

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Wie Hacker arbeiten



Liebe KCC-Mitglieder,

Danke für Ihr Interesse an diesen Folien. Der Vortrag lebte vor Allem vom Erzählen. Die Folien sind daher bedingt selbstverklärend (und manchmal gar nicht). Wenn Sie Fragen haben, kontaktieren Sie mich gerne direkt:

tglemser@secuvera.de

+49 7032 9758-15

Ihr Tobias Glemser



- Sitz der Gesellschaft: Stuttgart/Gäufelden
- Gründung: 1. Juli 1982
- Inhabergeführt
- Herstellerunabhängig
- Berater, keine „Consultants“
- IT-Sicherheit seit 1988
- reiner IT-Sicherheitsdienstleister



- **Drei Beratungsfelder**
 - Sicherheitsberatung (BSI-Grundschatz/ISO 27001)
 - Penetrationstests
 - BSI-Prüfstelle (Produktzertifizierungen) 62443 für Industrial Security (TÜV Nord)



- whoami
 - Tobias Glemser
 - 20 Jahre in der Branche
 - BSI-zertifizierter Penetrationstester
 - Autor
 - iX, c't, ...
 - Whitepaper „Projektierung der Sicherheitsüberprüfung von Webanwendungen“
 - OWASP Top10 Übersetzung
 - Engagements: TeleTrust Experte, OWASP German Chapter Lead, Botschafter casayoana



Ausgangslage

SalzburgMilch

Hunderte Coop-Supermärkte in Schweden

Pandemien und Hacker machen bayerischer Wirtschaft am meisten Angst

Welche Risiken machen bayerischen Firmen am meisten Sorgen? Pandemien sind nun auf dem ersten Platz. Doch damit geht nicht automatisch Vorsorge einher.

 Die Folgen eines nicht näher beschriebenen Cyberangriffs auf die Versicherung

Asiatische Axa-Partner von Ransomware getroffen

Teile des Versicherungskonzerns Axa in Asien wurden von Ransomware angegriffen, es soll um 3 Terabyte Daten gehen.

Kenfm.de: Anonymous hackt website des

Aktivisten Ken Jepsen

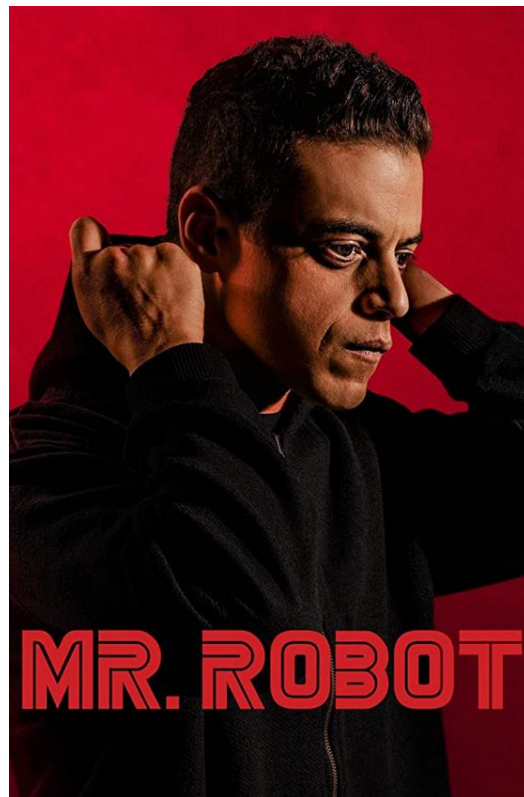
Das Hackerkollektiv hat Zugriff auf kenfm.de erlangt und von dort nach eigenen Angaben 3 GByte Daten kopiert.

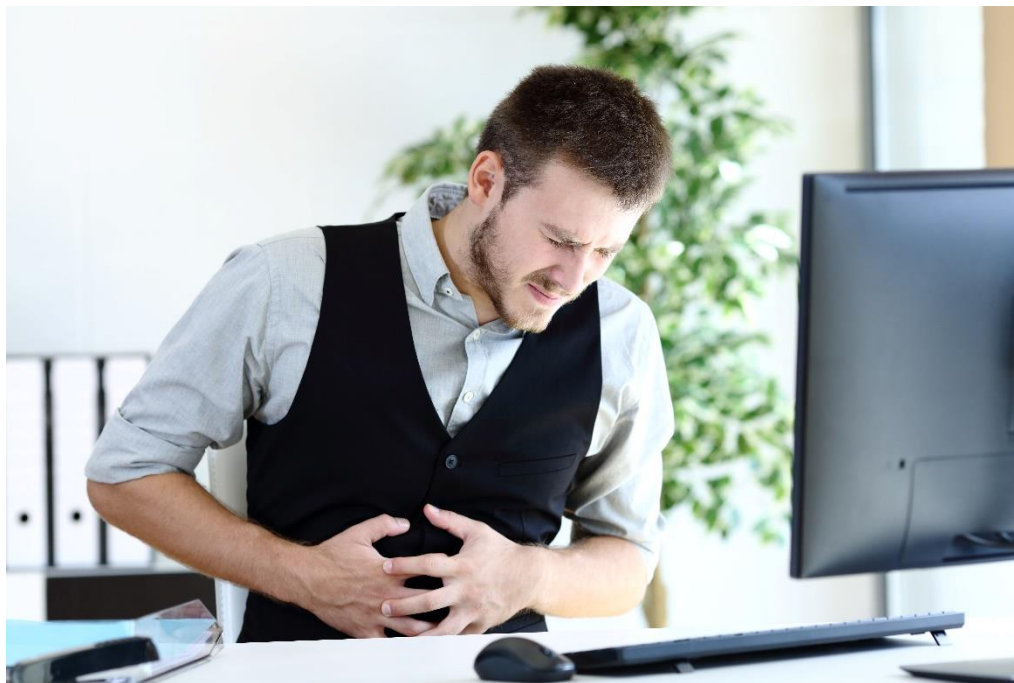
Attack

verangriff
eingestellt

angriffs geworden. In
Ausmaß ist noch nicht

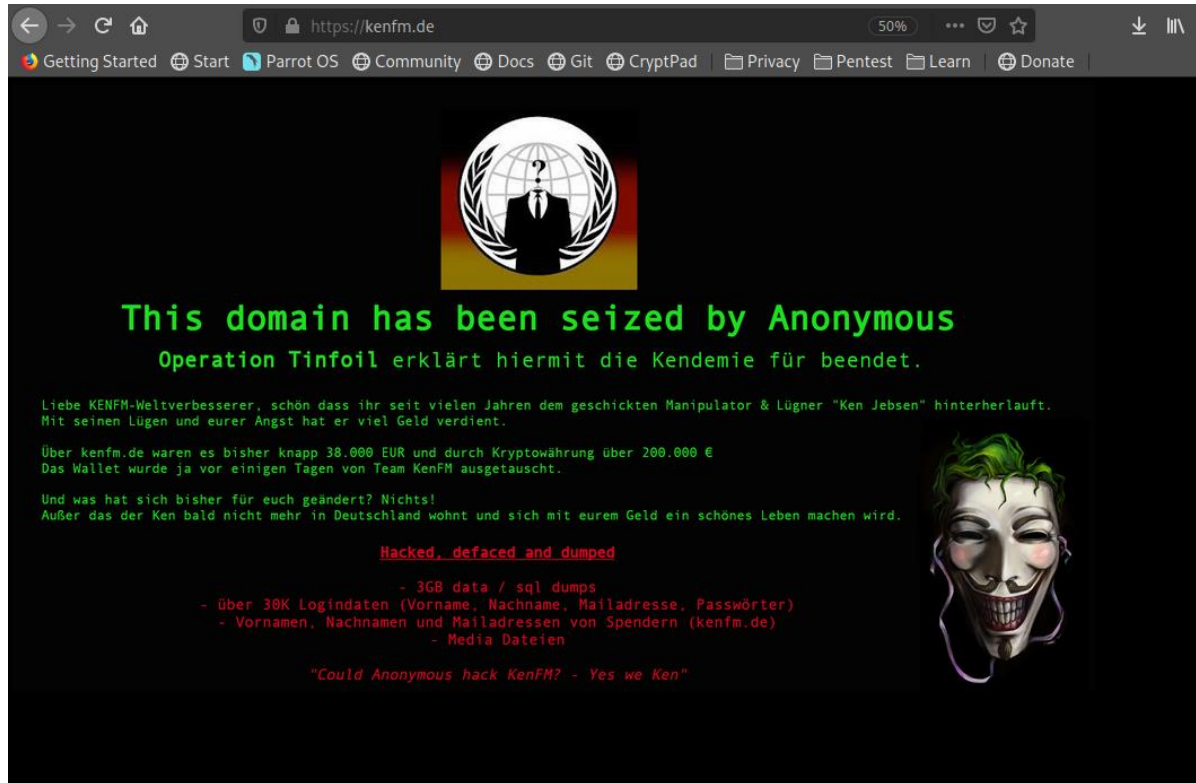






© Antonioguilllem - Adobe Stock

Angriff der Hacker



Kapitel I

Angriff der Profis

Your account is suspended

Your Google Ads account is temporarily suspended for [Circumventing systems](#).

We want to help you regain control of your account as quickly as possible. p>

Here are some steps you can take to make your account secure:

1. Check your computer for malware and viruses with trusted anti-virus software, and remove any suspicious programs or applications.
2. log-in [here](#) to restore your account.

Learn more [about suspended accounts](#).

The Google Ads Team

This email was sent to update you about your Google Ads account.

Google

Google LLC
1600 Amphitheatre Parkway,
Mountain View, CA 94043

Sehr geehrter Kunde,



Dies ist eine letzte Erinnerung, Sie haben eine unvollendete Rückerstattung ...

Die Rückerstattung von 46,25 Euro gilt noch bis zum 24.10.2020

Diese E-Mail informiert Sie darüber, dass der Betrag nach dem Fälligkeitsdatum nicht mehr verfügbar ist und wir später nicht mehr bezahlen können.

- Ziel: Einzelpersonen
- Methode: Phishing mit Link
- Zieldaten: Nutzernamen, Kennwörter

Kapitel II

Angriff der Profis

Absender



01.06.2021 23:11

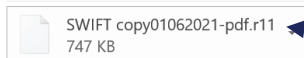
payment.advice.501541376.1040035.3515039904 <payment.advice.501541376.1040035.3515039904@hsbc.com>

[SPAM MAILPROXY] Payment Advice - Advice Ref:[BIBA60174475] [Z1 UNGESICHERT]

An: secuvera Sekretariat

Wir haben zusätzliche Zeilenumbrüche aus dieser Nachricht entfernt.
Diese Nachricht wurde in das Nur-Text-Format konvertiert.

Spamerkennung



Dateiendung

Dear Sir/Madam

unpersönliche/falsche Anrede

Upon the request of G**G LIM**D, attached please find payment e-Advice for your reference.

Yours faithfully
HSBC

親愛的先生/小姐：

謹此附上我們的客戶 G**G LIM**D 所要求發出的付款「e-Advice」，以供參考之用。

香港上海滙豐銀行 謹啟

We maintain strict security standards and procedures to prevent unauthorised access to information about you. HSBC will never contact you by e-mail or other means, such as telephone, fax, or account numbers. If you receive such a request, please call our Direct Financial Services hotline (852) 2748 8222.

Please do not reply to this e-mail. Should you wish to contact us, please send your e-mail to commercialbanking@hsbc.com.hk and we will respond to you.

Absender zwar „OK“, aber irrelevant

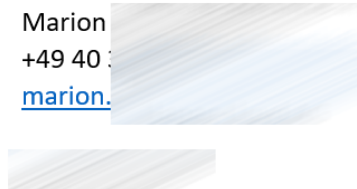


Sehr geehrter secuvera GmbH

Diese ist eine automatisch gesendete Nachricht mit Ihrem Zahlungsavis.

Im Zweifelsfall, wenden Sie sich bitte an Ihren Sachbearbeiter.

Marion
+49 40
[marion.](#)



Nicht rechtskonforme Signatur

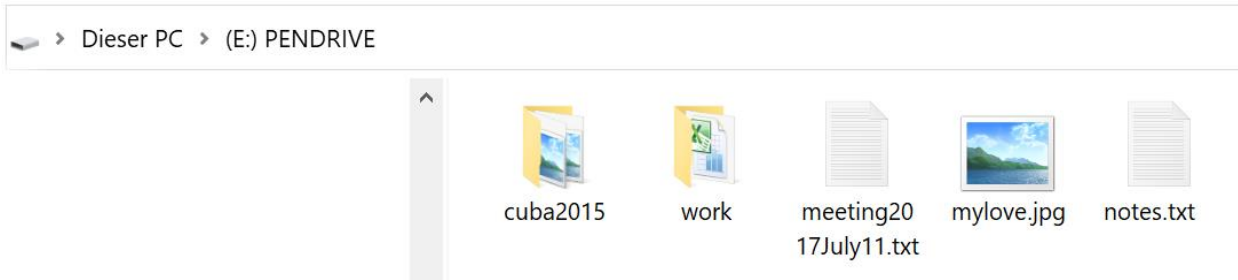
- Ziel: Firmen
- Methode: Phishing mit Anhang
- Zieldaten: Offen
 1. Infizieren
 2. Auskundschaften
 3. Kopieren und/oder verschlüsseln und/oder Daten verkaufen
 4. Erpressen

Kapitel III

Angriff der Profis vor Ort



- Ziel: Firmen
- Methode: USB-Stick
- Zieldaten: Offen
 1. Infizieren
 2. Auskundschaften
 3. Kopieren und/oder verschlüsseln und/oder Daten verkaufen
 4. Erpressen



Diese App wurde vom Systemadministrator gesperrt.

Wenden Sie sich an den Systemadministrator, um weitere Informationen zu erhalten.

In Zwischenablage kopieren

Schließen

Abwehr



- Organisation
 - Ist die Geschäftsleitung aufgeklärt?
 - Gibt es eine Cyberversicherung mit ausreichender Deckung?
- Technik
 - Können Nutzer Programme selbst starten?
 - Werden E-Mails mit eigener Domäne im Absender von außen blockiert/markiert?
 - Werden Nutzer regelmäßig sensibilisiert?
 - Lange Kennwörter und zwei-Faktor-Anmeldung?

- Strategisch
 - Stand der Dinge erheben lassen (z. B. TeleTrust „Stand der Technik“ oder „Cyber-Sicherheits-Check“)
 - Maßnahmen technisch prüfen (z. B. Penetrationstest)
 - Managementsystem einführen (z. B. ISO 27001)



Vielen Dank



KITZBÜHEL
COUNTRY CLUB



TeleTrust
Pioneers in IT security.