

Der Cyber-Bankraub von Bangladesch

Lars A. Wallenborn

FrOSCon — 22. August 2021

Mit Malware Analyse Großkriminellen auf die Spur kommen

Intro

Lars A. Wallenborn
lars@wallenborn.net
@larsborn

Seit 2004 Freiberufler im IT Bereich
2013 Diplom in Mathematik @ Uni Bonn
2014 - 2015 Softwareentwickler @ Bonn
Seit 2015: Security Researcher @ CrowdStrike
Seit 2021: Podcaster @ <https://armchairinvestigators.de/>

Agenda

1. Was ist passiert?
2. Reverse Engineering
 - 2.1 Was ist das?
 - 2.2 Assembly
 - 2.3 Tools
 - 2.4 Ghidra
3. Demo!

Was ist passiert?

- 
- A vintage beige Apple LaserWriter printer is shown from a three-quarter front view. The printer has a paper tray open at the bottom, revealing a blue paper tray. The Apple logo is visible on the top right corner. The text "UDW" is printed on the front panel above the paper tray. A power cord is coiled in the foreground. A manual titled "LaserWriter and LaserWriter Plus" is visible in the bottom right corner.
- Drucker ausgefallen
 - 5./6. Februar 2016
 - Zentralbank von Bangladesch



- Entwicklungsland östlich von Indien
- 165 Millionen Einwohnern
- 220 Milliarden USD BIP

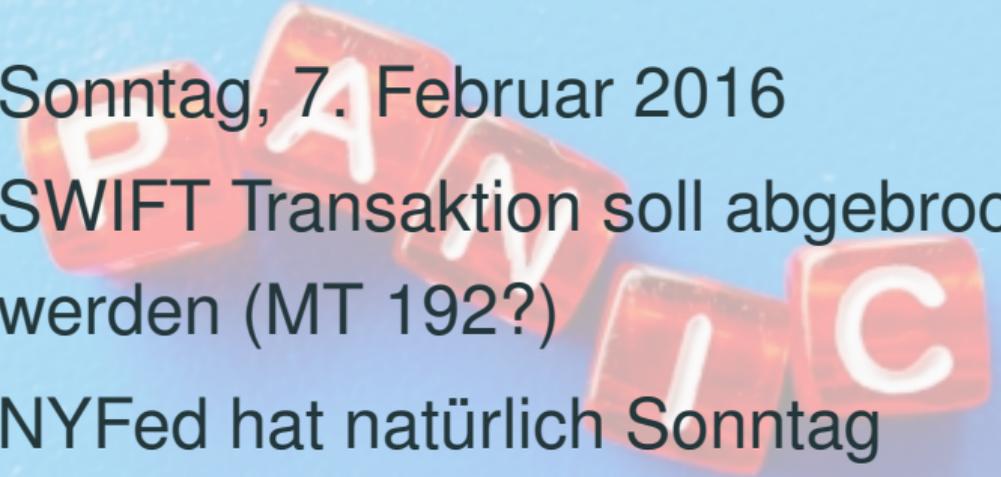
- 
- An aerial photograph of a densely populated city, likely Dhaka, Bangladesh. The city is filled with numerous multi-story buildings and residential structures. In the center, a tall, modern skyscraper with a distinctive design stands out against the sky. The background shows a vast expanse of the city stretching towards the horizon under a clear blue sky.
- Bangladesh Bank
 - Zentralbank des Landes
 - Notenbank für die Stabilität des Taka

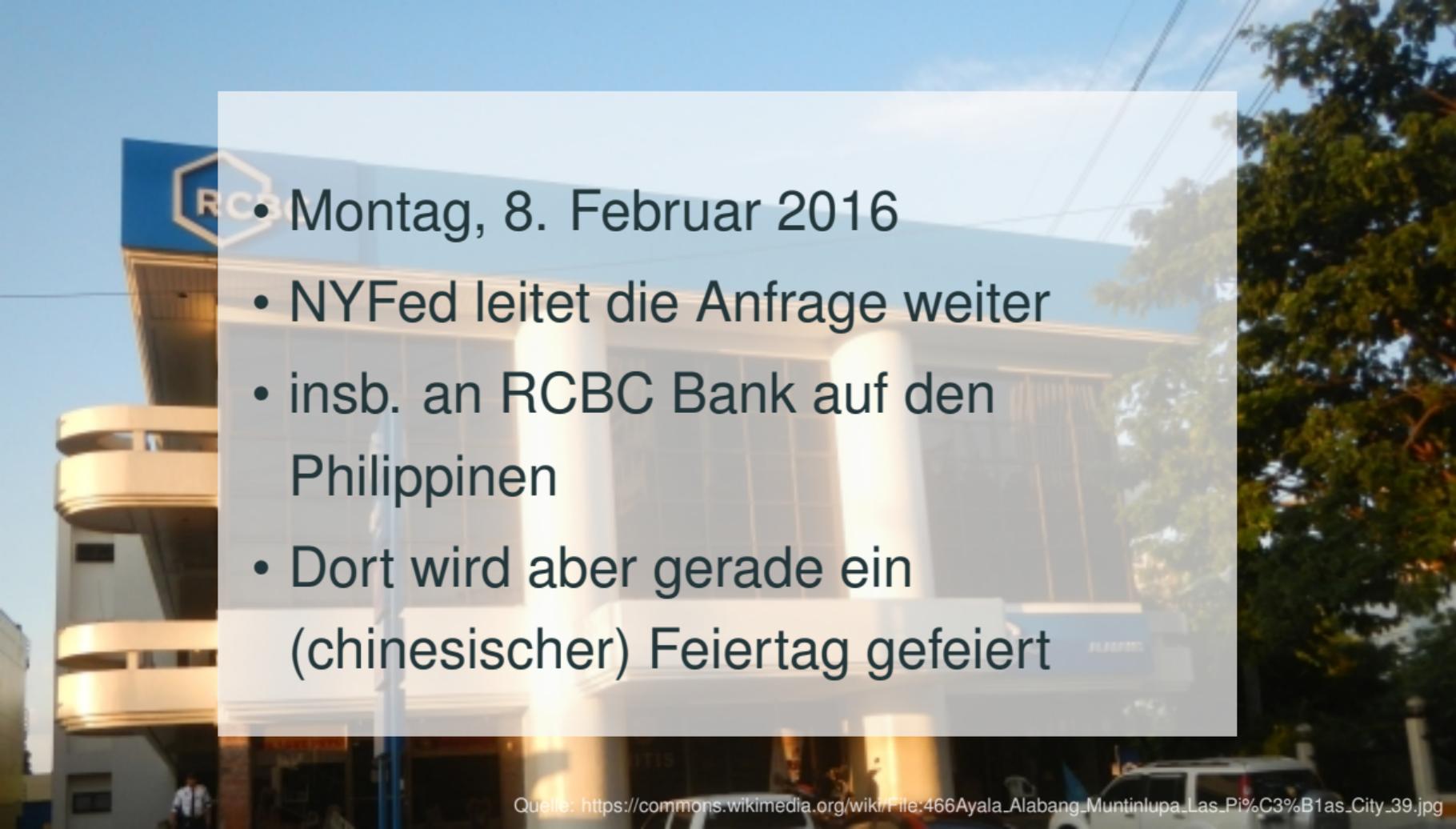
- Donnerstag, 4. Februar 2016
- Feierabend
- 35 SWIFT Nachrichten gehen an NYFed
- Eine Milliarde Dollar

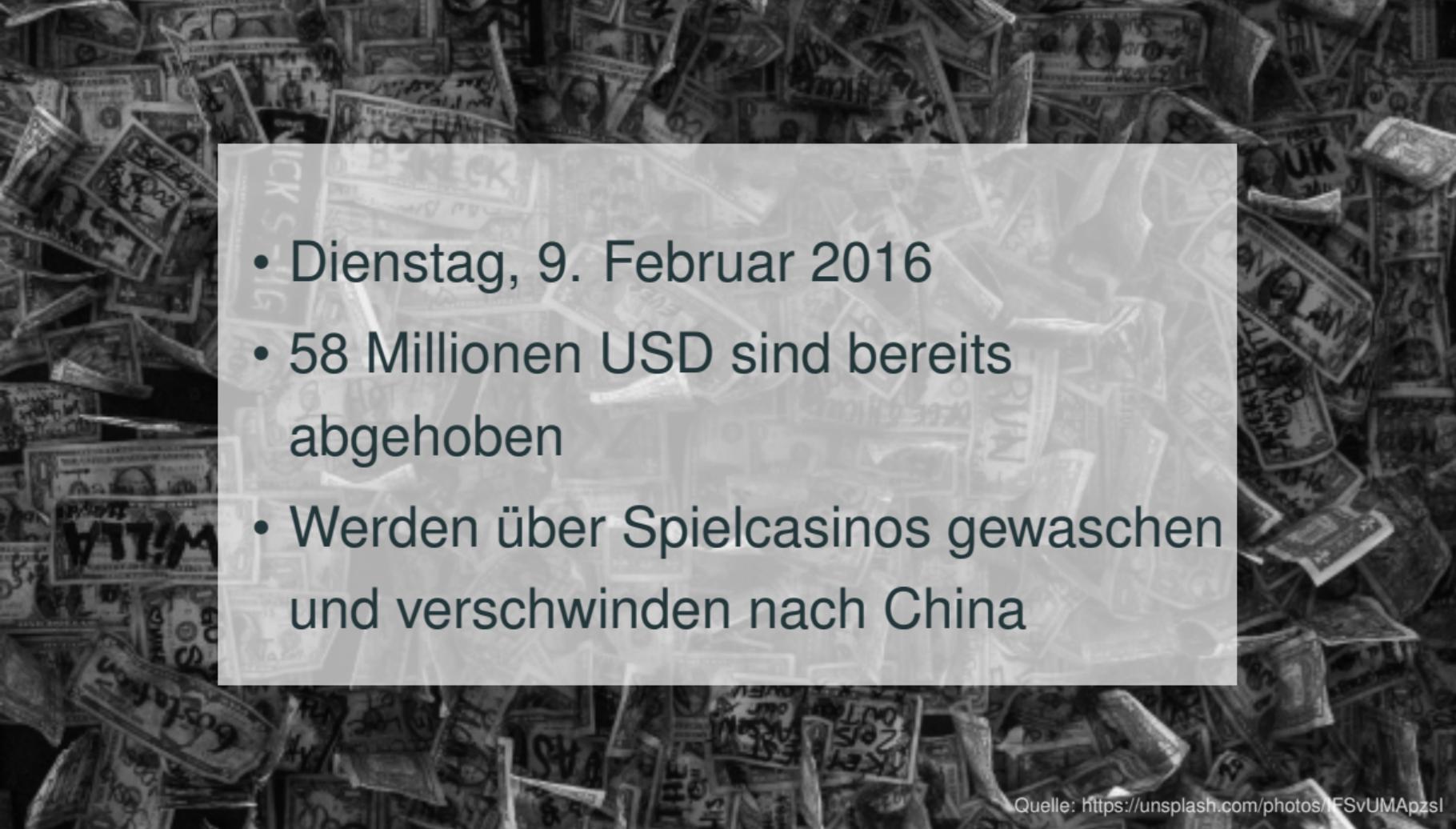
- 
- Freitag, 5. Februar 2016
 - NYFed versucht Bangladesh Bank zu kontaktieren
 - Freitag (Muslims) \approx Sonntag (Christen)

- Samstag, 6. Februar 2016



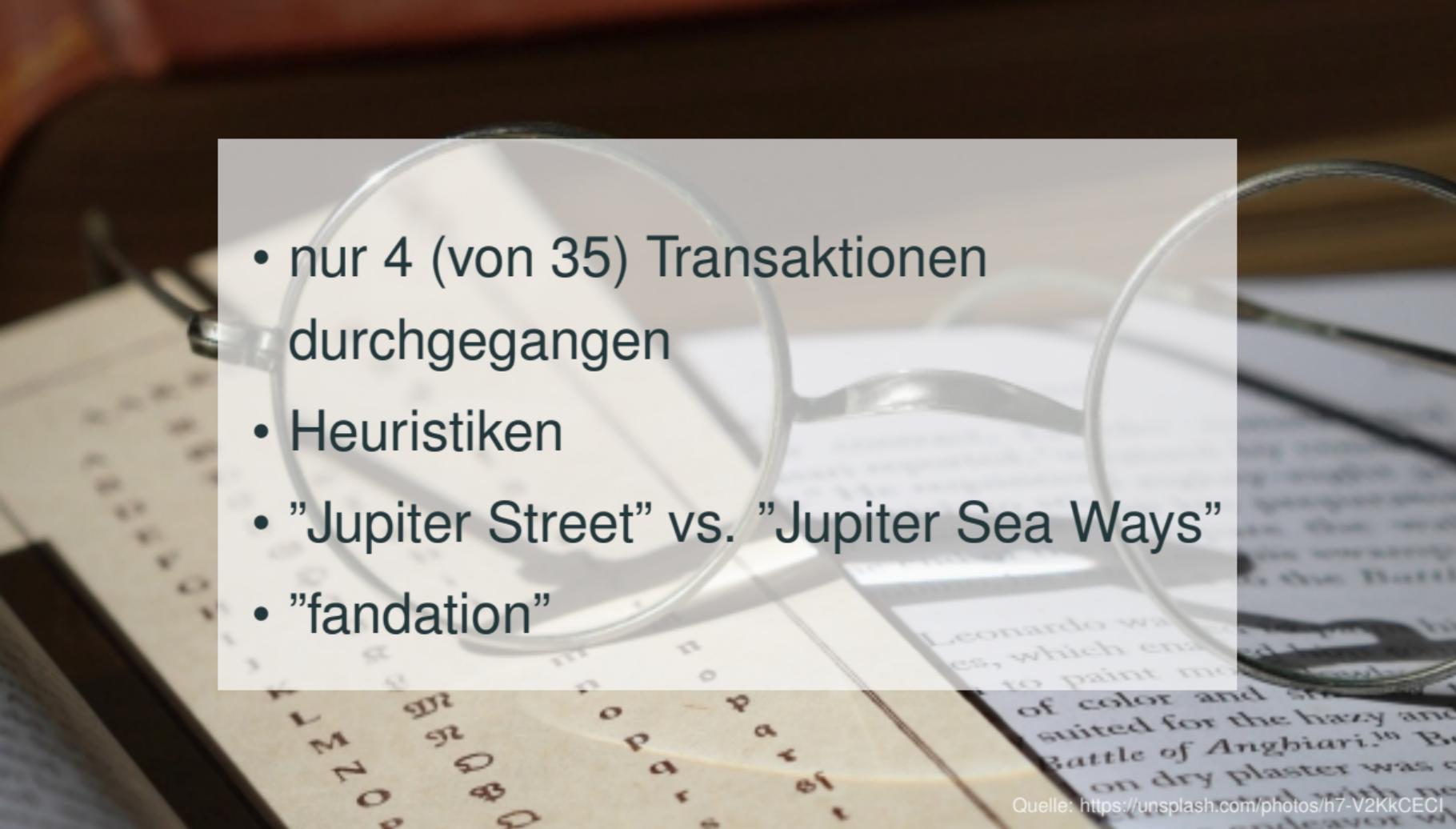
- 
- The background of the slide features a light blue gradient with a semi-transparent white rectangular area in the center. Within this white area, there are several red dice with white letters on their faces, arranged to spell out the word 'BANK'. The dice are slightly tilted and overlapping, creating a 3D effect. The letters are 'B', 'A', 'N', 'K' in order from left to right.
- Sonntag, 7. Februar 2016
 - SWIFT Transaktion soll abgebrochen werden (MT 192?)
 - NYFed hat natürlich Sonntag

- 
- The background image shows a modern RCBC Bank building with a blue and white facade. The RCBC logo is visible on the upper left. The building has large windows and a prominent entrance. The scene is set outdoors with trees and a clear sky.
- Montag, 8. Februar 2016
 - NYFed leitet die Anfrage weiter
 - insb. an RCBC Bank auf den Philippinen
 - Dort wird aber gerade ein (chinesischer) Feiertag gefeiert

- 
- Dienstag, 9. Februar 2016
 - 58 Millionen USD sind bereits abgehoben
 - Werden über Spielcasinos gewaschen und verschwinden nach China

Zeitlicher Verlauf

	Februar 2016	Donnerstag (4.)	Freitag (5.)	Samstag (6.)	Sonntag (7.)	Montag (8.)	Dienstag (9.)
Bangladesh Bank		35 SWIFT Instruktionen (Feierabend)	Wochenende Drucker läuft nicht	Wochenende Drucker läuft nicht	Drucker repariert, Cancel Request		
NewYork Federal Reserver Bank			Rückfrage an Bangladesh Bank	Wochenende	Wochenende	Cancel Request erhalten und weitergeleitet	
RCBC (Philippinen)				Wochenende	Wochenende	Chinesisches Neujahr	58 Millionen USD sind bereits abgehoben

- 
- A pair of round, light-colored glasses is positioned over an open book. The book's pages are visible, with some text like "Leonardo was" and "of color and" appearing. In the foreground, a portion of a keyboard is visible, showing keys like 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z'. The background is softly blurred, suggesting a desk or study environment.
- nur 4 (von 35) Transaktionen durchgegangen
 - Heuristiken
 - "Jupiter Street" vs. "Jupiter Sea Ways"
 - "fandation"



Cool Story Bro

Was ist Reverse Engineering?

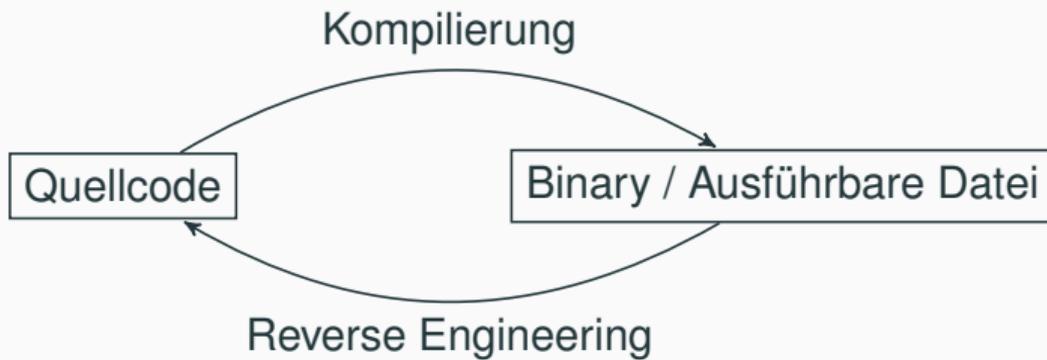
Was ist Reverse Engineering?

- zu Deutsch: Rückwärtsanalyse
- kurz: *RE* oder *reversing*
- sehr allgemeiner Ausdruck: einen Produktionsprozess rückwärts durchführen
- mit dem Ziel das Design, die Architektur oder — ganz allgemein — Wissen über das RE Ziel zu ermitteln

In diesem Vortrag

Konzentrieren wir uns auf:

Reversing von kompilierter Software



Assembly

Assembly

- Schwer zu lesende Programmiersprache, die direkt von einer CPU ausgeführt werden kann.
- Erlaubt nur sehr einfache Dinge wie addieren oder Speicherzugriffe.
- Wird oft im "disassembled" Zustand angezeigt: Anstelle von

```
90907504
```

schreibt man

```
NOP
```

```
NOP
```

```
JNZ 6
```

- Sehr zeitaufwendig zu lesen

Reversing Tools

Reversing Tools

- IDA (Interactive Disassembler) + HexRays Decompiler
- Binary Ninja
- RetDec (retargetable decompiler)
- Ghidra

Ghidra

Was ist Ghidra?

- Existenz ist bekannt seit den Vault7 leaks 2017.
- Die NSA kündigte 2019 auf der RSA Konferenz an, dass sie Ghidra als OSS veröffentlichen werden.
- Das ist dann auch passiert: <https://github.com/NationalSecurityAgency/ghidra>
- In Java geschriebene GUI.
- In C geschriebenes Decompiler backend.
- Kann native PE Dateien (.exe-Dateien) *dekompilieren*
- (und auch viele andere Formate)

[Bangladesh Bank] Verdächtige Datei auf dem SWIFT Terminal

[Anfrage für Malware-Analyse](#)

Description Edit

Unser Netzwerk ist Ziel eines Cyber-Angriffs mit verheerenden Folgen geworden. Während der "incidence response" wurde durch forensische Analyse unseres hausinternen SWIFT-Terminals eine verdächtige Portable Executable (PE) Datei aufgetan. Sie trug den Namen `evtdiag.exe` im Dateisystem und hat den folgenden SHA256 hash:

```
4659dadbf5b07c8c3c36ae941f71b631737631bc3fded2fe2af250ceba98959a
```

Wir möchten verstehen ob und wenn ja, wie, diese Datei mit dem Angriff in Verbindung steht.

Activity

Show details



Write a comment...

Danke für die Aufmerksamkeit

- Angriffe hinterlassen Spuren
- Reversing kann man lernen
- Mit Reversing kann man solche Spuren analysieren

Lars A. Wallenborn

lars@wallenborn.net

[@larsborn](#)

Eigenwerbung:

- Ich gebe Schulungen im Reverse Engineering: **mal.re** (mit Jesko Hüttenhain)
- Hört in den Podcast rein: **armchairinvestigators.de** (mit Christian Dietrich)