Compass Security
[The ICT-Security Experts]

Ransomware – Wie schütze ich mein Unternehmen?
[Berlin – 20.06.2016]

Jan-Tilo Kirchhoff

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Darf ich mich vorstellen?

Jan-Tilo Kirchhoff

- Country Manager Compass Security Deutschland GmbH
- verheiratet, zwei Kinder
- Werdegang: Von der TK-Security zur IT-Security
- Kompetenzen
  - Netzwerk Sicherheitsprüfungen
  - ICT- Security
    (VoIP, PSTN, GSM …)

CISSP Certified Information Systems Security Professional

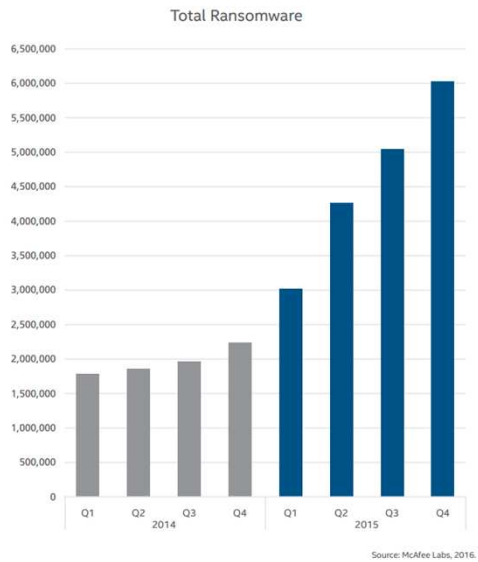
Offensive Security [OSCP]

Hobbys

- Meine Familie
- Musik (Trompete und Chor)
- Electronic Jazz, Jazz Funk
- Laufsport
- ICT-Security

Probieren geht über Studieren …

Warum sind Sie heute hier?



Was macht ein Krypto Trojaner

https://en.wikipedia.org/wiki/Wheel_clamp#/media/File:Wheel_clamps_Texas.jpg

Ein kurze Geschichte der …

Kryptographie

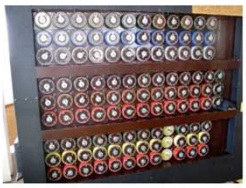
Cyber-Kriminalität

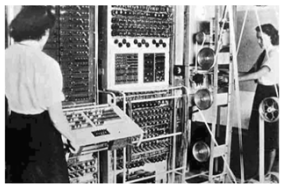
- „Hacker"
- Malware
- Ransomware
- Marktentwicklung
- Zahlungsmethoden
- Krypto-Trojaner

Kryptographie

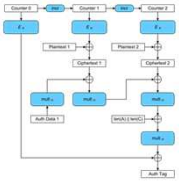
ca. 500 v. Chr.

Vor 70 Jahren





heute



Bildquelle:
https://commons.wikimedia.org/wiki/

Cyber-Kriminalität

Der virtuelle Schwarzmarkt

„Cybercrime is a growth industry. The returns are great, and the risks are low. We estimate that the likely annual cost to the global economy from cybercrime is more than $400 billion. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. “

Source: McAfee June 2014

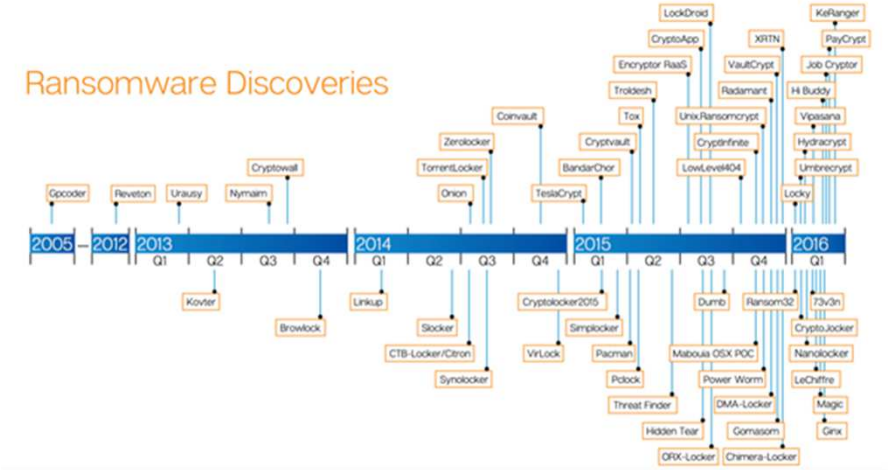
Zahlungsverkehr

WESTERN UNION MONEY TRANSFER

Ukash

paysafecard

Entwicklung der Krypto-Trojaner



Bildquelle: https://cert.ro/

Vorbeugung ist besser als Heilung

Infektionen verhindern – Mitarbeiter schulen

- Mails unbekannter Absender ignorieren
- Auch bei bekannten Absendern zweimal hinsehen
- Vor allem keine Anhänge öffnen

- System aktualisieren
- Nur legal erworbenen Software aus vertrauenswürdigen Quellen nutzen

Schaden minimieren

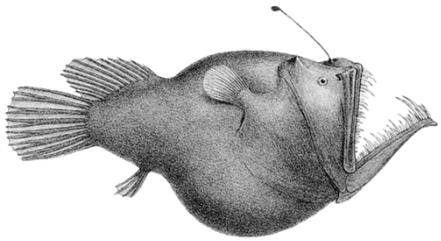
- regelmäßige Backups
  - Wiederherstellung testen
  - Getrennte Medien

- Sicherheitsfunktionen des Betriebssystems nutzen
- Schreibrechte (auf Fileservern) einschränken
- Virenschutzprogramme sind keine Garantie können aber helfen.

Krypto Trojaner erkennen

Verbreitungswege

- E-Mail
  - Anhänge
    - ZIP Dateien (teilweise 2 fach gepackt)
      - Ausführbare Dateien (EXE, vbs, js, java)
    - Word (DOC) oder Excel (XLS) Dateien mit Macros
  - Links
- Browser
  - Unseriöse Webseiten
  - Malwaretisement
  - Gehackte Webseiten

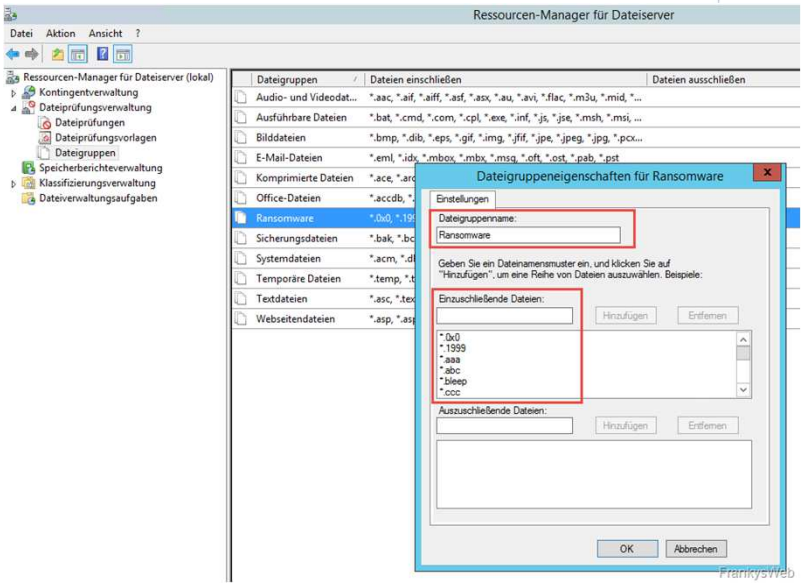


Indikatoren einer Infektion

- Dateien sind plötzlich nicht mehr zu öffnen
- Anzeige der Erpressernachricht
- (Auffälliger Netzwerkverkehr)

Bildquelle: https://commons.wikimedia.org/wiki/File:Melanocetus_murrayi_(Murrays_abyssal_anglerfish).jpg

Resourcen-Manager für Dateiserver



FrankysWeb

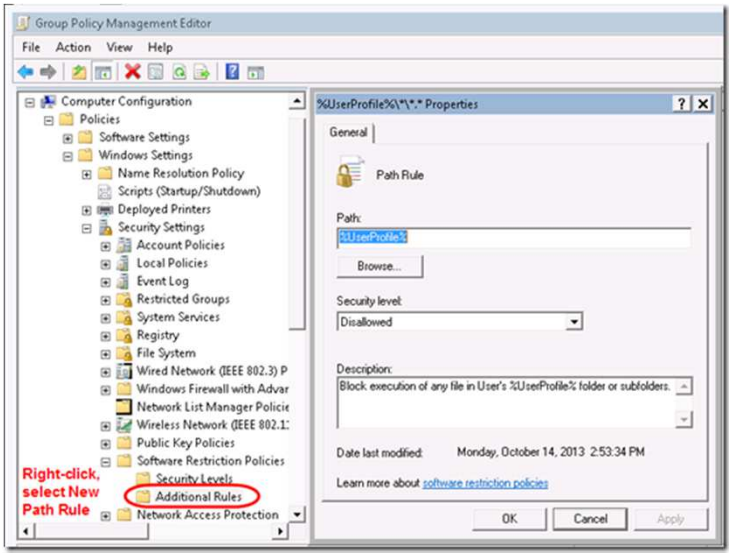
Typische Dateiendungen und Dateien

```
*.k
*.encoderpass
*.locky
*.key
*.ecc
*.ezz
*.exx
*.zzz
*.xyz
*.aaa
*.abc
*.ccc
*.vvv
*.xxx
*.ttt
*.micro
*.encrypted
*.locked
*.crypto
_crypt
*.crinf
*.r5a
*.xrtn
*.XTBL
*.crypt
*.R16M01D05
*.pzdc
*.good
*.LOL!
*.OMG!
*.RDM
*.RRK
*.encryptedRSA
*.crjoker
*.EnCiPhEred
*.LeChiffre
*.keybtc@inbox_com
*.0x0
*.bleep
*.1999
*.vault
*.HA3
*.toxcrypt
*.magic
*.SUPERCRYPT
*.CTBL
*.CTB2
*.locky
```

```
HELPDECRYPT.TXT
HELP_YOUR_FILES.TXT
HELP_TO_DECRYPT_YOUR_FILES.txt
RECOVERY_KEY.txt
HELP_RESTORE_FILES.txt
HELP_RECOVER_FILES.txt
HELP_TO_SAVE_FILES.txt
Decryptallfiles.txt
DECRYPT_INSTRUCTIONS.TXT
INSTRUCCIONES_DESCIFRADO.TXT
How_To_Recover_Files.txt
YOUR_FILES.HTML
YOUR_FILES.url
encryptor_raas_readme_liesmich.txt
Help_Decrypt.txt
DECRYPT_INSTRUCTION.TXT
HOW_TO_DECRYPT_FILES.TXT
ReadDecryptFilesHere.txt
Coin_Locker.txt
_secret_code.txt
About_Files.txt
Read.txt
ReadMe.txt
DECRYPT_ReadMe.TXT
Decryptallfiles.txt
FILESAREGONE.TXT
IAMREADYTOPAY.TXT
HELLOTHERE.TXT
READTHISNOW!!!.TXT
SECRETIDHERE.KEY
IHAVEYOURSECRET.KEY
SECRET.KEY
HELPDECYPRT_YOUR_FILES.HTML
help_decrypt_your_files.html
HELP_TO_SAVE_FILES.txt
RECOVERY_FILES.txt
RECOVERY_FILE.TXT
RECOVERY_FILE*.txt
HowtoRESTORE_FILES.txt
HowtoRestore_FILES.txt
howto_recover_file.txt
restorefiles.txt
howrecover*.txt
_how_recover.txt
recoveryfile*.txt
recoverfile*.txt
recoveryfile*.txt
Howto_Restore_FILES.TXT
help_recover_instructions+*.txt
_Locky_recover_instructions.txt
```

https://www.frankysweb.de/windows-fileserver-vor-ransomware-crypto-locker-schuetzen/

Group Policies – Execution Prevention



http://www.mcbsys.com/blog/2013/10/block-user-folder-executables/

Weitere Werkzeuge

Microsoft

`Applocker`

- https://technet.microsoft.com/de-de/library/hh831440.aspx

`Enhanced Mitigation Experience Toolkit (EMET)`

- https://support.microsoft.com/de-de/kb/2458544

Andere

`CryptoPrevent`

- https://www.foolishit.com/cryptoprevent-malware-prevention/

Mail Signaturen

- Sicherstellen, dass Nachrichten tatsächlich und nicht nur scheinbar von einem bestimmten Absender stammen.

Wenn doch mal was passiert ist

Informieren Sie

- Ihren Vorgesetzten
- Ihre Kollegen
- Die Mitarbeiter

Don't Panic!

Zahlen oder nicht?

- Das BSI und die Polizei empfehlen nicht zu zahlen
  - Zahlungen motivieren die Täter
  - Zahlungen finanzieren die Weiterentwicklung der Malware

Empfehlungen

Erstellen Sie regelmäßig Backups Ihrer wichtigen Dateien

`und prüfen Sie, ob Sie diese auch wieder herstellen können!`

Erst denken dann handeln

`Beim Öffnen von E-Mails und beim Surfen im Web`

- Meiden Sie Mails und Anhänge von unbekannten Absendern
- Nutzen Sie seriöse und bekannte Angebote im Internet

Halten Sie Betriebssystem und Software aktuell

`Das gilt insbesondere auch für den Virenschutz`

Wissen ist Macht...

- Wir wollen niemanden zu einer Straftat anstiften!
- Alle gezeigten Informationen dienen ausschließlich dazu, sie zu sensibilisieren! Denn nur wer um die Gefahren weiß, kann sich davor schützen.
- Wenn sie Fragen im Bereich IT-Sicherheit haben, sprechen sie uns an.

Vielen Dank!

Vielen Dank für Ihre Aufmerksamkeit!

Zeit für Ihre Fragen

Compass Security

Penetration Testing/Security Assessment

IT Forensik

Security Training (www.hacking-lab.com)

Unser Leistungsspektrum:

- Prüfungen von Web-Applikationen sowie Client- und Server-Applikationen
- Analysen und Test-Angriffe aus dem Internet, Intranet und dem Telekommunikationsnetz
- Security Assessments von Industrial Control Systems (industrielle IT-Anlagen)
- Sicherheitsanalysen von Geldautomaten und SB-Terminals
- Social Hacking und Social Engineering
- Prüfung von drahtlosen Medien (WLAN, Bluetooth, DECT, 2G/3G/4G, Wireless Radio Devices etc.)
- Analyse von Mobile-Lösungen und Konzepten (BYOD)
- Konzept Reviews von Informations- und Kommunikationslösungen (ICT)
- IT-Forensische Analysen
- IT-Security-Trainings

Kontakt

Compass Security Deutschland GmbH

Tauentzienstr. 18
10789 Berlin
Germany

team@csnc.de | www.csnc.de | +49 30 21 00 253-0

Secure File Exchange: www.filebox-solution.com