



RANSOMWARE AS A SERVICE - SCHADSOFTWARE AUS SOFTWAREFABRIKEN

KNF-KONGRESS 2022

ROLAND WAGNER

ROLAND@DATEVNET.DE

Abfahrt **Linie** **Ziel** **Gleis**

Zeit	Über	Nach	Gleis
22:10 RB81	Flöha - Pockau-Lengefeld	Olbernhau	8
22:30 RB30	Flöha - Freiberg - Fahrt heute	Hbf	11
22:31 RB30	Hohenstein	(S) Hbf	10
22:36 RB80	Flöha - Zsch...	g-B. Süd	8
22:36 RB45	irt heute von	Hbf	9
22:44 RE6	Geithain - B...	Hbf	5
22:45 RB89	Einsiedel - Thalheim (Erzgeb)	Aue (Sachs)	14
23:30 RB30	Flöha - Freiberg (Sachs) - Tharandt Fahrt heute von Gleis 11	Dresden Hbf	11

Oops, your files have been encrypted!

Bitte bezahlen Sie mit Bitcoin. Ihre Dateien sind verschlüsselt und können nur durch die Zahlung eines Lösegelds wiederhergestellt werden. Wenn Sie die Zahlung nicht leisten, werden Ihre Dateien dauerhaft gelöscht. Für weitere Informationen besuchen Sie die Website www.bitcoin.com.

Handelt sich um ein Bitcoin-Adressen?

Bitcoin

Check Payment

Decrypt

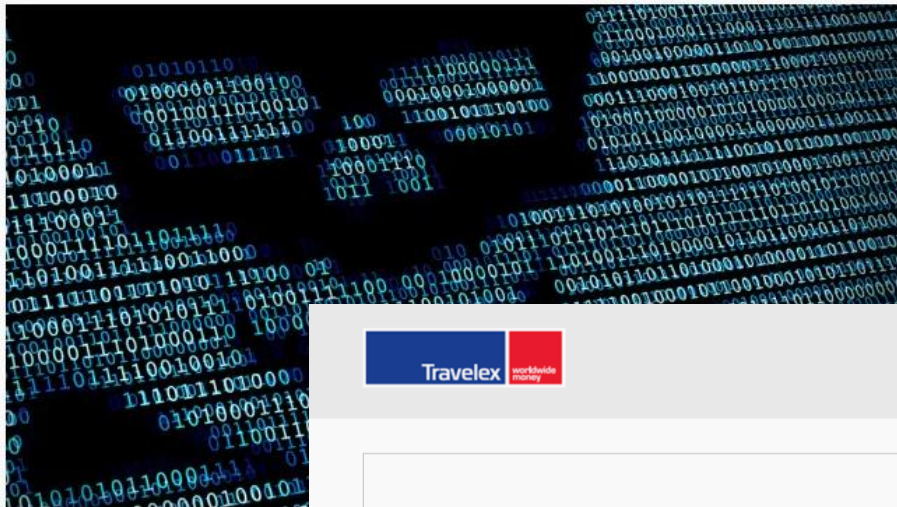
BMG | MIS

CVAG

Frankfurt City Officials Shut Down IT Network Over Malware

Dominique Adams

20 December 2019, 04.02pm



The financial hub h systems following

Travelex Ransomware Attack Enters Its Third Week



FRANKFURT, DARMSTADT, MAINZ

Stadtwerke und ÖPNV mit Ransomware angegriffen

Ein IT-Dienstleister mehrerer Energieversorger sowie Betreiber des öffentlichen Nahverkehrs wurde mit einer Ransomware angegriffen. Die Ermittlungen dauern an.

[in Pocket speichern](#) [merken](#) [teilen](#)

14. Juni 2022, 14:03 Uhr, Moritz Tremmel/dpa

BREACH OF THE MONTH


Colonial Pipeline
WORST RANSOMWARE ATTACK EVER

(Bild: Mohamed Hassan/Pixabay)

This website will be back online soon!

This website is temporarily unavailable while we make upgrades to improve our service to you.

We are sorry for any inconvenience and thank you for your patience.

Thank you for using Travelex!

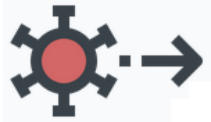
Travelex UK Limited - Registered Number 01985596. Registered Office - 65 Kingsway, London WC2B 6TD.

travelex.com?r=0cHM6Ly93d3cu29vZ2xLmRlLW&guce_referrer_sig=AQAAAJzgKC1N1bNDjYnMi6nT9lVwxz_r748BEbvYUqg-
t5_khCoNQCR5OatKETldZUCIdyNOpDwMQUVWw5dfx6TQhDzTG-qjW_X400SiELGDUe

WAS IST „RANSOMWARE“

„ransom“ = Lösegeld „ware“ (Software / Hardware)

WIE FUNKTIONIERT „RANSOMWARE“ ?



- Mail-Attach
- Drive-By-Download
- Schwachstellen



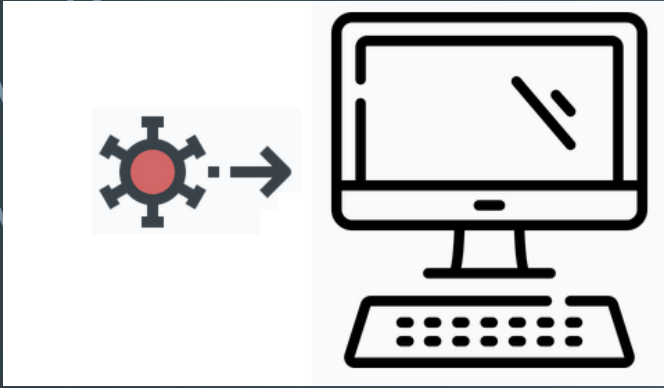
HTTPS, IRC, Tunnel
(SSH, DNS, ICMP) zu C&C-Server



- automatisiert
- manuell
- IBAN, Kreditkarten, Keys, Wallet, persönliche Daten ...
- Kommunikation zu C&C-Server



Autostart, Scheduler, Service,
Plugins, (DLL-) Injection, ...
(„Bekannte Methoden“)



Viren



Trojaner

Würmer



Botnetz



Schadsoftware

„SPEZIALFUNKTION“

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

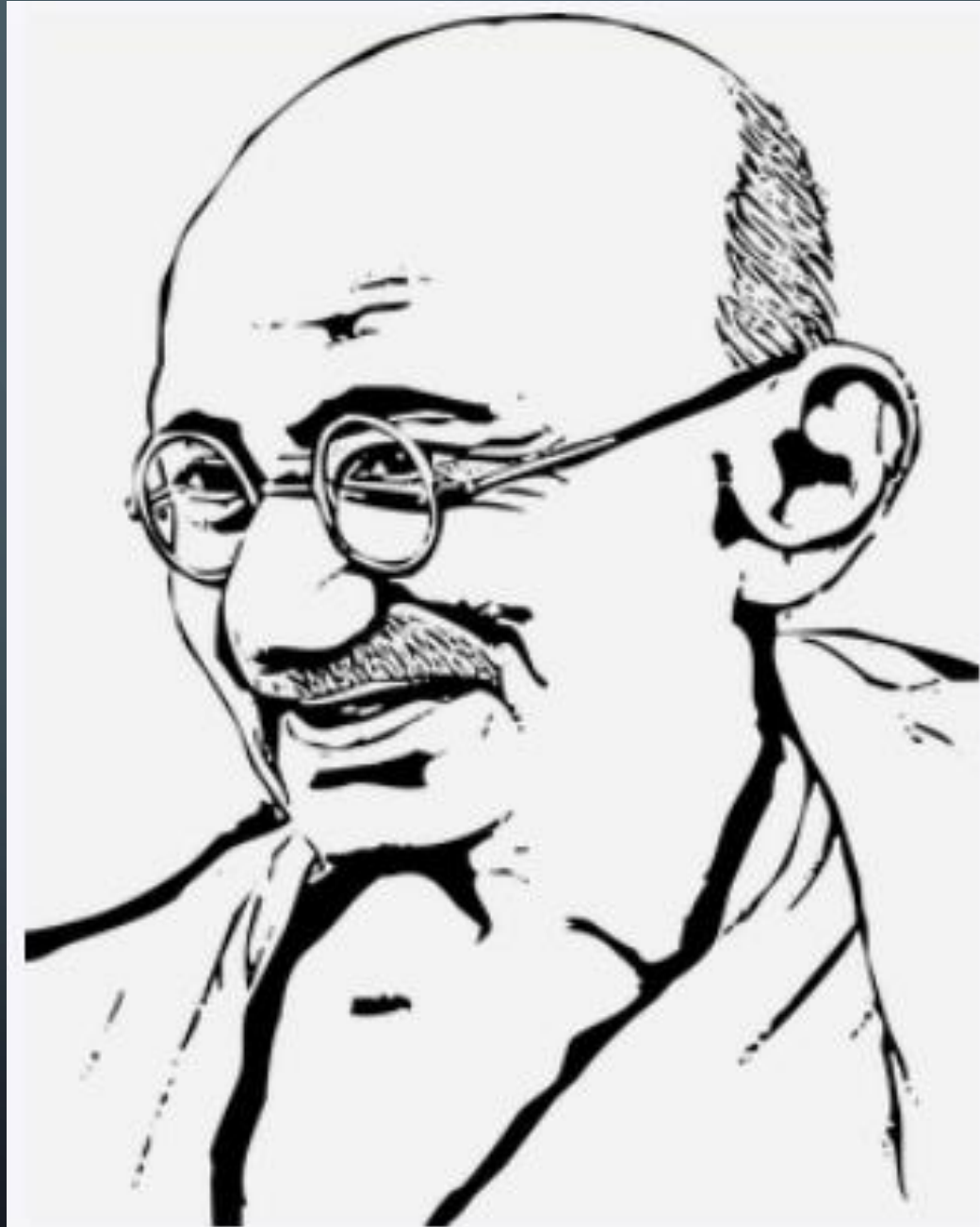
Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

 **Send \$300 worth of bitcoin to this address:**
115p7UMMngoJ1pMvKpHijcRdfJNXj6LrLn

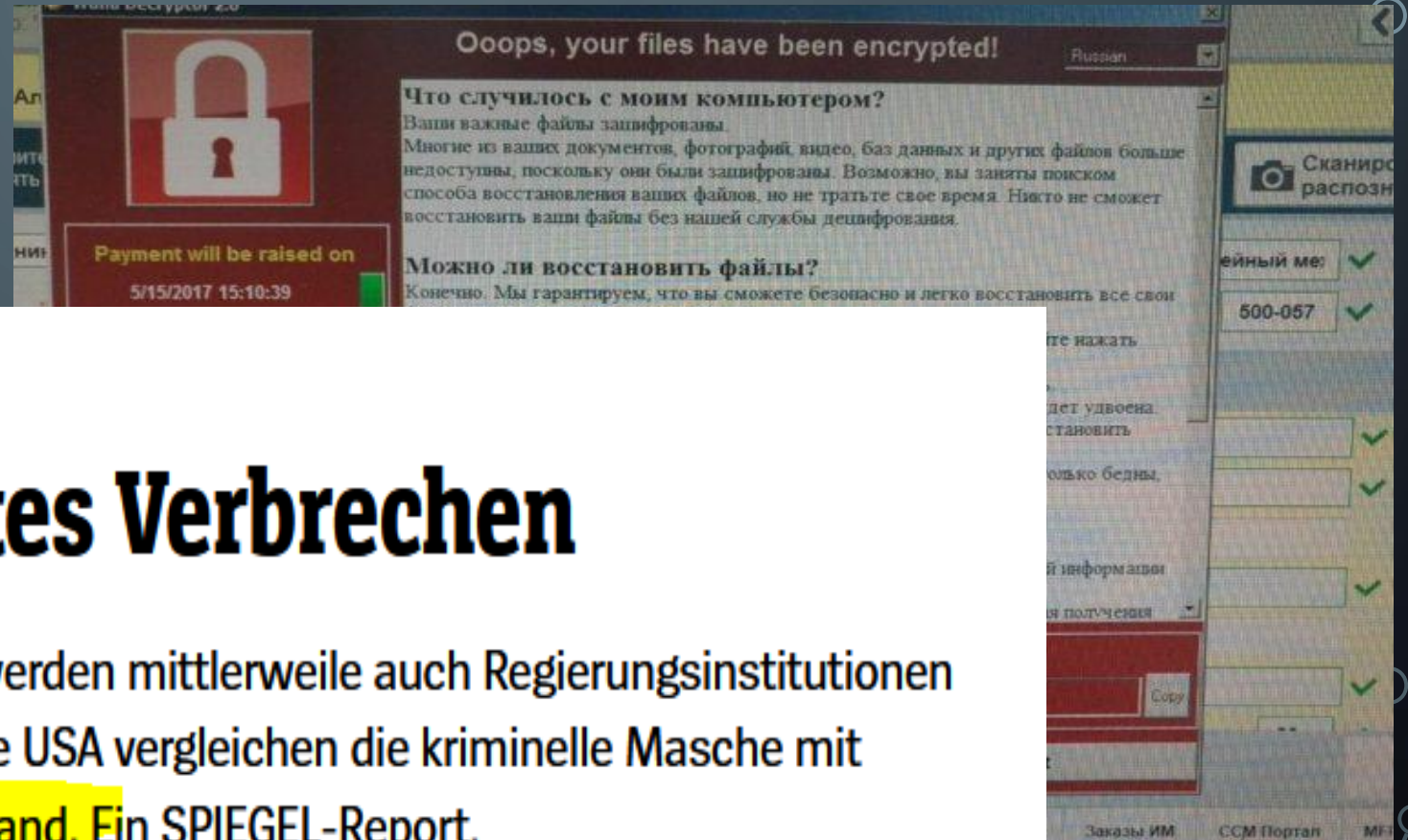
WER MACHT DENN SOWAS?



WER MACHT DENN SOWAS?



WER MACHT DENN SOWAS?



Die Erpressungstrojaner russischer Hacker

6+ Ein nahezu perfektes Verbrechen

Neben Unternehmen und deren Kunden werden mittlerweile auch Regierungsinstitutionen zum Opfer von Ransomware-Angriffen. Die USA vergleichen die kriminelle Masche mit Terrorismus. Die Spur führt oft nach Russland. Ein SPIEGEL-Report.

WER MACHT DENN SOWAS? RAAS (RANSOMWARE AS A SERVICE)

- „Crimeware-Kits“ / „Rent an Attack“
- Spezialisten für jeden Bereich
- Kein IT-Wissen notwendig
- Professionelle Software-Entwicklung (9to5)
- Professioneller Service (Chat, 14 Tage: Key kostenlos, ...)
- Erpressung: Target dependent amount !

WER MACHT DENN SOWAS? RAAS (RANSOMWARE AS A SERVICE)

DarkSide:

“... our goal is to make money, and not creating problems for society...”

FunFact: Juni 2019: „GandCrab geht in Rente“

GandCrab seit Januar 2018; mehr als 2 Milliarden \$

GEGENMAßNAHMEN

- Backup, Backup, Backup
- Patchen, patchen, patchen
- Virenschutz
- Firewall / Content-Filter
- Proxy
- Awareness

be prepared

GEGENMAßNAHMEN

- Internet trennen / Segmente trennen
- Rechner ausschalten
- Neustart nutzlos! (persistence)
- von USB booten
- **Kill Switch**
- **„Root cause“ finden!**



**DON'T
PANIC**

GEGENMAßNAHMEN

- „Bezahlen oder nicht bezahlen, das ist hier die Frage“
„Nicht bezahlen !!!“
bezahlt? „Schlüssel oder nicht Schlüssel, das ist...“
- Temporäre Dateien
- Schlüssel extrahieren
- Teilverschlüsselung
- „Sicheres“ Backup verwenden



GEGENMAßNAHMEN



No More Ransomware & bleib-Virenfrei


NO MORE RANSOM

bleib-Virenfrei

Achtung double extortion (Multiple extortion) !

GEGENMAßNAHMEN - PRIVAT

- Backup, Backup, Backup
- Patchen, patchen, patchen
- Nur vertrauenswürdige Software
- Virenschutz
- Administrator? → User !
- Keine persönlichen Daten
- Keine unbekannten USB-Sticks

GEGENMAßNAHMEN - PRIVAT

- Lokale Firewall
- (externe Firewall / Content-Filter) -> pfSense (auch virtuell)
- (Proxy) -> pfSense , squid (auch virtuell)
- Awareness
- Anzeige erstatten!



Stopp, nicht nachmachen

Infraud: US-Justiz gelingt Schlag gegen Cybercrime-Ring

Ukrainische Cyberpolizei verhaftet Ransomware-Bande Cl0p

Behörden der Ukraine und Südkoreas feiern einen Schlag gegen die Ransomware-Bande Cl0p in Kiew. 6 Personen sind verhaftet, Bargeld, Kfz, Computer beschlagnahmt.

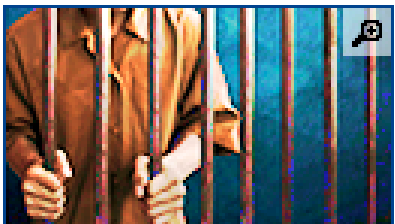
RANSOMWARE

Revil-Mitglieder verhaftet

Ermittlern ist ein Schlag gegen die [Ransomware](#)-Gruppe Revil gelungen. Diese hatte unter anderem den IT-Dienstleister Kaseya gehackt.

AUSGESCHALTET: GLOBALE RANSOMWARE-ERPRESSER ENDLICH GEFASST

LockBit: Russisch-kanadischer Ransomware-Operator festgenommen



Nach jahrelangen Ermittlungen konnten amerikanische Behörden einen Operator der LockBit-Gruppe verhaften. Der russisch-kanadische Bürger Mikhail Vasiliev wurde in Kanada festgenommen und könnte demnächst in die Vereinigten Staaten ausgeliefert werden.

Any
Questions