



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.).







Cyber Crime – Die Gewinne sprudeln!



DIEBE

WE HAVE YOUR
CREDIT CARD IF YOU
DON'T PAY US
1000 DOLLARS
BY PAYPAL WE
WILL DELETE
YOUR TWITTER
ACCOUNT.



ERPRESSER



DATA BREACH



RANSOMWARE



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 끝에 내린 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 풀어서겠다.

Anatomie einer Ransom Attacke

≈ 15 Minuten

Exploitation and Infection

Social Engineering, Phishing und menschliche Fehler sind die primären Mechanismen um ein System 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”

Logout

The virus kSgBjrOmDX has been created: [Download](#)

Create a virus

Ransom - \$

Notes

Captcha

[Create](#)

| Ransom | Infections | Payments | Profit | Notes | Actions |
|--------|------------|----------|---------|-------|--------------------------|
| | 0 | 0 | 0.00 \$ | | Download |
| | 6 | 0 | 0.00 \$ | | Download |

Page 2 →

“Targets as a Service”

Google

email listen|

- e mail listen
- e mail listen kaufen
- e mail listen mieten
- e mail listen uni ulm
- e mail listen aufbau
- e mail listen download
- e mail listener plugin openfire
- e mail listen verwalten
- e mail listener php
- e mail listen erstellen

Weitere Informationen

Unangemessene Vervollständigungen melden

[Email List - Start Free Today - constantcontact.com](#)

[Anzeige](#) [www.constantcontact.com/de](#)

Create Professional Emails That Bring Customers to Your Doors.

[B2B Firmen-Adressen kaufen - aktuell und geprüft - firmen-adressen.biz](#)

[Anzeige](#) [www.firmen-adressen.biz/](#)

TOP Qualitäts Adressen für erfolgreiches Marketing. Jetzt kostenlos anfragen.

Datenaudit · Adressen Telefonmarketing

Dienstleistungen: Firmenadressen, Telefonmarketing Adressen, B2B E-Mail Adressen, Haushaltsa...

[Daten für Telemarketing](#) · [Firmenadressen](#) · [E-Mail Adressen B2B](#) · [Haushaltsadressen](#)

[Tagesaktuelle E-Mail-Adressen? - Kaufen Sie direkt beim Profi.](#)

[Anzeige](#) [www.address-publisher.de/email-adressen](#) 0791 20238990

Effektive Neukundengewinnung im B2B -Bereich - mit topaktuellen E-Mail-Adressen.

aktuelles Adressmaterial · günstige Preise · persönlicher Service · über 10 Jahre Erfahrung

Vorteile: Individuelle Zielgruppenanalyse, Persönliches Commitment, Exzellente Branchenkenntnis...

[AdressMonster Premiumadressen - B2B&StartUp Adressen ab 0,12€](#)

[Anzeige](#) [www.adressmonster.de/](#)

Handgeprüft und Top-Aktuell. Branchenadressen inkl. Tel., Email, Webadressen.

Ich verkaufe Emails von bester Qualität



Vollansicht



Von: Finn Walter

01.01.2018 um 23:33 Uhr

Hallo,

Ich verkaufe Emails!

@gmx.de (12,4 Millionen)

@web.de (8,2 Millionen)

@gmx.net (2,4 Millionen)

@t-online.de (8,9 Millionen)

@freenet.de (3,4 Millionen)

Alle Emails sind gecheckt und aktiv (Stand Dezember 2017)

Kosten pro 1 Million Emails 500 Euro

Falls Sie alle kaufen möchten können wir ueber den Preis verhandeln!

Ich akzeptiere als Zahlungsmittel nur Bitcoin

Falls Sie interessiert sind kontaktieren Sie mich über Jabber!

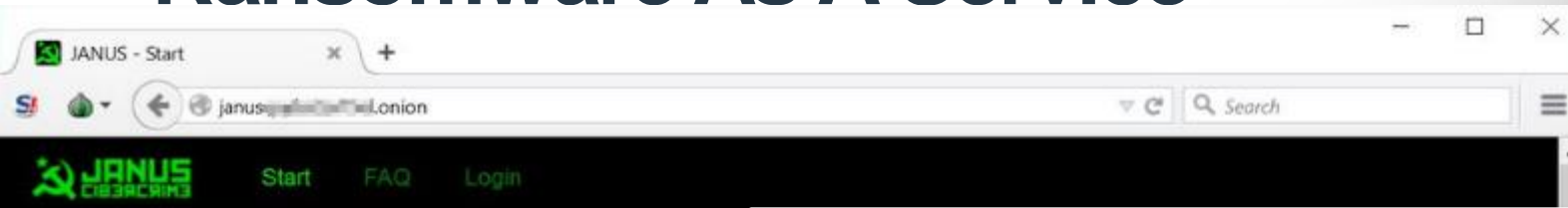
Meine Jabber ID:

manux@jabber.ru

oder

manux@xmpp.jp

Ransomware As A Service



PROFIT FROM P

HIGH INFECTION RATES

PETYA comes bundled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.

PETYA does a low level encryption of the disk, which is a completely new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.

Registration (Step 1)

First you have to enter a bitcoin address and it's public key. All payments are made on multisig addresses generated from your public key and a public key from us. **WARNING:** It is highly recommended to store the WIF key in a secure place. No one can access your generated bitcoins if you loose that key!

For more informations please check our FAQ, read <https://en.bitcoin.it/wiki/Multisignature> or ask our Support for help.

| Volume/Week | Share |
|-------------|-------|
| <5 BTC | 25% |
| <25 BTC | 50% |
| <125 BTC | 75% |
| >=125 BTC | 85% |

Address (Share)

Public key (Share)

Enable client-side generation

Private key (WIF key)

This page uses javascript to generate your address within your browser, this means we never receive your private key, this can be independently verified by reviewing the source code. You can even [download](#) the script and host yourself or run it offline.

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**

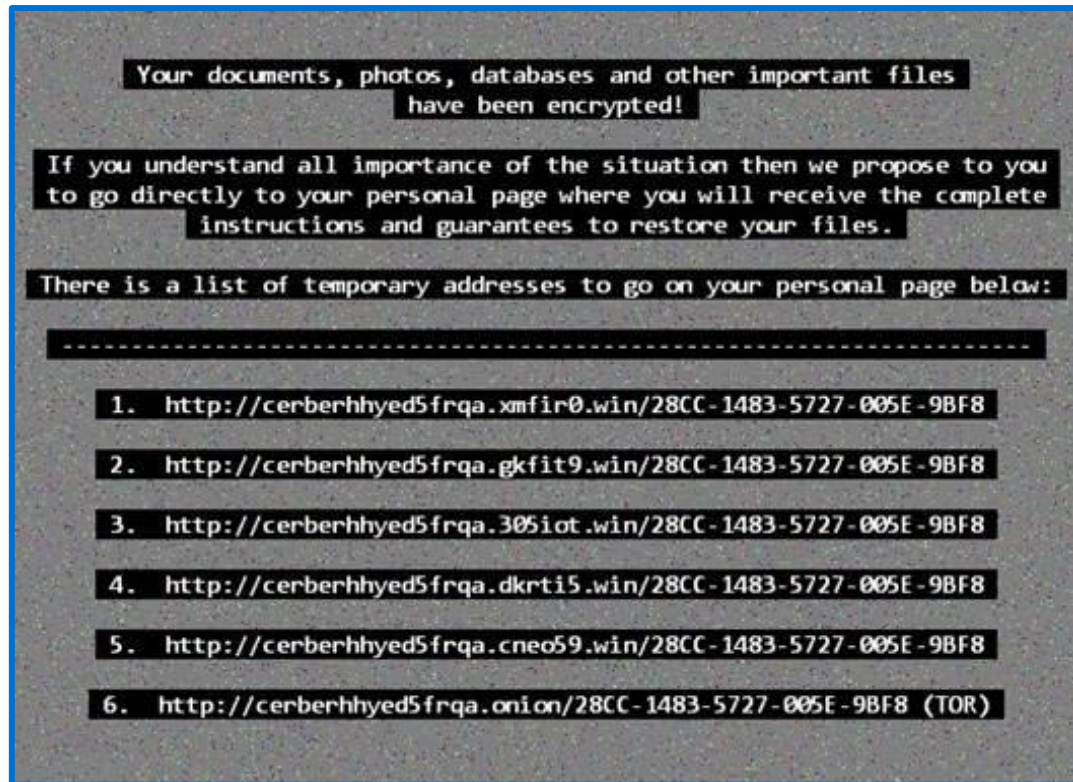
Ransomware Business

Benötigt für ein erfolgreiches Business:

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

Cerber: erfolgreiche Ransomware in der RaaS Industrie

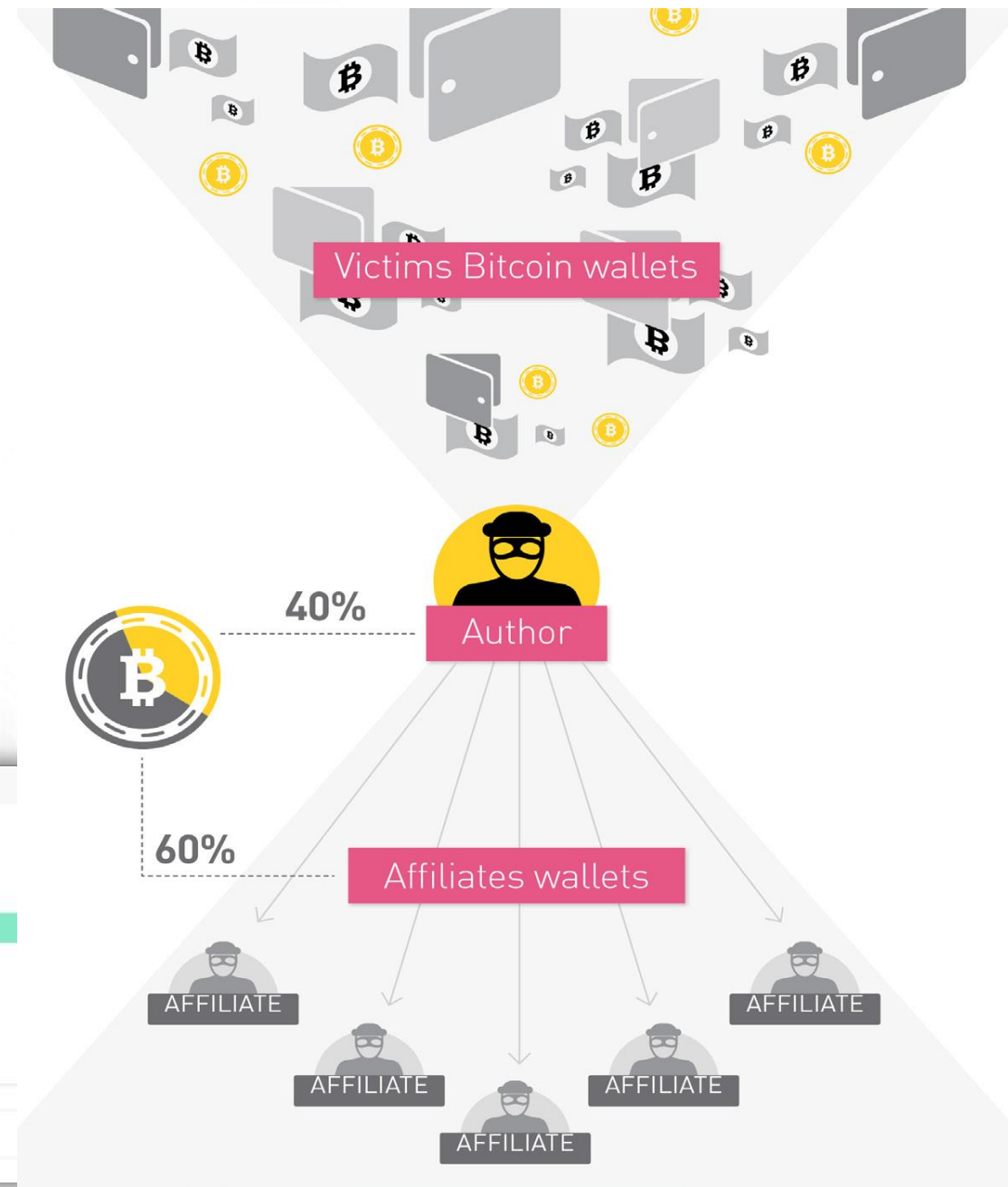
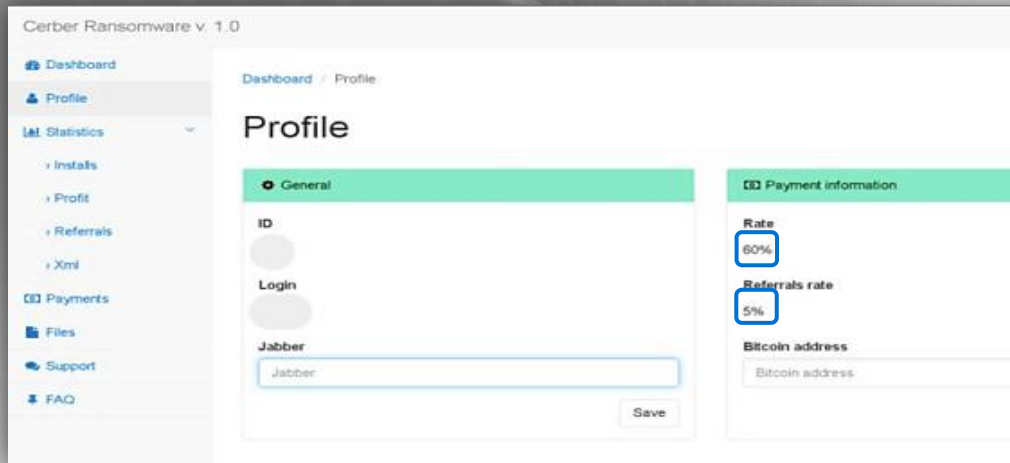
Produkt/Lösung: Cerber



- 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

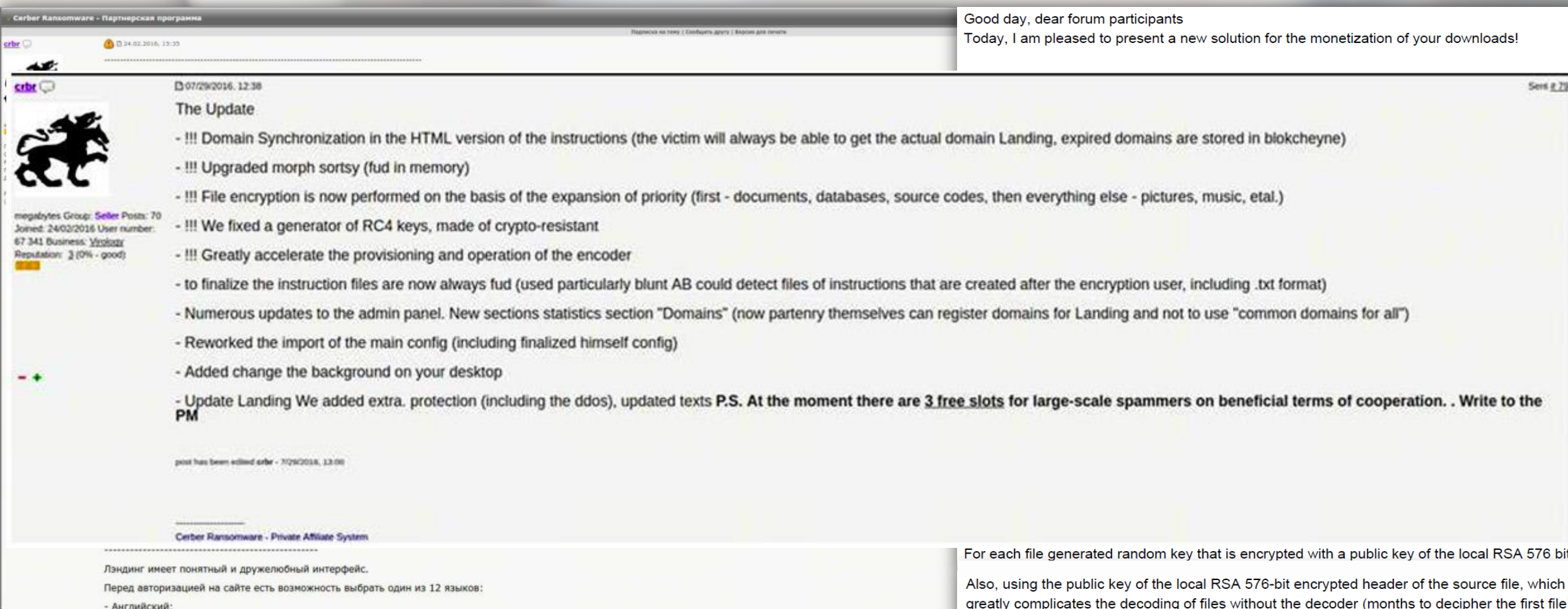


Marketing

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!



Cerber Ransomware - Партнерская программа

crbt 24.02.2016, 13:33

07/29/2016, 12:38

The Update

- !!! Domain Synchronization in the HTML version of the instructions (the victim will always be able to get the actual domain Landing, expired domains are stored in blokcheyne)
- !!! Upgraded morph sorts (fud in memory)
- !!! File encryption is now performed on the basis of the expansion of priority (first - documents, databases, source codes, then everything else - pictures, music, etal.)
- !!! We fixed a generator of RC4 keys, made of crypto-resistant
- !!! Greatly accelerate the provisioning and operation of the encoder
- to finalize the instruction files are now always fud (used particularly blunt AB could detect files of instructions that are created after the encryption user, including .txt format)
- Numerous updates to the admin panel. New sections statistics section "Domains" (now partenry themselves can register domains for Landing and not to use "common domains for all")
- Reworked the import of the main config (including finalized himself config)
- Added change the background on your desktop
- Update Landing We added extra. protection (including the ddos), updated texts **P.S. At the moment there are 3 free slots for large-scale spammers on beneficial terms of cooperation. . Write to the PM**

post has been edited crbt - 07/29/2016, 13:00

Cerber Ransomware - Private Affiliate System

Лэндинг имеет понятный и дружелюбный интерфейс.
Перед авторизацией на сайте есть возможность выбрать один из 12 языков:
- Английский;

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

Cerber Ransomware v. 1.0

Dashboard / Files / Price setting

Price setting for SubID 1

Price setting

Count files Price Price after 5 days

BTC USD

| Count files | Price | Price after 5 days |
|----------------|----------------------|-----------------------|
| Default | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 1-500 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 500-1000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 1000-2000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 2000-5000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 5000-10000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 10000-20000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 20000-50000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 50000-100000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 100000-200000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 200000-500000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 500000-1000000 | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |
| 1000000+* | B 1.2500 \$ 531.79 | B 2.5000 \$ 1063.97 |

Save

benötigt 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: 9292

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 | 328 | 7 | 2.15% | 5.19% | 4.3481 (1943.45) |
| 4/21/2016 | 336 | 204 | 45 | 164 | 374 | 8 | 1.80% | 1.79% | 3.6576 (1634.79) |
| 4/20/2016 | 145 | 63 | 22 | 64 | 443 | 5 | 1.13% | 3.45% | 4.0008 (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 | 658 | 13 | 1.98% | 7.60% | 13.6265 (6090.49) |
| 4/17/2016 | 94 | 40 | 6 | 29 | 200 | 3 | 1.50% | 3.19% | 1.7589 (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% | 1.76% | 14.0076 (6260.85) |
| 4/14/2016 | 780 | 606 | 32 | 434 | 535 | 7 | 1.31% | 0.92% | 5.2572 (2349.78) |
| 4/13/2016 | 475 | 354 | 30 | 280 | 512 | 12 | 2.34% | 2.53% | 7.1005 (3173.63) |
| 4/12/2016 | 472 | 317 | 44 | 285 | 541 | 15 | 2.77% | 3.18% | 9.7783 (4389.61) |
| 4/11/2016 | 797 | 571 | 52 | 485 | 701 | 15 | 2.14% | 1.86% | 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 | 2185 | 344 | 1585 | 643 | 16 | 2.49% | 0.48% | 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 (797.08) |
| 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% | 7.6084 (3480.83) |
| 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 | 3.26% | 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


How to get «Cerber Decryptor»?

1. Create a Bitcoin Wallet (we recommend [Blockchain.info](#))

 CERBER DECRYPTOR

Wähle deine Sprache

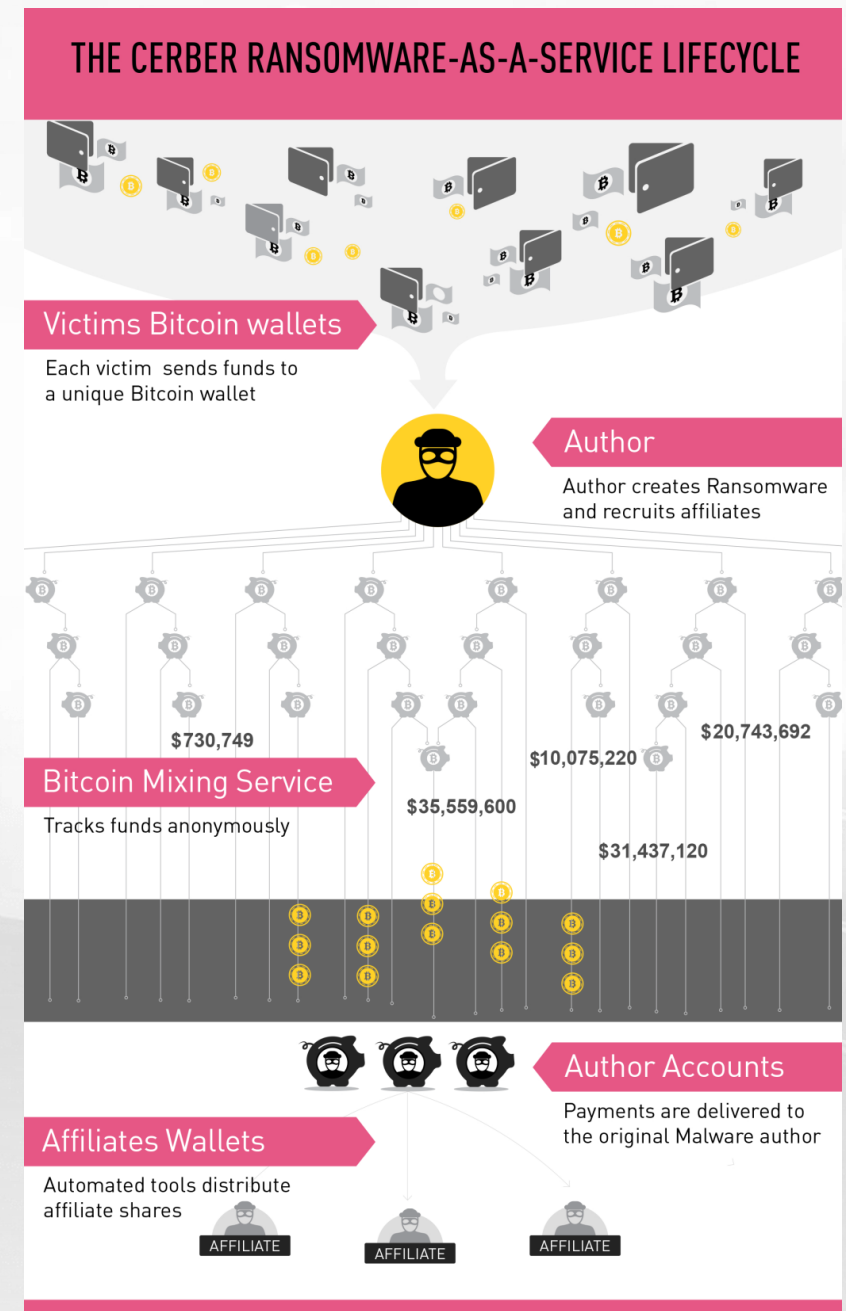
| | | |
|---|---|--|
|  English |  Deutsch |  Español |
|  Français |  中文 |  日本語 |
|  Português |  Polski |  Italiano |
|  Türkçe |  العربية |  Nederlands |

2. Send  1.000 to the following Bitcoin address:

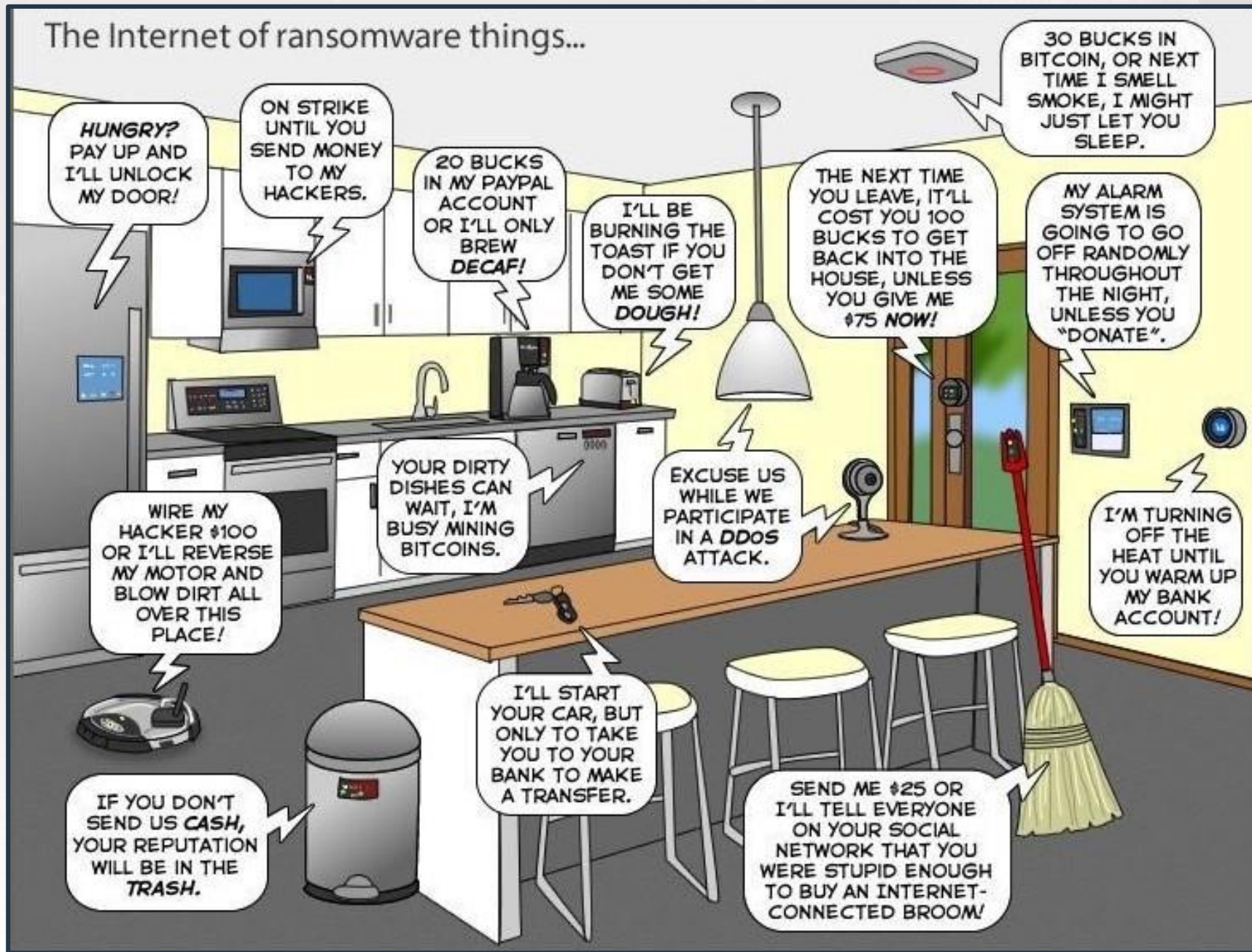
18hkSa5bS3c2LjQ3yUHNUaiCwi6gWXtZkX

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...



Was können wir tun?

(offline)
Backup



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



Office

Kritische Daten und Prozesse
erkennen und kennen



Patch
(IPS)



Eine Security Strategie haben
und diese auch durchführen



Schulungen
Anwendertrainings



Wissen wo ich Decryptors finde

NO MORE RANSOM!

Eine Kette ist nur so stark wie ihr schwächstes Glied



WARNUNG
VIRUS
MALWARE
SPYWARE

Fortinet Security Fabric

- Network Security
- Multi-Cloud Security
- Device, Access, and Application Security
- Open Ecosystem
- Security Operations

BROAD

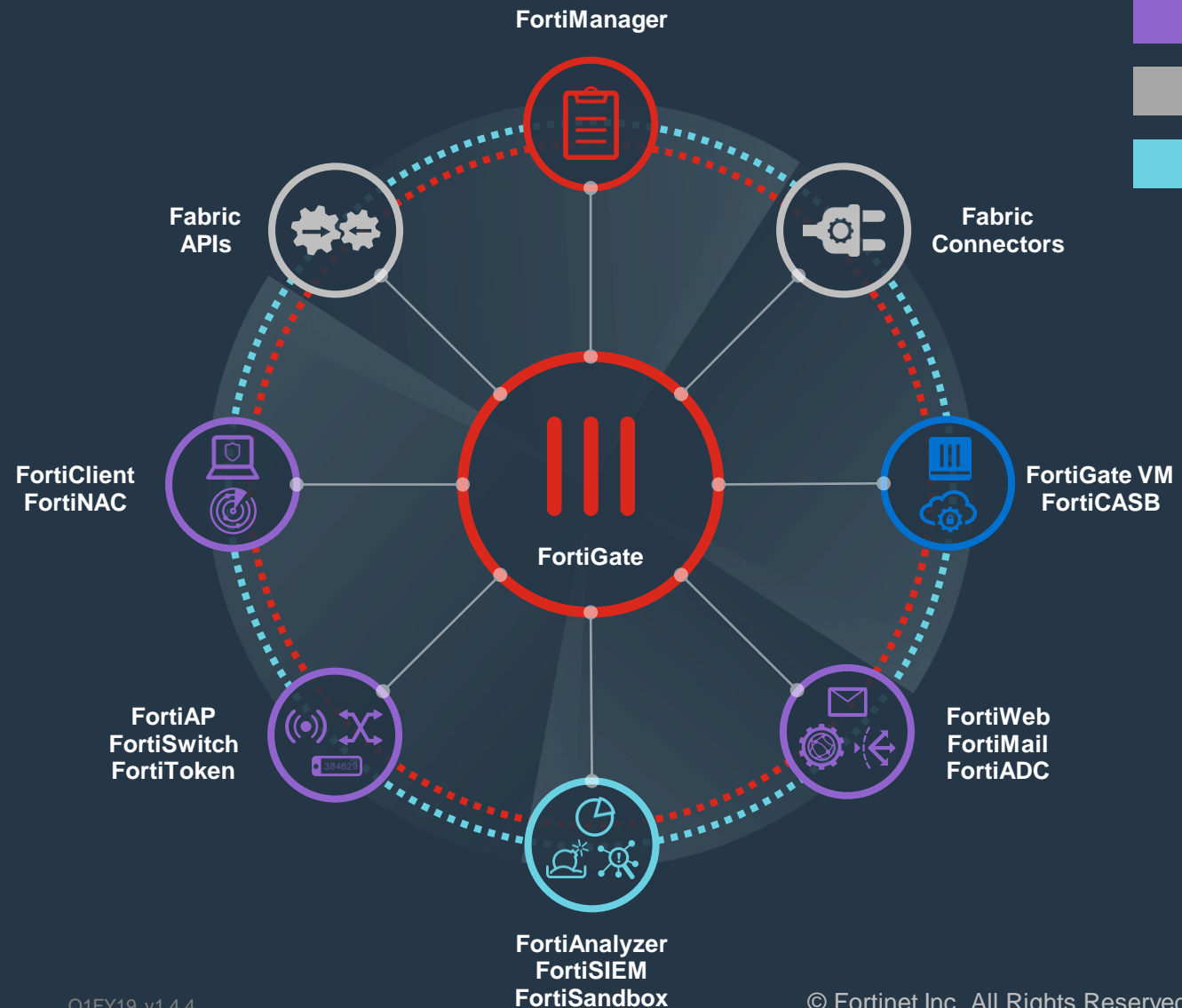
Visibility of the entire digital attack surface

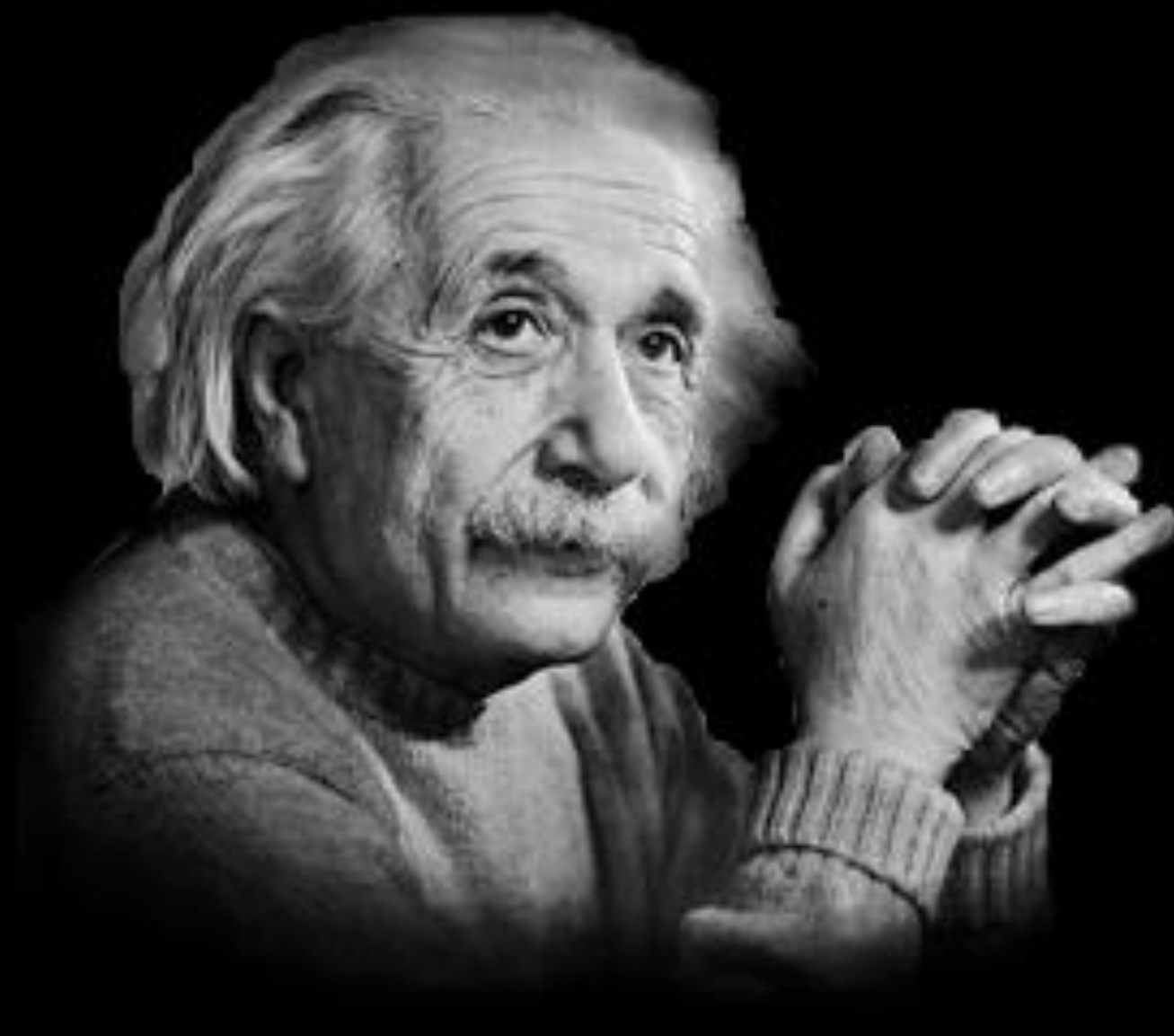
INTEGRATED

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®