Cyber Crime nimmt keine Rücksicht auf Normen

Anatomie einer Ransomware Attacke

Oldenburg, 04. April 2019

Jan Willeke, Major Account Manager MSSP & Carrier

Definition

Ransomware (von englisch *ransom* für „Lösegeld“), auch *Erpressungstrojaner*, *Erpressungssoftware*, *Kryptotrojaner* oder *Verschlüsselungstrojaner*, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.

Die Bezeichnung setzt sich zusammen aus *ransom*, dem englischen Wort für Lösegeld, und *ware*, entsprechend dem für verschiedene Arten von Computerprogrammen üblichen Benennungsschema (*Software*, *Malware* etc.).

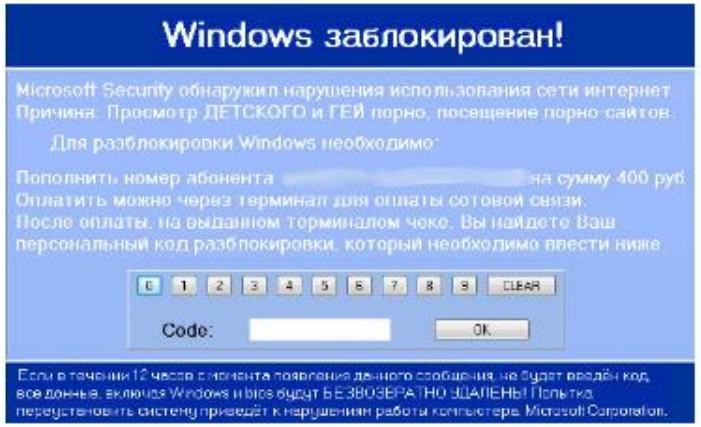
Ransomware – ein wachsendes Problem

Erste Ransomware
“AIDS Trojaner”
per Diskette


加油卡自助服务终端
Fuel Card Self-service Terminal
中国石油


DB
Abfahrt Departure
Nach
Gleis
platform


Mai 17
KISA



Quelle: https://ransomware.at/website_old/gallery.php

Cyber Crime – Die Gewinne sprudeln!

DIEBE

ERPRESSER

DATA BREACH

RANSOMWARE

FORTINET

Web-hosting firm agrees to pay over $1 million to ransomware extortionists

BY GRAHAM CLULEY POSTED 20 JUN 2017 - 12:05PM

CYBERCRIME

Nayana, ein südkoreanischer Web Hosting Anbieter, wurde Opfer einer groß angelegten Ransomware Attacke, welche über 153 Linux Server getroffen und damit einhergehend über 3.400 gehostete Webseiten der Geschäftskunden beeinträchtigt hatte.
Nayana's Systeme wurden durch eine Linux Variante der Erebus Ransomware getroffen, welche dafür entwickelt wurde Daten auf Web Servern zu verschlüsseln und eine Zahlung für die sichere Rückgabe dieser Daten zu verlangen.
Insgesamt hatte Erebus 433 verschiedene File Typen auf den Web Servern verschlüsselt – einschließlich Dokumenten, Datenbanken, Bilder und Videos.
Zwei Wochen nach der Attacke war Nayana immer noch dabei den Normalbetrieb für die Kunden wiederherzustellen und stellte regelmäßig und detailliert Updates über diesen Prozess in einem eigens dafür vorgesehenen Forum bereit.

My boss tell me, you buy many machine, give you a good price 550 BTC
If you do not have enough money, you need make a loan

You company have 40+ employees, every employee's annual salary $ 30,000
all employees 30,000 * 40 = $ 1,200,000
all server 550BTC = $ 1,620,000

If you can not pay that, you should go bankrupt.
But you need to face your child, wife, customers and employees.
Also, you will lose your reputation, business.
You will get many more lawsuits.

아래는 마지막 협상 글에 대한 답변 내용입니다.

My boss accept your price.
About 397.6BTC.
Please purchase machine,
when you pay over 397.6 , you tell me your all machine ID.
i'll open your all machine.

>Now i think you are sincerity.
>i go talk with my boss.
>i think my boss will accept this price.

내 보스가 제시한 가격을 받아 들인다.
약 397.6BTC.
너의 서버는
397.6 이상을 지불하면 모든 서버의 ID를 알려줄것이다.
내가 너의 모든 서버를 풀어주겠다.

Anatomie einer Ransom Attacke

≈15 Minuten

Exploitation and Infection

Social Engineering, Phishing und menschliche Fehler sind die primären Mechanismen um ein Systems zu infizieren.

Delivery and Execution

Sobald der initiale Exploit aktiviert wurde, ist die Ransomware ausgeliefert und permanent im System etabliert

Backup Corruption

Hauptziel sind Backup Systeme, File Server, Festplatten und Dateien wie Bilder, Videos und Dokumente, aber auch z.B. Shadow Copies um sicher zu gehen, dass die Betriebsstörung maximal ist

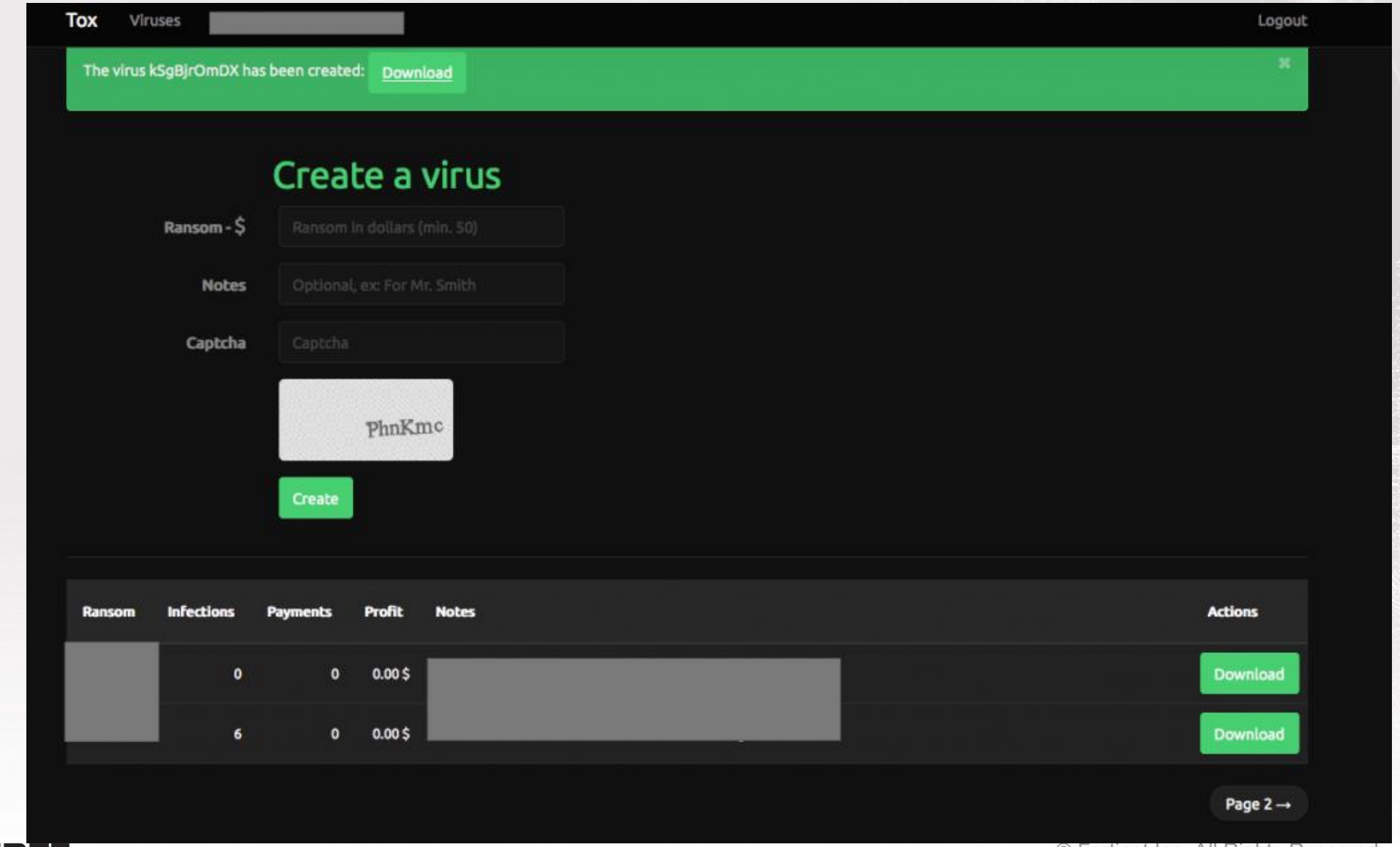
File Encryption

Die Ransomware startet einen aktiven Austausch mit dem Command and Control Server um sich die Schlüssel für die Verschlüsselung zu holen um dann die Zieldaten entsprechend zu verschlüsseln

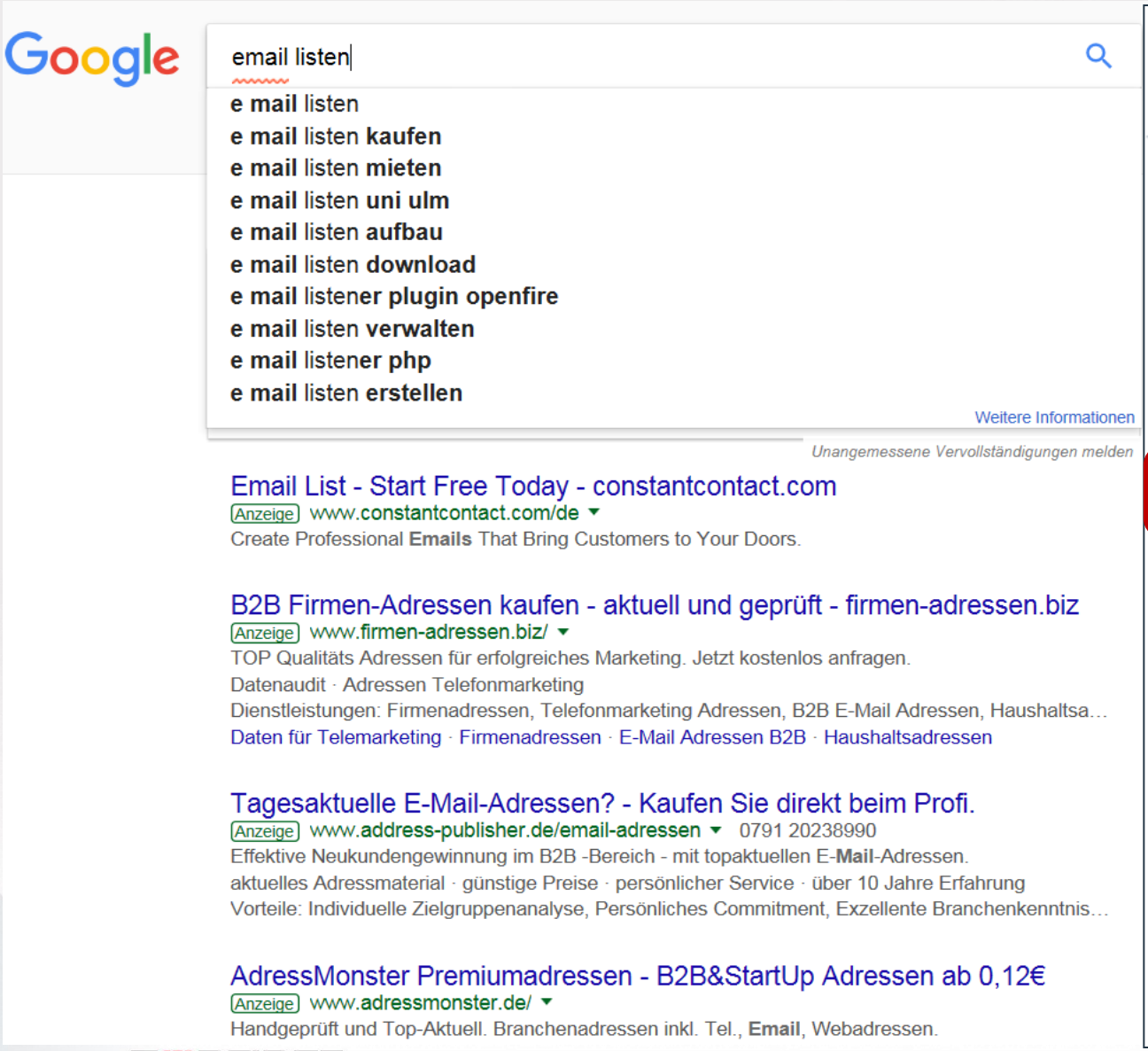
Ransom Demand

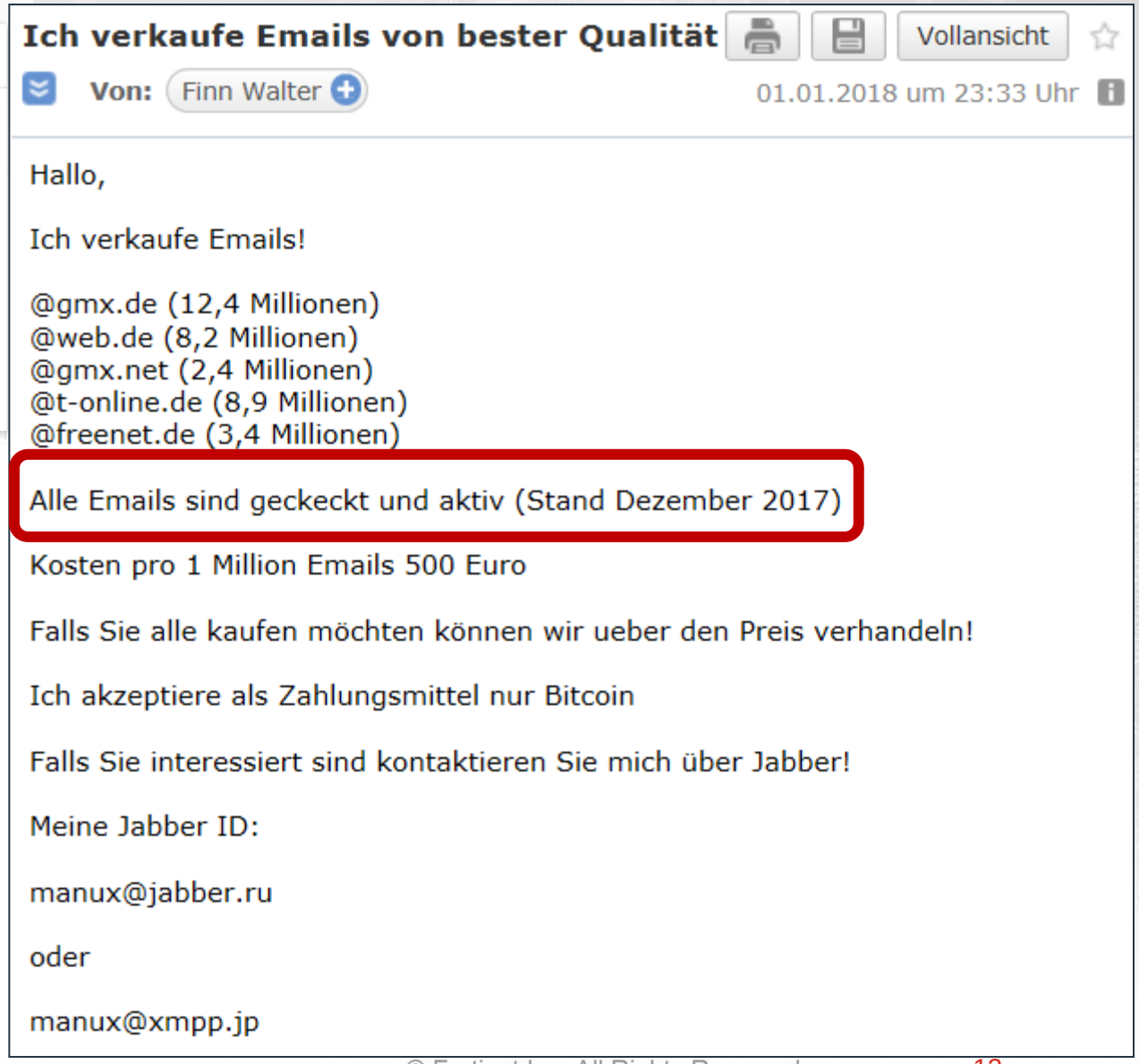
Der Anwender wird per Ransom Note darüber informiert, dass seine Daten verschlüsselt sind und wie viel und wohin Kryptowährung (z.B. Bitcoin) fällig wird um die Daten zurück zu bekommen. Meistens läuft auch eine Uhr (Ticker), je länger es dauert, desto teurer wird es

“Malware as a Service”

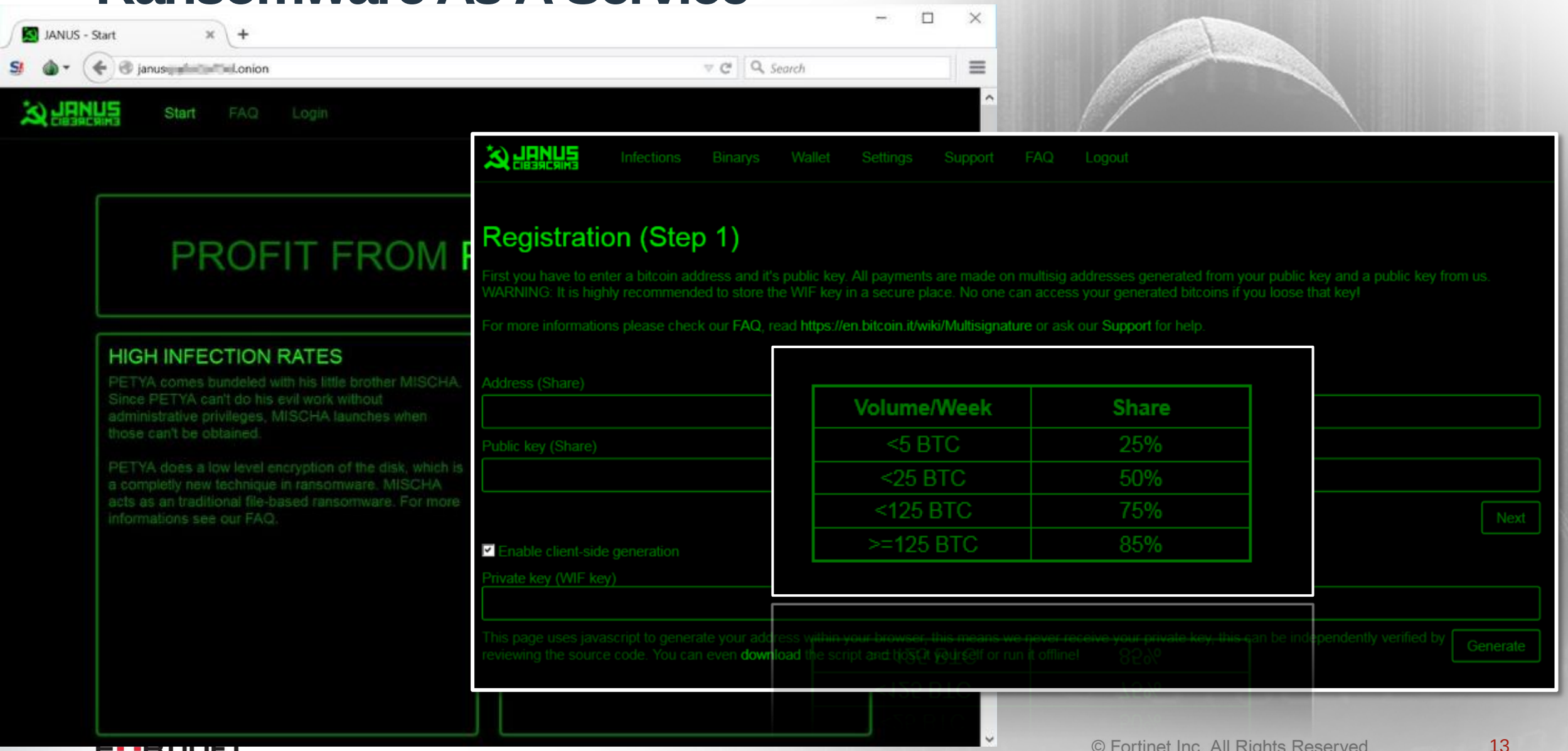


“Targets as a Service”





Ransomware As A Service



Business Case – Research Jamison Utter

- Kosten Ransomware mit 90 Tagen Support: $3.000
  - »Garantierte Infizierungsquote: 10%
    - Erwartete Einnahmerate: 0.5%
- SEO und Traffic Acquisition Kampagne: $3.000
  - »Garantierte Rate: 20.000 Klicks am Tag
- Ransom Einnahmen: ca. $300

Die Berechnung

20.000 Besucher x **10%** Infizierungsquote
= **2.000** Infektionen pro Tag

2.000 x 0.5% erwartete Einnahmenrate
= **10** Einnahmen pro Tag

10 Einnahmen x **$300 x 90** Tage
= **$270.000**

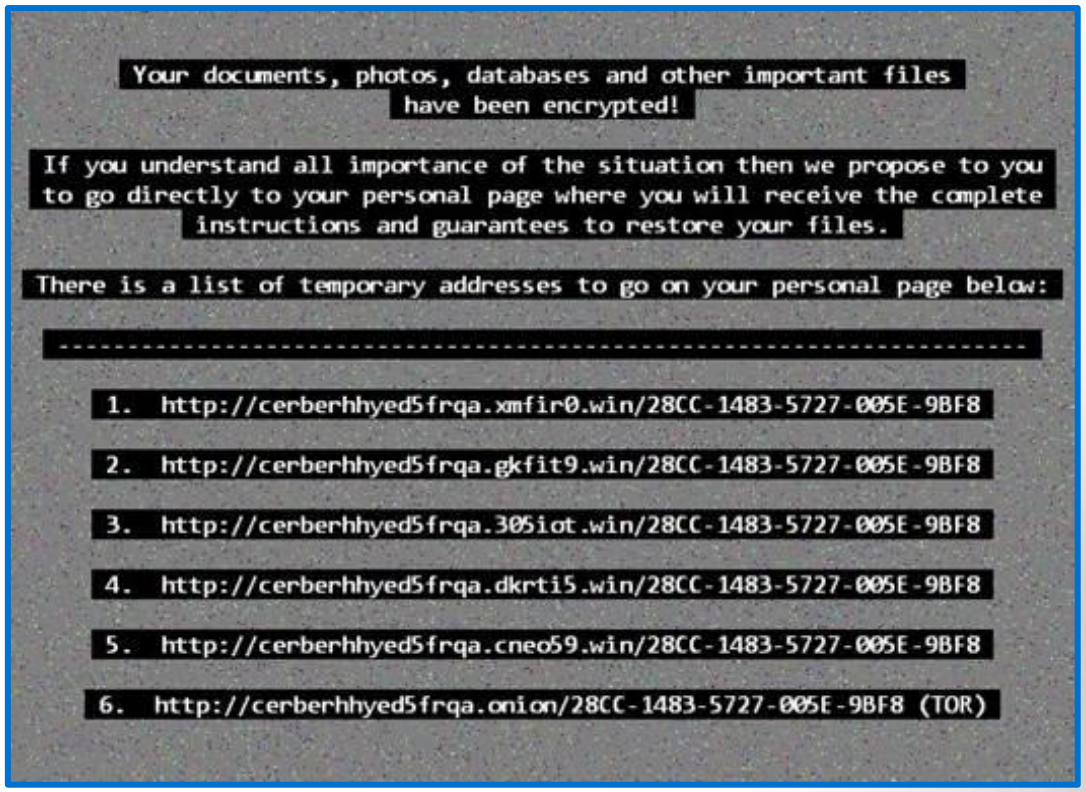
Ransomware Business

Benötigt für ein erfolgreiches Business:

- Produkt/Lösung
- Business Model
- Marketing
- Betrieb/Analyse
- Support
- Finanzwesen

Cerber: erfolgreiche Ransomware in der RaaS Industrie

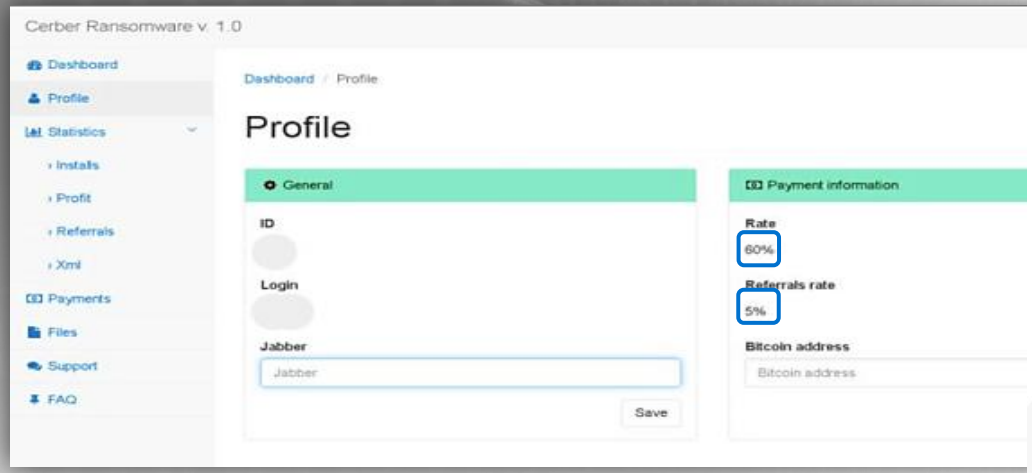
Produkt/Lösung: Cerber

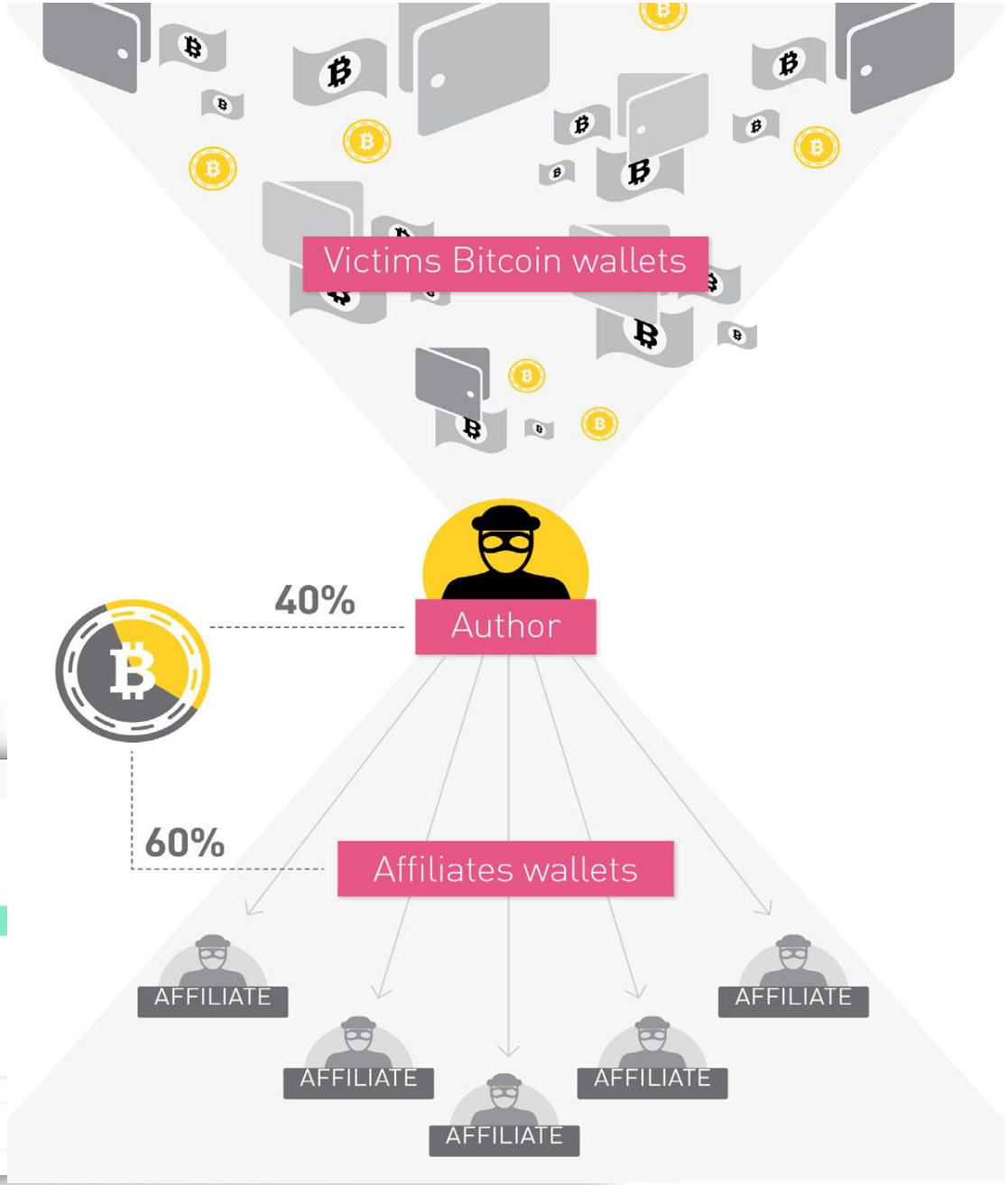


- Erschienen im Februar 2016
- Stetig verbessert und gewartet
- Getestet Security zu bypassen
- Sobald Files verschlüsselt sind, erscheint eine Ransom Note, welche auch von den Computer Lautsprechern durchgegeben wird

Business Model

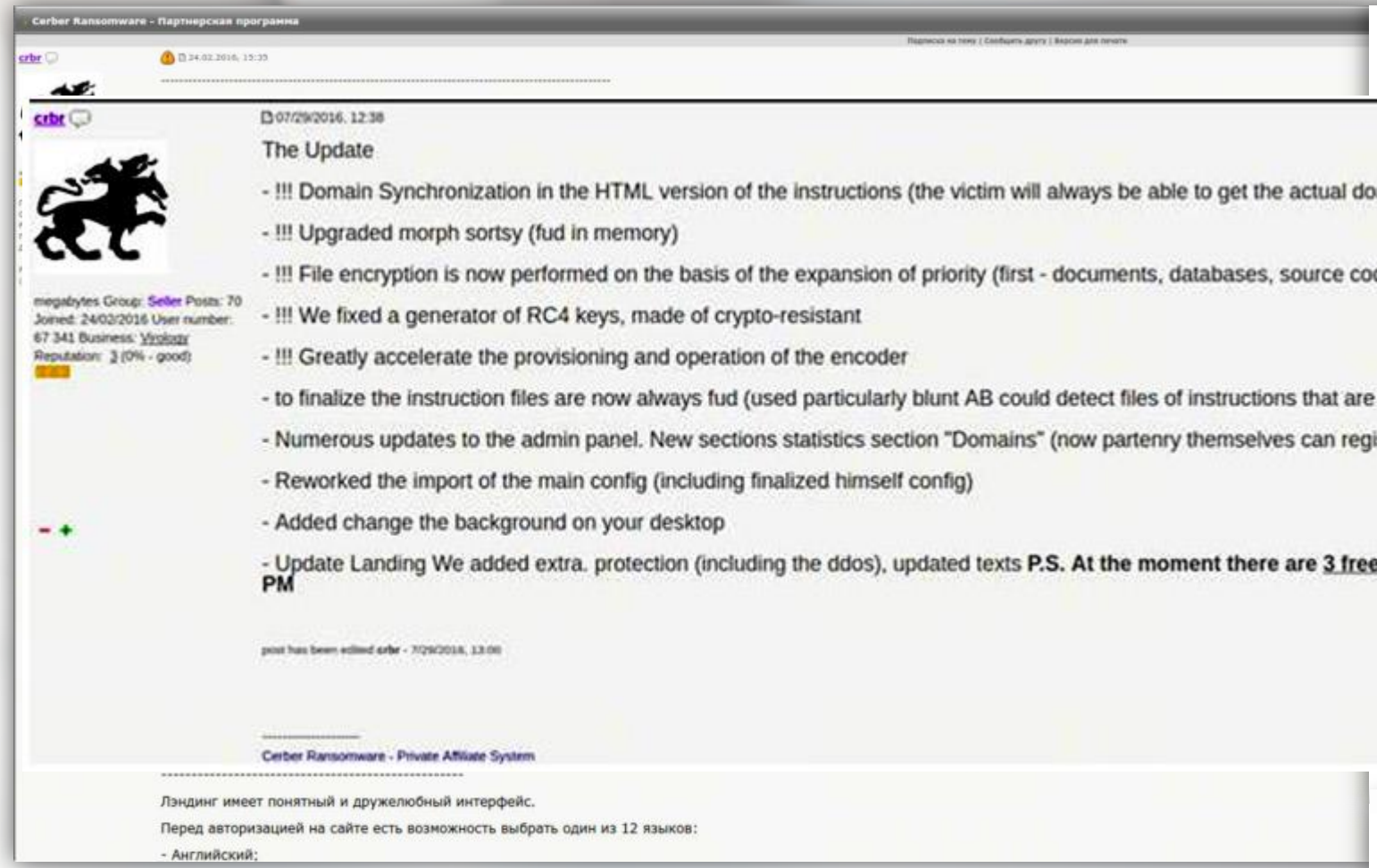
- Cerber wird über ein Partnerprogramm angeboten
- 60% des Ertrages, 5% Freundschaftswerbung für neue Teilnehmer





Marketing

Werbeanzeigen – Informationen über das Partnerprogramm, Erträge, Web Panel und Verschlüsselungsschema

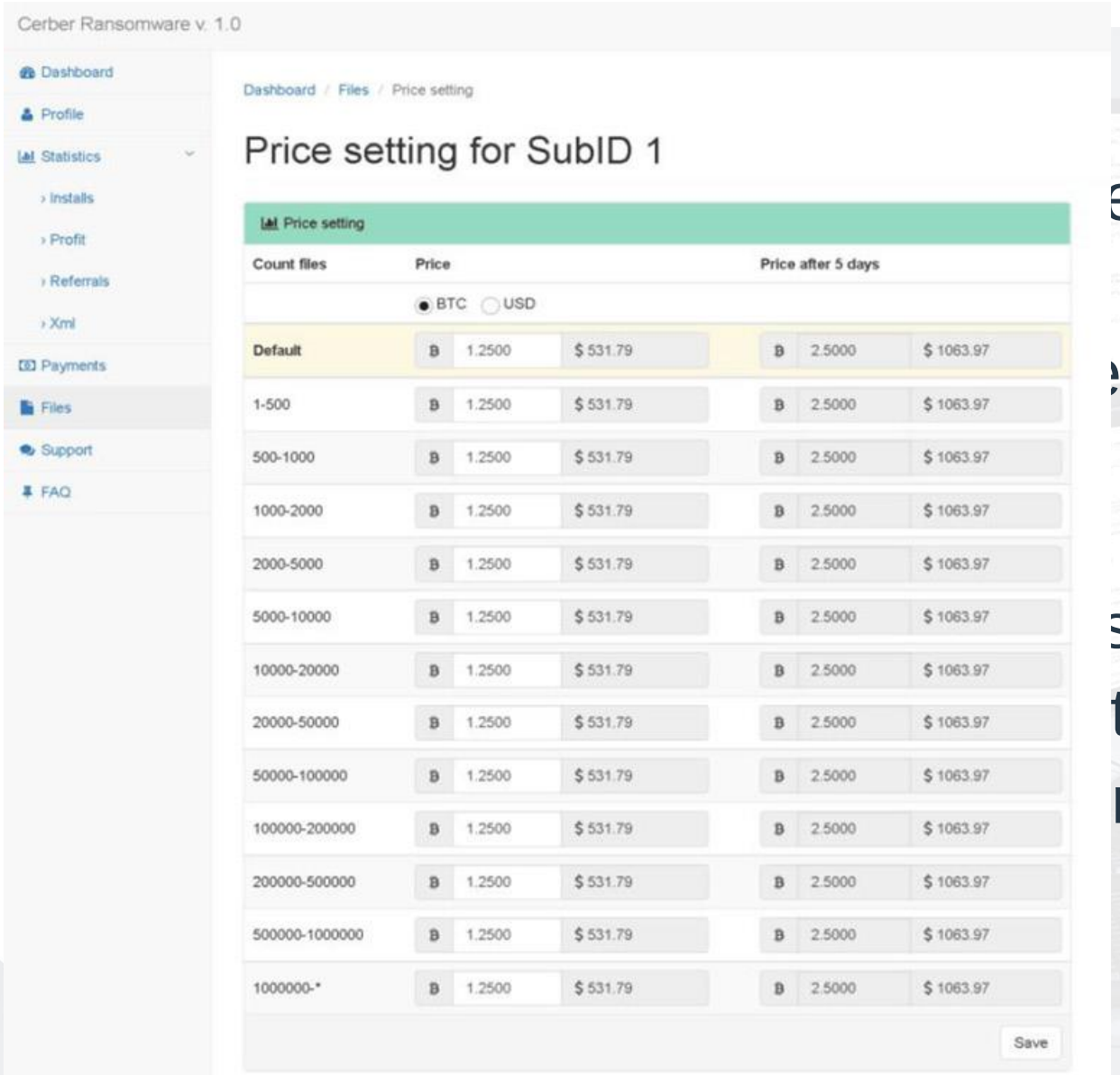


Good day, dear forum participants
Today, I am pleased to present a new solution for the monetization of your downloads!

For each file generated random key that is encrypted with a public key of the local RSA 576 bits.

Also, using the public key of the local RSA 576-bit encrypted header of the source file, which greatly complicates the decoding of files without the decoder (months to decipher the first file).

Betrieb



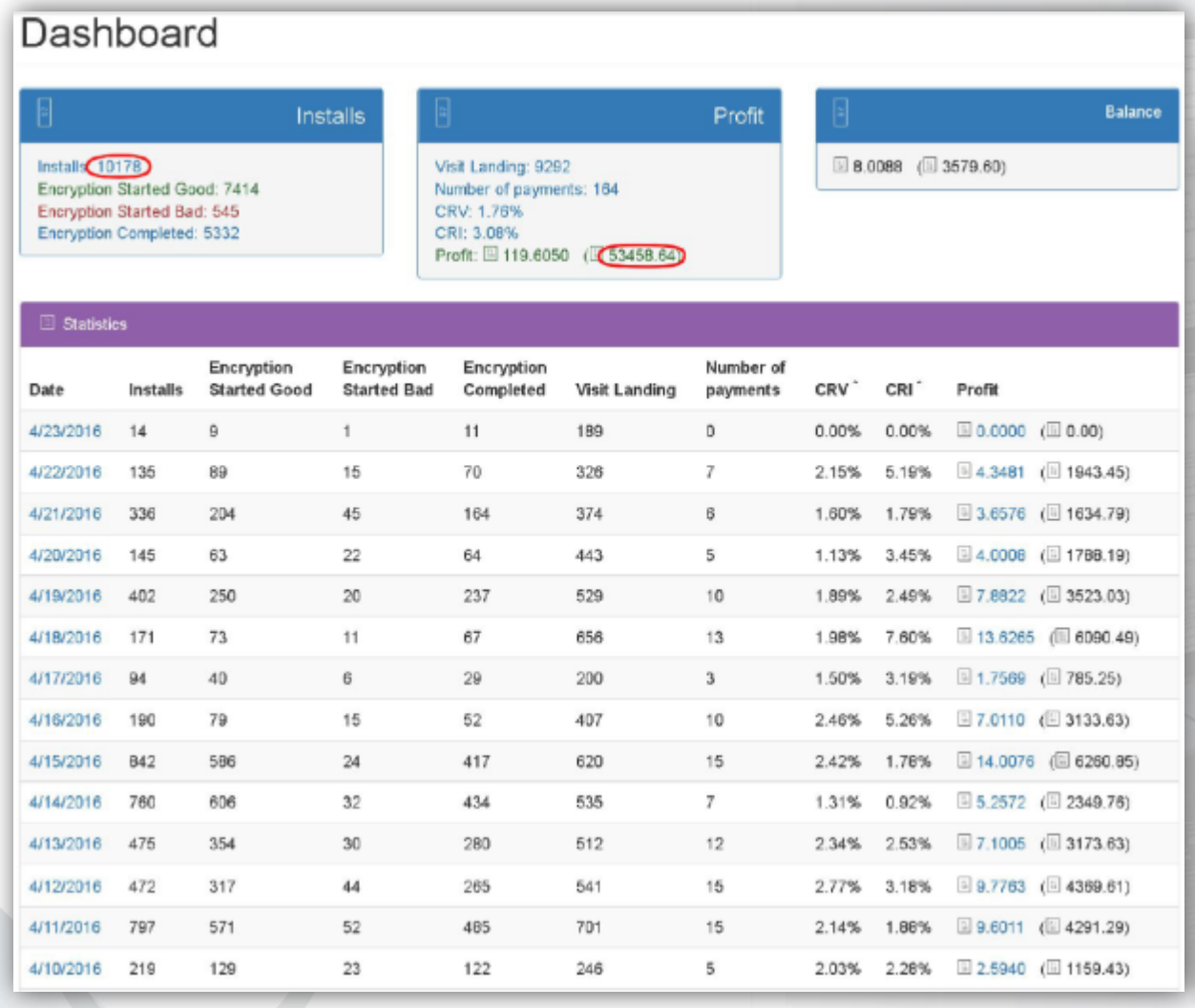
enötigt für den
für die Statistik
en u.a.:

s

t

mit einem Control Panel

Analyse



Dashboard

Installs

Installs: 10178
Encryption Started Good: 7414
Encryption Started Bad: 545
Encryption Completed: 5332

Profit

Visit Landing: 9282
Number of payments: 184
CRV: 1.76%
CRI: 3.08%
Profit: 119.6050 (53458.64)

Balance

8.0088 (3579.60)

Statistics

Date	Installs	Encryption Started Good	Encryption Started Bad	Encryption Completed	Visit Landing	Number of payments	CRV *	CRI *	Profit
4/23/2016	14	9	1	11	189	0	0.00%	0.00%	0.0000 (0.00)
4/22/2016	135	89	15	70	326	7	2.15%	5.19%	4.3481 (1943.45)
4/21/2016	336	204	45	164	374	6	1.60%	1.79%	3.6576 (1634.79)
4/20/2016	145	63	22	64	443	5	1.13%	3.45%	4.0006 (1788.19)
4/19/2016	402	250	20	237	529	10	1.89%	2.49%	7.8822 (3523.03)
4/18/2016	171	73	11	67	656	13	1.98%	7.60%	13.6265 (6090.49)
4/17/2016	94	40	6	29	200	3	1.50%	3.19%	1.7569 (785.25)
4/16/2016	190	79	15	52	407	10	2.46%	5.26%	7.0110 (3133.63)
4/15/2016	842	586	24	417	620	15	2.42%	1.78%	14.0076 (6260.85)
4/14/2016	760	606	32	434	535	7	1.31%	0.92%	5.2572 (2349.76)
4/13/2016	475	354	30	280	512	12	2.34%	2.53%	7.1005 (3173.63)
4/12/2016	472	317	44	265	541	15	2.77%	3.18%	9.7763 (4369.61)
4/11/2016	797	571	52	485	701	15	2.14%	1.88%	9.6011 (4291.29)
4/10/2016	219	129	23	122	246	5	2.03%	2.28%	2.5940 (1159.43)

Statistics

Date	Installs	Encryption Started Good	Encryption Started Bad	Encryption Completed	Visit Landing	Number of payments	CRV *	CRI *	Profit
5/8/2016	22	3	4	4	92	1	1.09%	4.55%	0.9731 (445.27)
5/7/2016	36	4	7	4	249	8	3.21%	22.22%	5.3871 (2465.10)
5/6/2016	148	36	18	26	262	9	3.44%	6.08%	6.8622 (3140.09)
5/5/2016	280	102	25	91	602	15	2.49%	5.36%	9.5242 (4358.19)
5/4/2016	3683	2200	367	1716	641	18	2.81%	0.49%	12.1432 (5556.62)
5/3/2016	3454	2165	344	1565	643	16	2.49%	0.46%	10.2516 (4691.02)
5/2/2016	86	10	3	8	291	7	2.41%	8.14%	5.5179 (2524.92)
5/1/2016	26	2	1	2	32	0	0.00%	0.00%	0.0000 (0.00)
4/30/2016	55	7	7	10	102	2	1.96%	3.64%	1.7419 (797.06)
4/29/2016	183	34	14	43	485	18	3.71%	9.84%	15.1289 (6922.82)
4/28/2016	5792	3987	538	2885	500	10	2.00%	0.17%	7.6064 (3480.63)
4/27/2016	46	1	0	9	143	4	2.80%	8.70%	0.3560 (162.89)
4/26/2016	37	3	0	7	140	3	2.14%	8.11%	0.2263 (103.53)
4/25/2016	38	6	0	19	128	3	2.34%	7.89%	0.2388 (109.27)
4/24/2016	55	14	1	28	61	2	3.28%	3.64%	0.0947 (43.33)
Total	**13941**	**8574**	**1329**	**6417**	**4371**	**116**	**2.65%**	**1.35%**	**76.0522 (34800.74)**

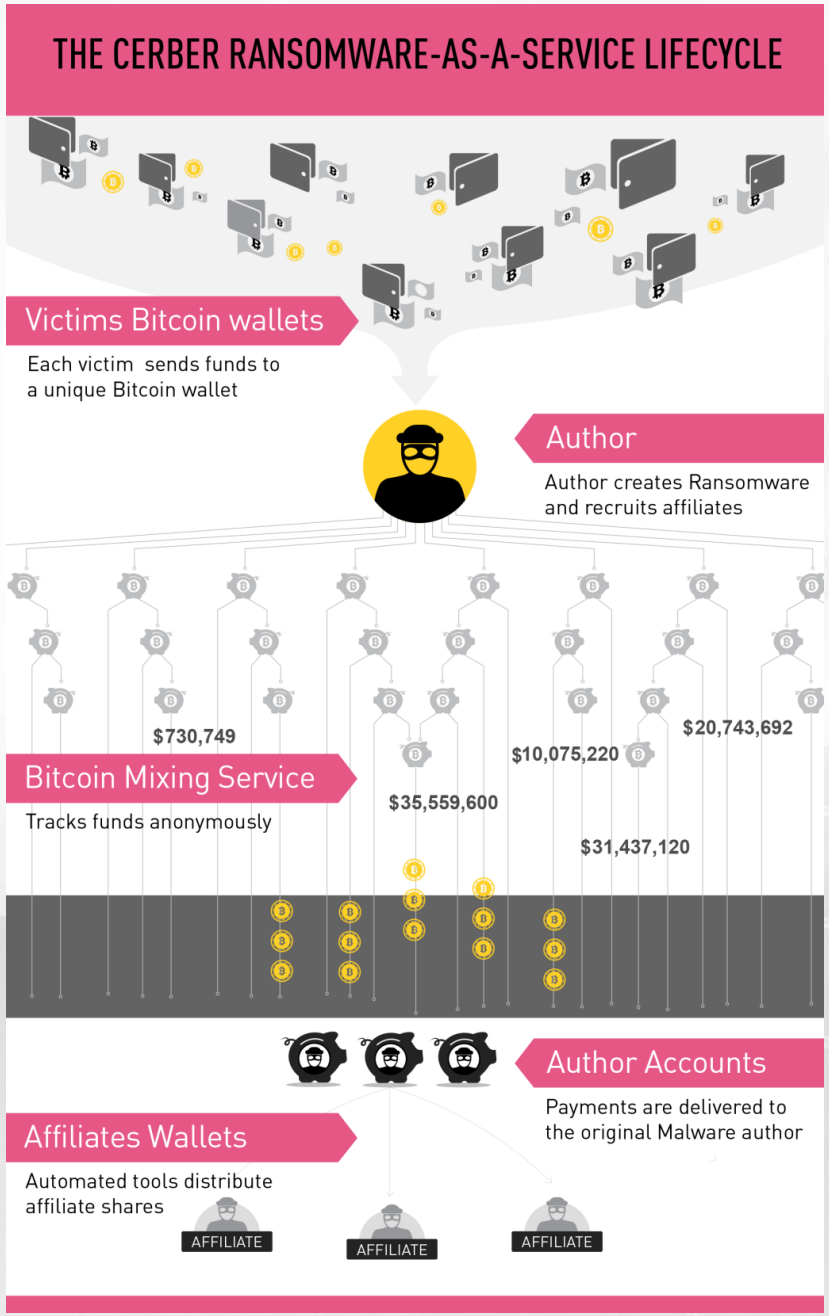
* CRV - Conversion Rate (Number of payments / Visit Landing)
* CRI - Conversion Rate (Number of payments / Installs)

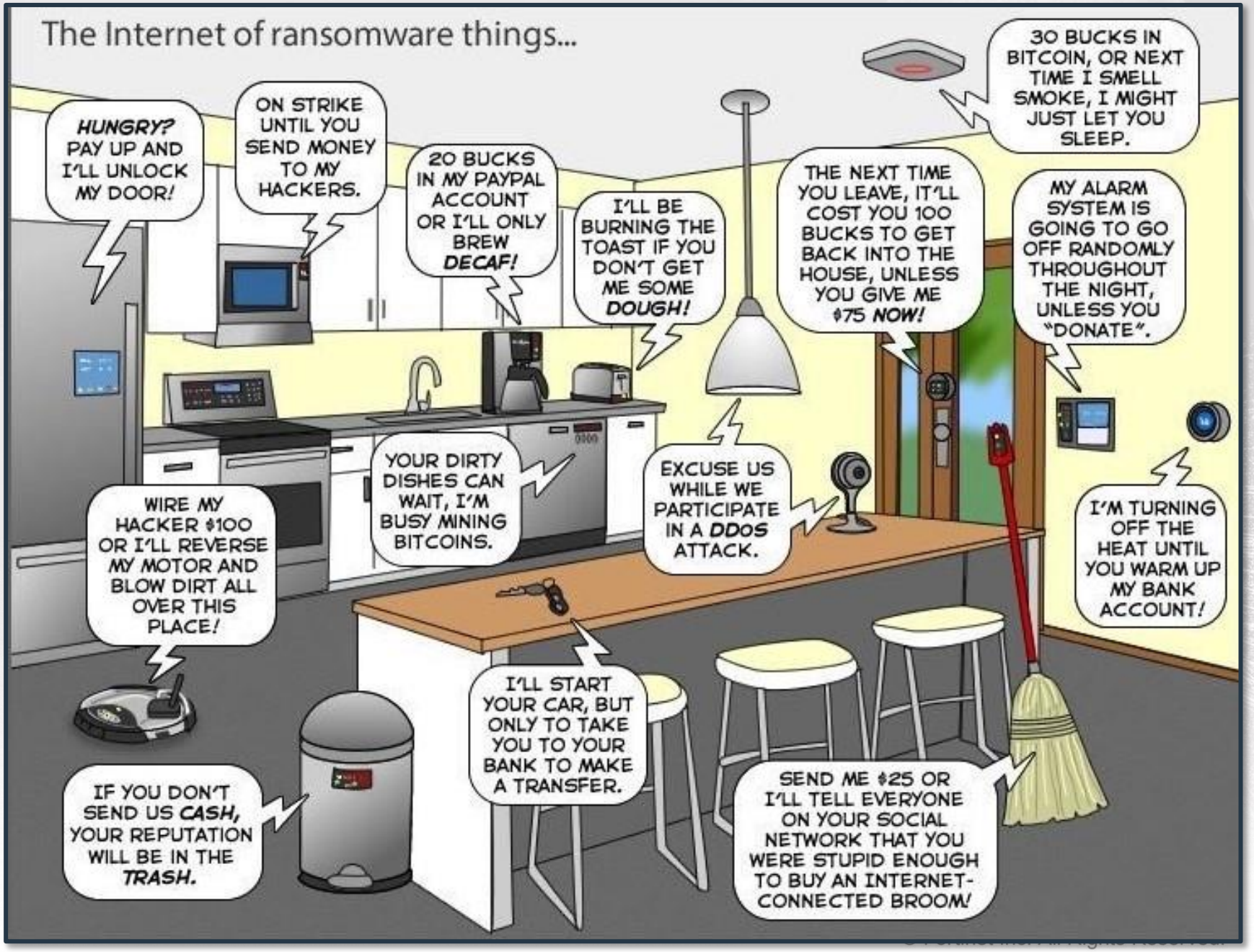
Support

- Pro Opfer wird ein eigenes Bitcoin Walltet angelegt
- Opfer werden aufgefordert Bitcoin zu zahlen um die Daten zurück zu bekommen
- Zahlungen werden über Tor ausgeführt

Finanzwesen

- Effektive Zahlungsüberwachung der Bitcoin Wallets
- Das Geld wird über einen Mixing Service (Bitcoin Laundry) abgewickelt
- Nur an den "Author" und dieser verteilt weiter an die Partner
- $195.000 /Monat, $2.3 Millionen /Jahr




The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

Was können wir tun?

(offline)
Backup

Rechte verwalten und Zugänge kontrollieren,
aktive Inhalte (wie z.B. Macros) deaktivieren

Kritische Daten und Prozesse
erkennen und kennen

Patch
(IPS)

Eine Security Strategie haben
und diese auch durchführen

Schulungen
Anwendertrainings

Wissen wo ich Decryptors finde

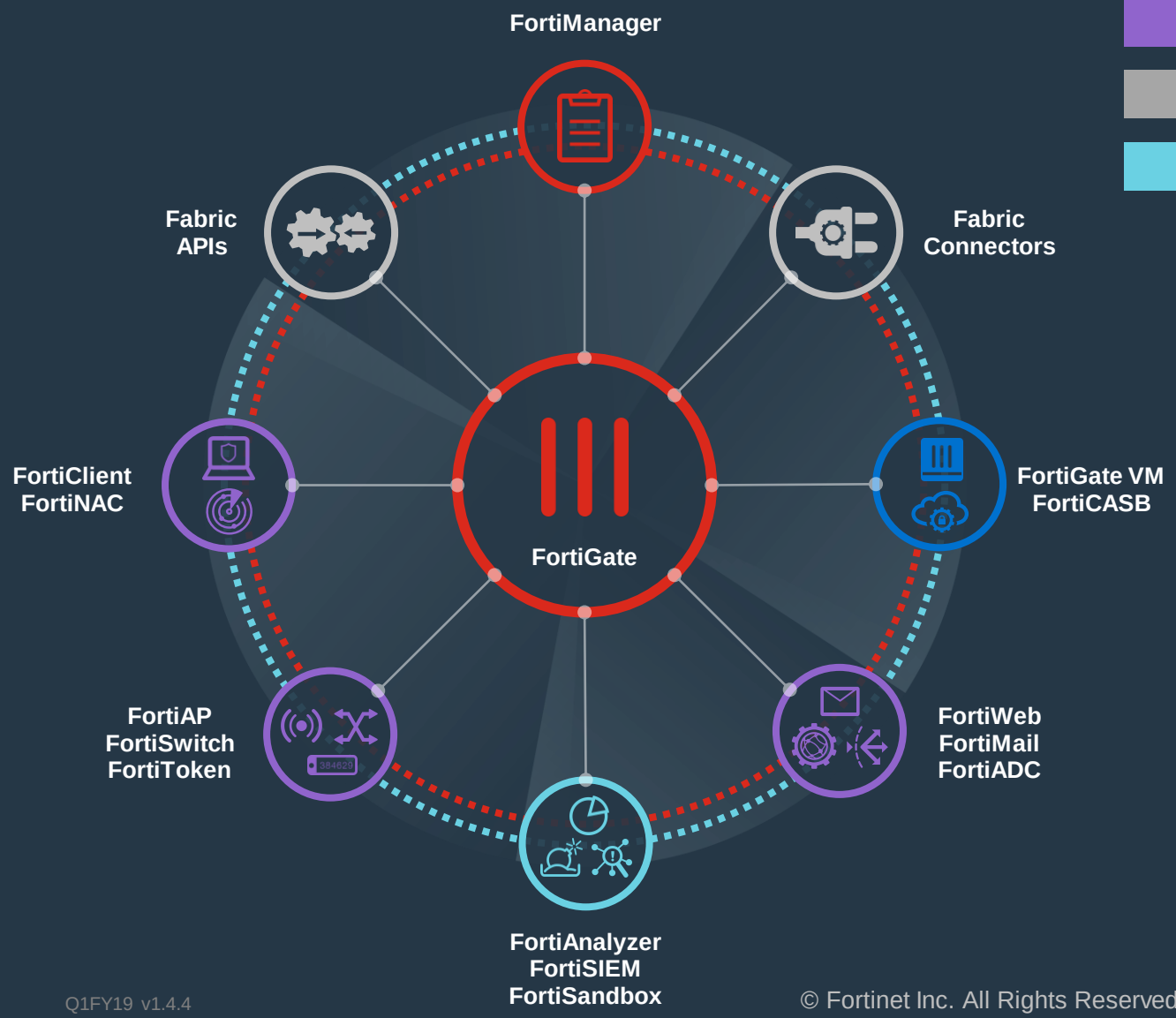
Eine Kette ist nur so stark wie ihr schwächstes Glied

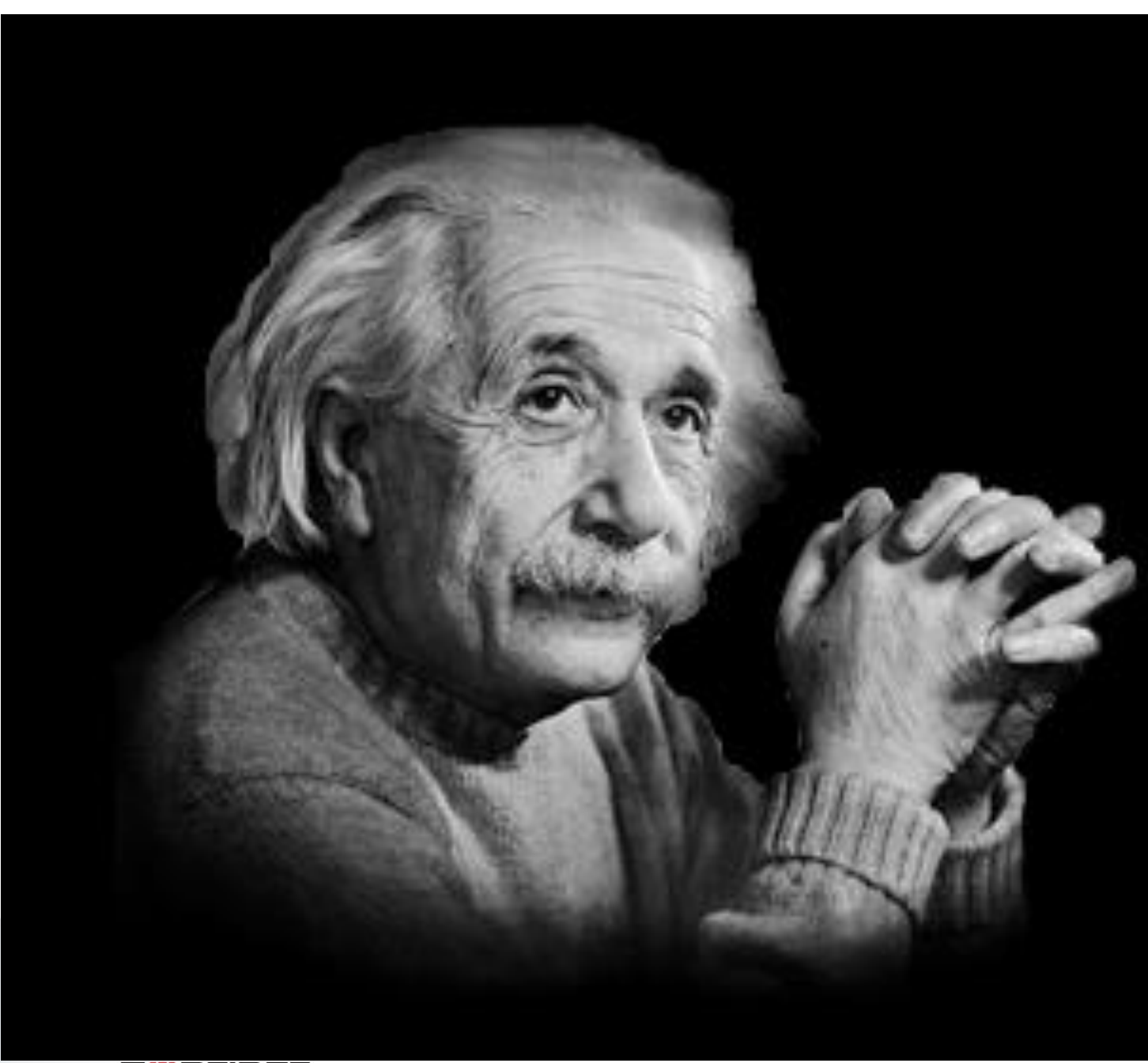
Fortinet Security Fabric

BROAD
Visibility of the entire digital attack surface

INTEGRATED
AI-driven breach prevention across devices, networks, and applications

AUTOMATED
Operations, orchestration, and response





Probleme kann man niemals mit derselben Denkweise lösen, durch die sie entstanden sind.

Zitat: Albert Einstein

Vielen Dank


FORTINET