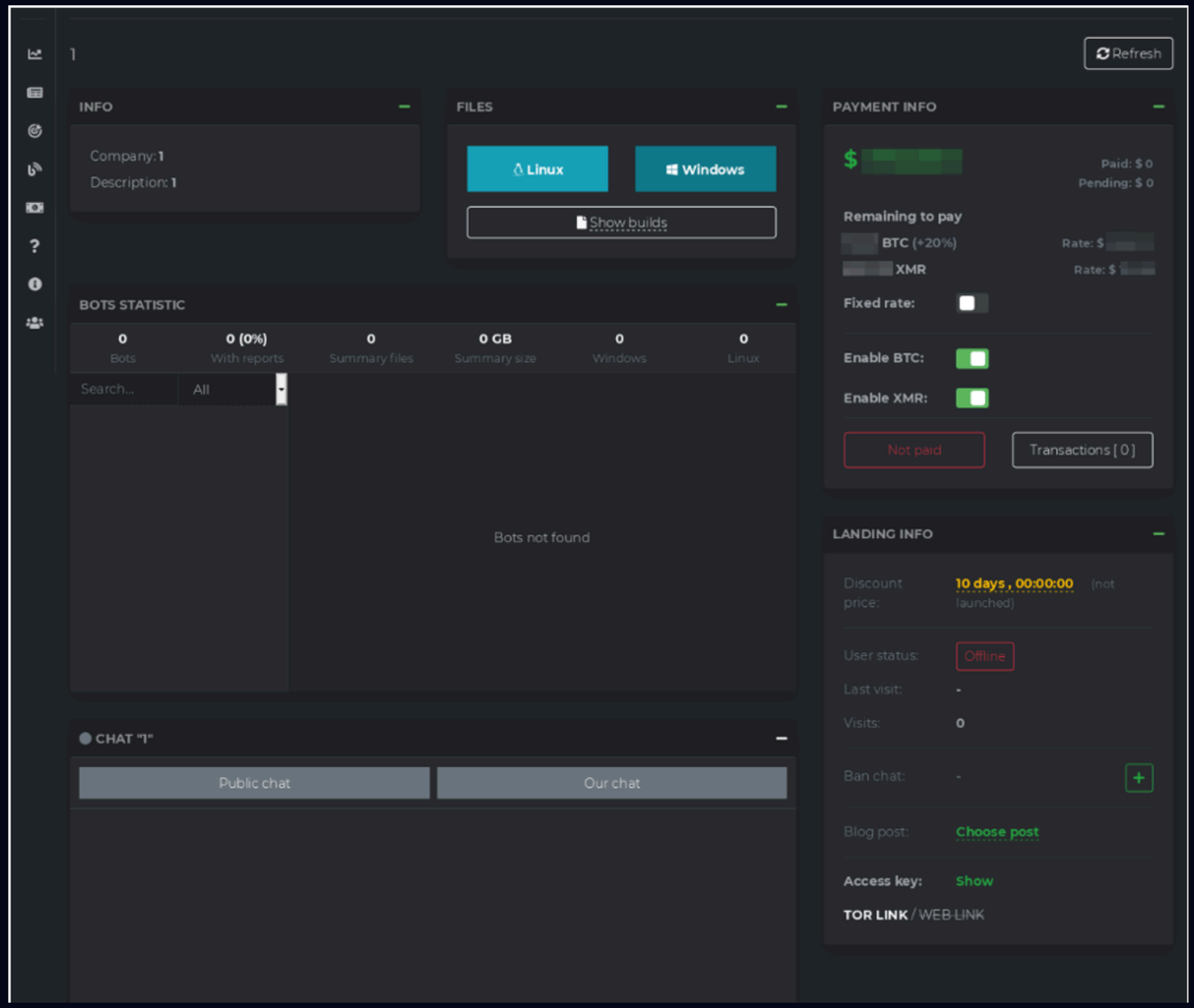
- **Forschung und Entwicklung:** Programmieren am eigenen Produkt, finden neue Sicherheitslücken
- **"Vertrieb":** Kümmert sich um Zugänge **in** die Infrastruktur der Kunden.
- **PR / Marketing:** Etabliert die Marke, schafft Vertrauen
- **Helpdesk / Support:** Verhandelt & hilft Kunden
- **Geldwäsche:** Macht Bitcoin zu Offline-Geld

"Externer Vertrieb"

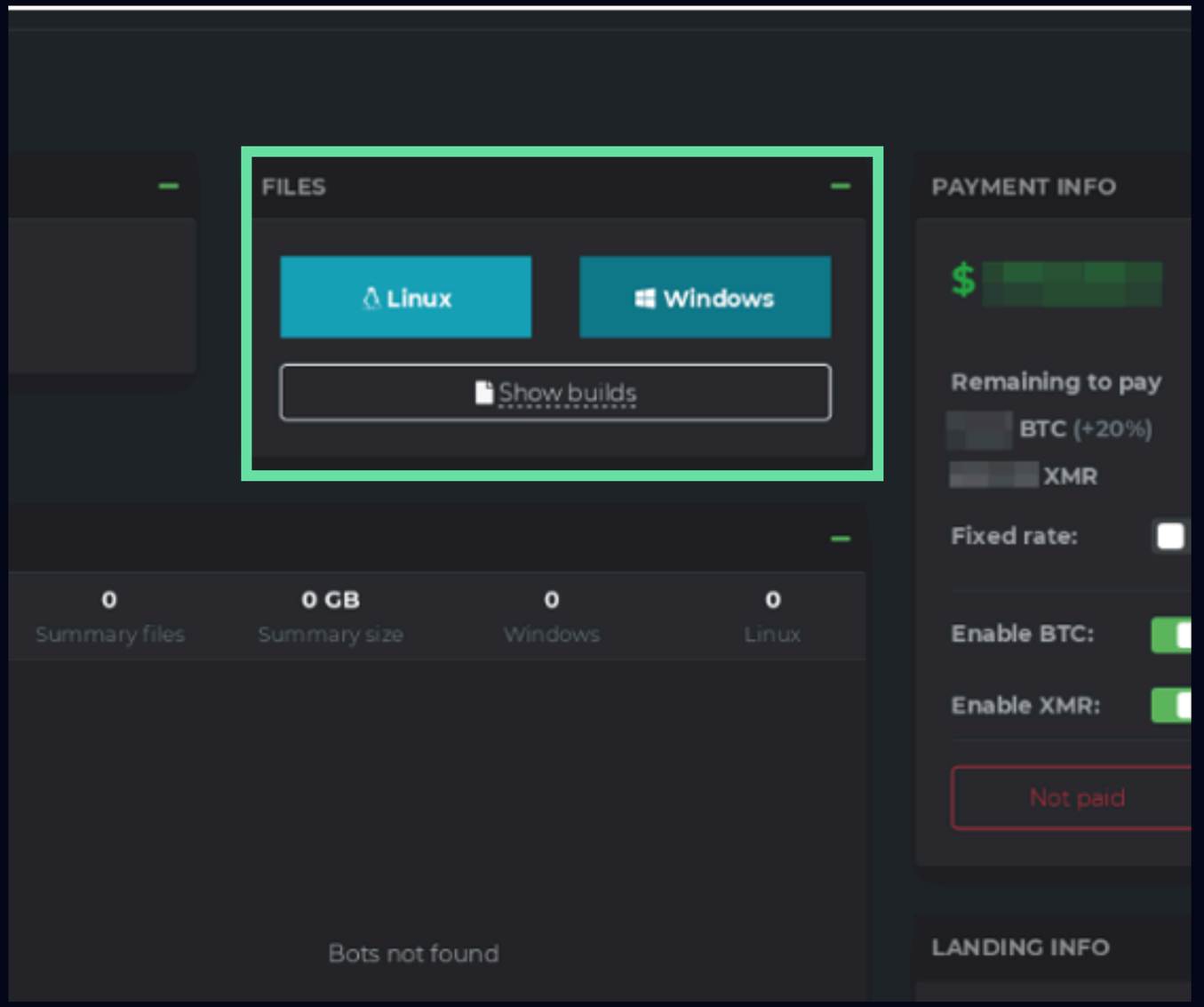
- **Affiliates:** Sind Hacker (müssen nicht all zu gut sein eigentlich), die in Unternehmen einsteigen.
- **Verwenden das Produkt** der Ransomware-Gruppe
- **Gewinn wird geteilt** (unterschiedliche Deals möglich)
- Kriegen **Dokumentation**

"Externer Vertrieb"

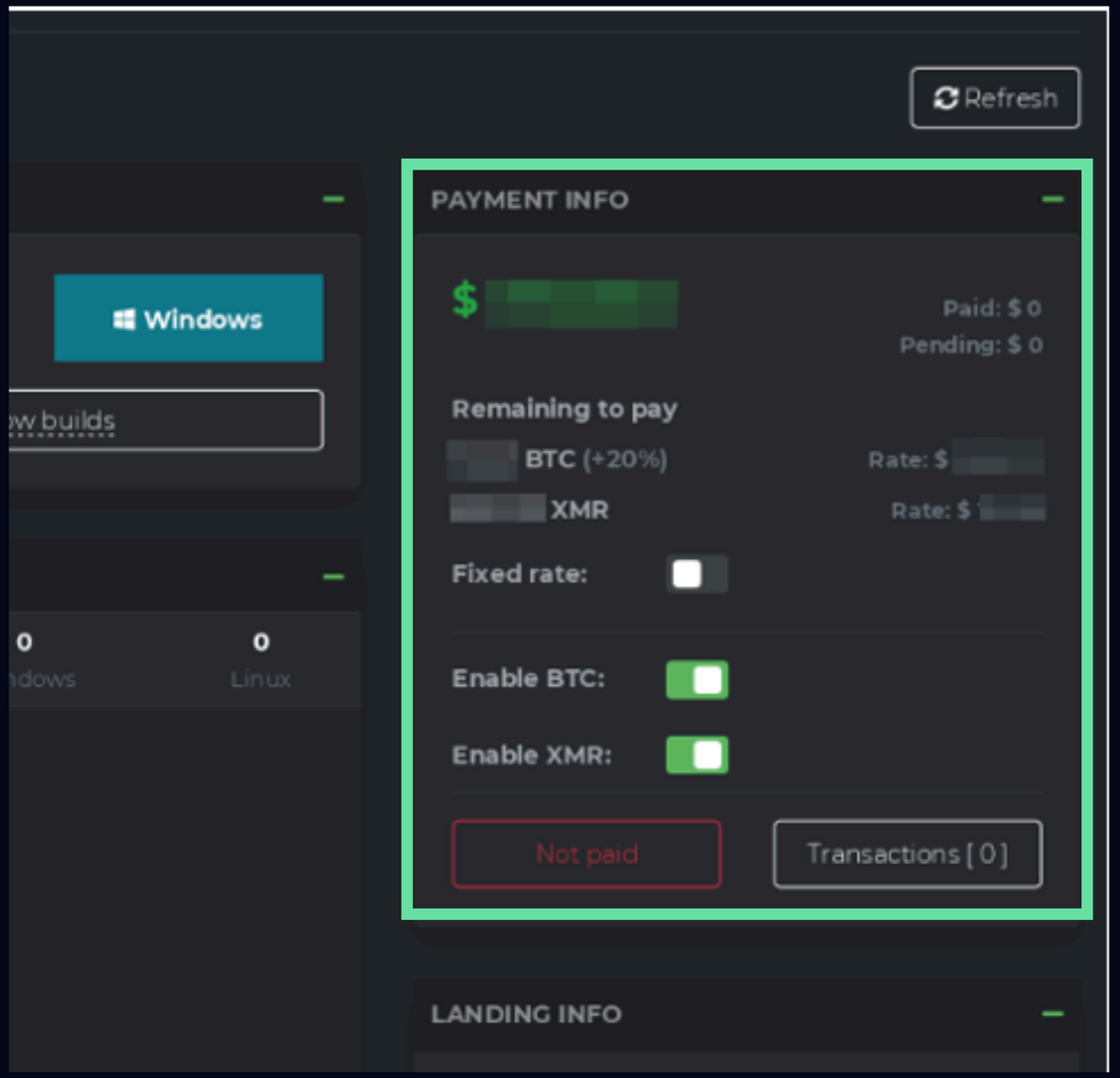
- Sieht sich interne Dateien an:
  - Gibt es eine Versicherung?
  - Wie sehen die Unternehmenszahlen aus?
- Wo sind die Backups?



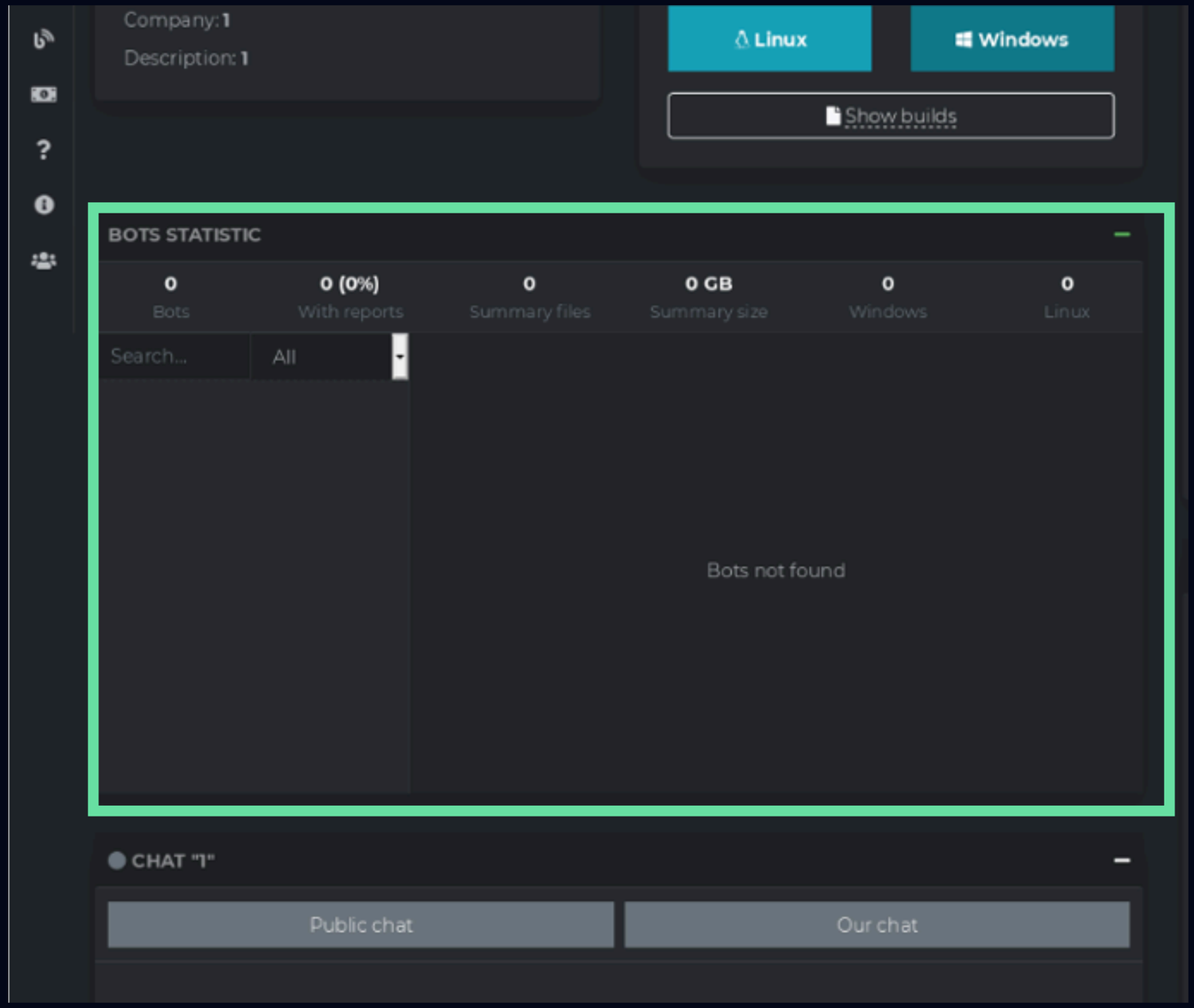
https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html



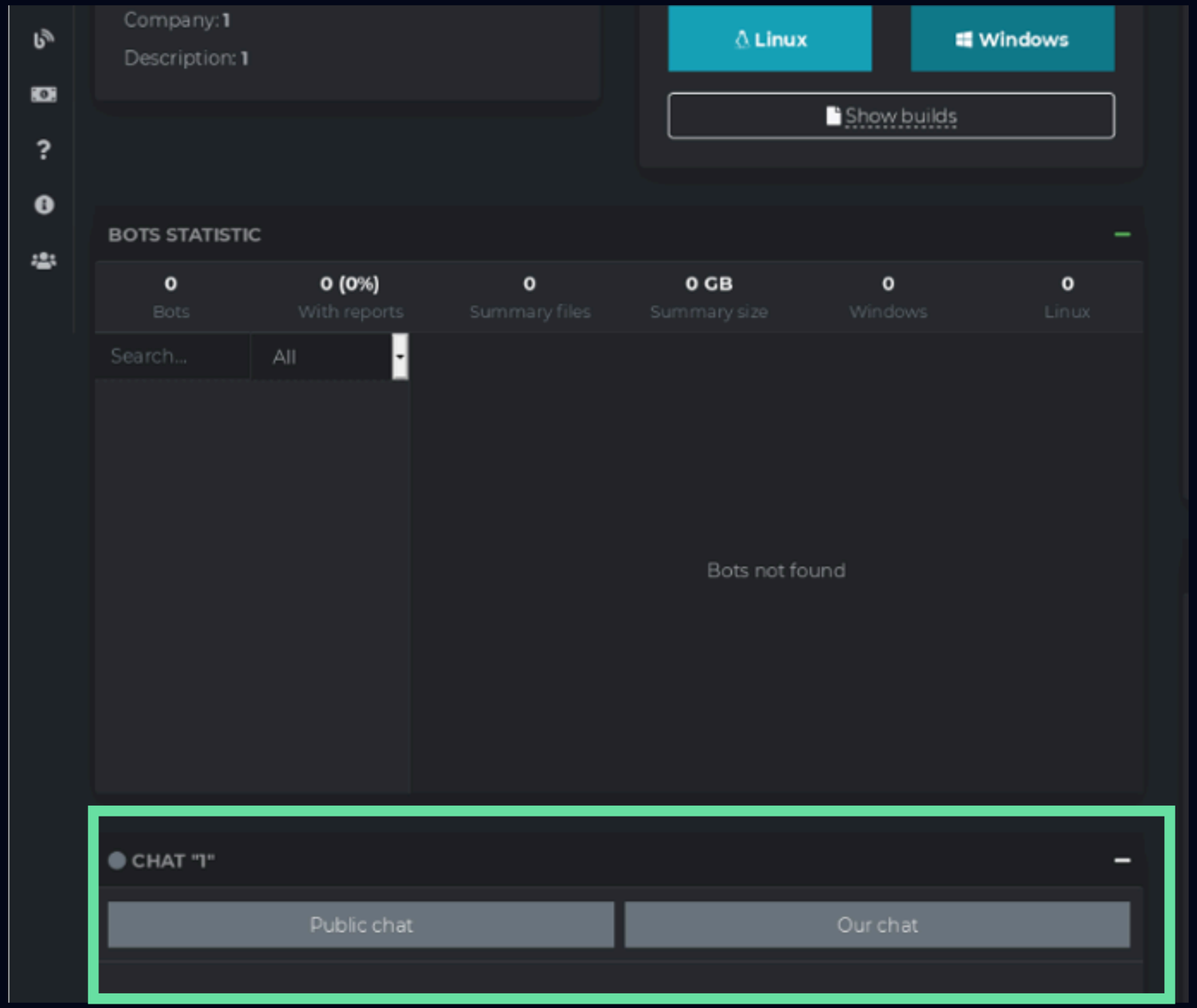
https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html



https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html



https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html



https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

DS: Elliptic Curve Cryptography (ECC) was a really good choice [editor's note: ECC has a smaller key size than the RSA-based public-key system, which makes it attractive to affiliates] what else are you proud of, what part of the code? How do you decide when it's time for new features in the code?

UNK: A search by IOCP [Input/output completion port], a back connection borrowed from crabs [carders], a server-side protection system—there are many advantages, it is better to read AV reviews. Personally, I really like the encryption system. It came out almost perfect.

KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

100% Remote Work

100% Digitaler "Sales"

100% Digitale Unternehmensprozesse

100% Skalierbar

100% Remote Work

100% Digitaler "Sales"

100% Digitale Unternehmensprozesse

100% Skalierbar

Und: Man erreicht den Kundendienst. Zu jeder Tages- und Nachtzeit.

"Wir verschlüsseln automatisiert über 2 Unternehmen hinweg 1.500 Unternehmen"

vs.

"Sie können diese Rechnung nicht per PDF schicken."

[2] Weil die Versicherungen noch ahnungslos sind.

DS: Do your operators target organizations that have cyber insurance?

UNK: Yes, this is one of the tastiest morsels. Especially to hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves.

Unpopuläre Meinung:
Versicherungen sind mit Schuld an der aktuellen Situation

* Wenn das Lösegeld von der Versicherung bezahlt wird

Warum?

Einsparungen durch fehlende IT-Security
+
Versicherung

< **Kosten des Vorfalls**

Die Folgen:

Bezahlen des Lösegeldes anstatt grundlegende Investitionen in IT-Sicherheit.

Ransomware ist der Geldtransfer von der Versicherung zu kriminellen Organisationen.

Die Hacks der Unternehmen selbst ist eigentlich nur ein Zwischenschritt.

Prophezeiung

- **Versicherungen** werden mehr versicherungsmathematische Analysen anstellen
- **Prämien** werden stark steigen
- **Deckung wird verringert** – oder zumindest an härtere Vorgaben gekoppelt

Versicherungen sollten hier nur das Restrisiko abdecken

Beispiel: AXA

[3] Weil einem nichts passiert.

Ukrainian police arrest multiple Clop ransomware gang suspects

Carly Page @carlypage_ / 6:33 PM GMT+2 • June 16, 2021

Comment

Nur die Geldwäscher, Ätsch!

Die Gruppe selbst macht weiter.
Weil man an sie nicht ran kommt.

🇷🇺

"Mir egal, solange ihr keine russischen Ziele angreift."

Verschlüsselungstrojaner ignorieren Systeme, auf denen Russisch als Standardsprache oder das kyrillische Keyboard installiert ist.

[4] Weil die Unternehmen (größtenteils) schlecht vorbereitet sind

Benötigte Erfolgsquote Verteidiger: **100%**

Benötigte Erfolgsquote Angreifer: **1 Mal**

Wobei: Das impliziert, dass Unternehmen überhaupt eine Verteidigung haben...

RDP

Phishing

Macros

Datenleaks

Passwörter

CEO Fraud

36 %

wissen nicht, wie viel Schaden verursacht wurde

KPMG: Cybersecurity in Österreich, Mai 2020

24 Tage

Sind Angreifer im System, bis der Hack entdeckt wird.

https://www.zdnet.com/article/cybersecurity-organisations-are-getting-quicker-at-discovering-cyber-attacks-in-their-networks-but-theres-a-catch/

Weil dann alles verschlüsselt wird, nicht weil die Unternehmen den Angreifer entdecken.

0-4 Tage

Dauer, bis eine Sicherheitslücke nach dem Patch aktiv ausgenutzt wird

0-4 Tage

z.B. PrintNightmare, WordPress, ...

Fazit

Fazit

- **Es sieht gut aus** – für die Cyberkriminellen
- **Versicherungen** helfen nur bedingt
- Unternehmen sind **nicht vorbereitet**
- **Politik** macht bisher wenig

Was tun!?

- **Business Continuity Plan:** Wie würden wir offline funktionieren?
  - **Business Recovery Plan:** Wie kommen wir wieder? => **Resilienz**
  - **Incident Response Plan**

https://www.enisa.europa.eu/topics/threat-risk-management/risk-management

Was tun!?

- **Backups:** Und zwar so, dass sie jemand im System **nicht findet oder nicht löschen/verschlüsseln kann.**
- **E-Mails, Passwörter, externer Zugriff:** Die 20%, die 80% bringen
- **Endpoint Protection:** Nicht nur Signaturbasiert, sondern auch Verhalten!

123456	654321	purple
12345	michael	angel
Danke	ashley	jordan
123456789	qwerty	liverpool
password	111111	justin
iloveyou	fürs	loveme
princess	iloveu	123123
1234567	000000	dabeisein
rockyou	michelle	football
12345678	tigger	secret
abc123	sunshine	andrea
nicole	chocolate	carlos
daniel	password1	jennifer
babygirl	soccer	joshua
monkey	anthony	bubbles
lovely	friends	1234567890
jessica	butterfly	superman

- martinhaunschmid.com
- contact@martinhaunschmid.com

Ressourcen

- **Darktracer:** Aktuelle Infos, wer von welcher Gruppe erwischt wurde
- **Raidforums:** Datenleaks / gehackte Datenbanken
- **Stopransomware.gov**: US-Plattform zum Thema, mit Empfehlungen