Behind the Ransom - Was steckt hinter Ihrem nächsten Erpressungstrojaner?

Jan Schreiber – js@schreiberconsulting.eu

Jan Felix Wiebe - clarity@hannover.ccc.de

Agenda

- Was ist ein Trojaner (und was haben die Griechen damit zu tun?)
- Wie funktioniert(e) der Angriff
- Warum ist das nach fast 3000 Jahren wieder/immernoch relevant?

- Was hat das ganze mit Patienten und Krankenhäusern zu tun?
- Wie haben sich die Angreifer und Bedrohungen weiterentwickelt?
- Fragen fragen!

Was ist ein Trojaner?

- Entspringt der griechischen Mythologie
  - Hölzernes Pferd gefüllt mit 50/23/30/40 griechischen Helden
  - Als “Geschenk” vor die Tore Trojas gerollt
  - Pferd wurde in die Stadt gerollt
  - Helden öffneten Stadttore
  - Trinken all den Wein
  - Niemand hat Spaß
  - Ist vermutlich nie so passiert

Trojaner: Ein harmlos aussehendes Objekt, das ein Angreifer zur Tarnung verwendet, um in einen geschützen Bereich zu gelangen.

Wie funktioniert der Angriff

- Angreifer versteckt sich in einem harmlos Aussehenden Objekt
  - Katzenbilder, ZIP-Archive, Mailanhänge, (hölzerne Pferde)
- Objekt wird in den geschützten Bereich überführt
  - ZIP-Archive werden geöffnet, Anhänge heruntergeladen
- Angreifer fängt an Ihren Wein zu trinken
  - wieder hat niemand Spaß
- Passiert leider wirklich und hat ernsthafte Konsequenzen

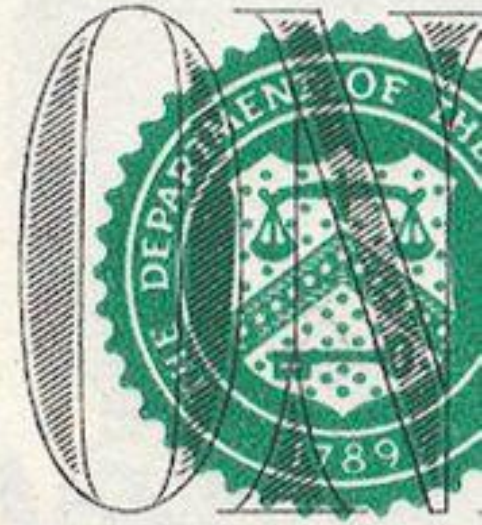
Warum immernoch relevant?

- Es gibt keine absolute Sicherheit in IT-Systemen
  - auch sonst nicht
- Es treten regelmäßig neue Sicherheitslücken auf
- Schwachstelle Mensch wird ausgenutzt

Der Angreifer muss nur einmal gewinnen!

S NOTE IS LEGAL TENDER
. DEBTS, PUBLIC AND PRIVATE

WASHINGTO



obeds Cabral

SERIES
2006

Henry M.

United States.

Secretary of t

220 M
Ransc

Deutsche
spielt Ran

Backup
wirksam

igen

zten Jahr
ste

Wana Decrypt0r 2.0

English

Payment will be raised on

5/15/2017 16:32:52

Time Left

02:23:59:49

Your files will be lost on

5/19/2017 16:32:52

Time Left

06:23:59:49

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

About bitcoin

How to buy bitcoins?

Contact Us

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Wieso Krankenhäuser und Patienten?

- Schadsoftware unterscheidet nicht zwischen Computersystemen
  - (genauso wie Krankheiten kein halt vor Personengruppen machen)
- Angriffe auf Krankenhäuser nehmen deutlich zu
- Inzwischen Gefährdung von Menschenleben
  - direkt und indirekt

In Frankreich mussten Notfall-Patienten verlegt und ein Covid-Impfzentrum geschlossen werden. In Deutschland und USA gibt es auch Opfer.

- Die Trägergesellschaft Süd-West des Deutschen Roten Kreuzes ist offenbar Opfer eines Ransomware-Angriffs geworden.
- 13 Krankenhäuser waren betroffen, auf die Patienten hat sich die Infektion des IT-Systems der Gesellschaft zufolge nicht ausgewirkt.
- Der Angriff ist offenbar verhältnismäßig glimpflich ausgegangen, das LKA ermittelt.

Mehrere französische S
wie das Krankenhaus L'

The untold story woman

German prosecutors tried to prove that a ransomware attack on a hospital was to blame for someone losing their life. Their story is a warning

Lösegeldangriffen an. In Deutschland gab es deswegen heute einen Todesfall an der Uniklinik Düsseldorf. Akademische Einrichtungen sind dringend aufgefordert, sicherzustellen, dass ihre Netzwerke widerstandsfähig genug sind, um sich vor Attacken zu schützen.

Wie haben sich die Angriffe weiterentwickelt?

- Früher: Daten verschlüssen – Geld verlangen – Daten entschlüsseln

- Jetzt: Daten stehlen, Daten verschlüsseln, Geld verlangen, wieder Geld verlangen, wieder Geld verlangen, wieder Geld verlangen, wieder Geld verlangen
  - schwieriger da häufig große Datenmengen gestohlen werden müssen
    - noch schwieriger wenn wir weiter auf Faxgeräte setzen
      - es ist 2021…
        - wieso gibt es noch Fax…?

Was tun wenn sie einen Angriff erkennen?

RUFEN SIE DIE IT-ABTEILUNG AN!

(wenn Sie die IT-Abteilung sind wissen Sie was zu tun ist)

Vielen Dank für Ihre Aufmerksamkeit!

Bleiben Sie gesund.

Fragen?

Fragen fragen!