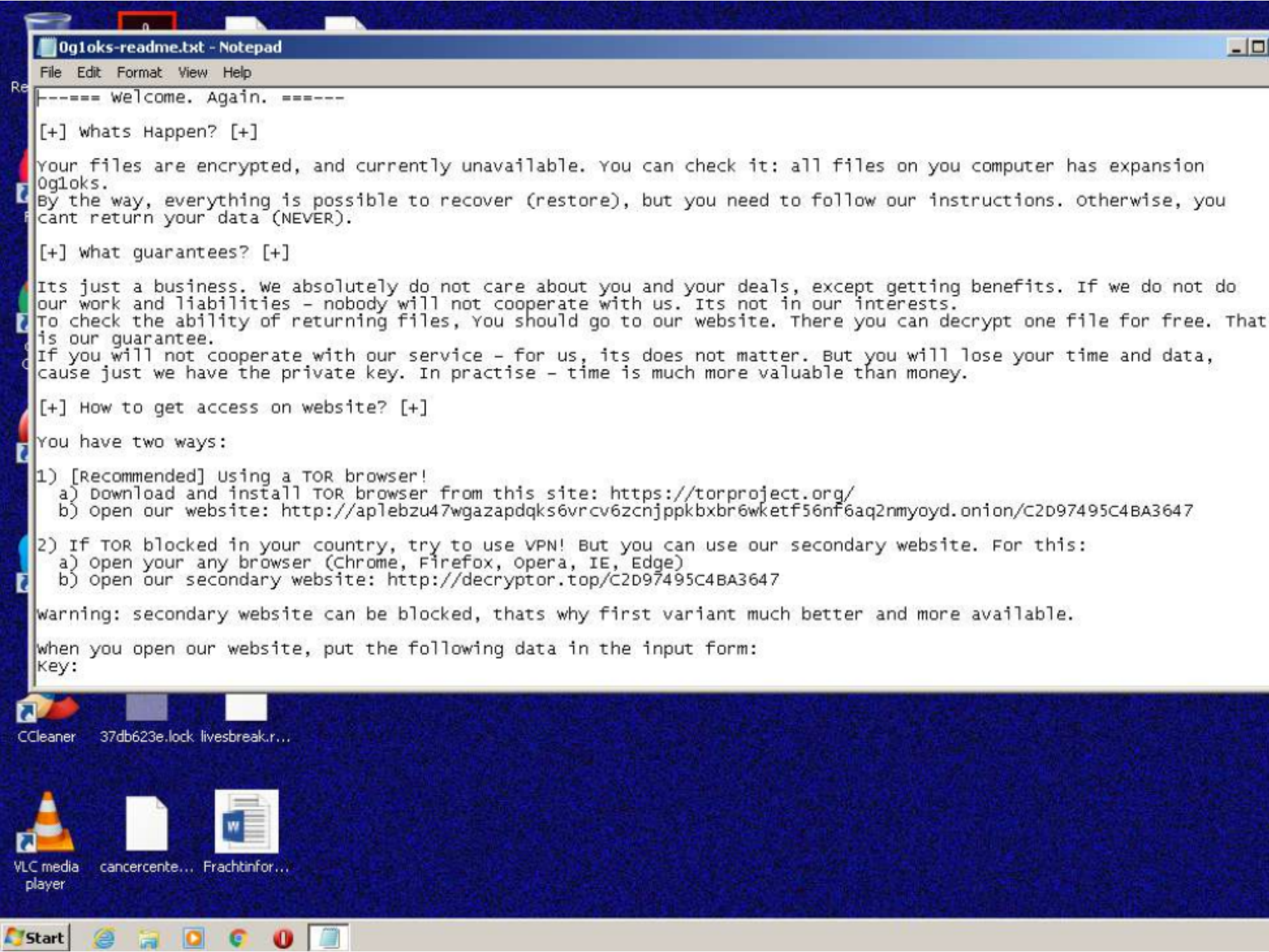
Ghidra Workshop
Intro

Jesko Hüttenhain & Lars A. Wallenborn

Coole Themen für Coole Leute

23. April 2020


0g1oks-readme.txt - Notepad
File Edit Format View Help
------ Welcome. Again. ------
[+] Whats Happen? [+]
Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion 0g1oks.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).
[+] What guarantees? [+]
Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.
[+] How to get access on website? [+]
You have two ways:
1) [Recommended] Using a TOR browser!
a) Download and install TOR browser from this site: https://torproject.org/
b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/C2D97495C4BA3647
2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
b) Open our secondary website: http://decryptor.top/C2D97495C4BA3647
Warning: secondary website can be blocked, thats why first variant much better and more available.
when you open our website, put the following data in the input form:
Key:
CCleaner
37db623e.lock
livesbreak.r...
VLC media player
cancercente...
Frachtinfor...
Start

Agenda

1. Sodinokibi / REvil
2. Kryptographische Algorithmen identifizieren
3. Ghidra Lifehacks
4. Ablauf des Workshops

Sodinokibi / REvil – Überblick

- Sodinokibi (aka REvil)
- Ransomware
- hängt vermutlich mit der Ransomware-Familie *GandCrab* zusammen (GandCrab hat angeblich 2.000.000.000 $ eingebracht)
- Aktuelle Version 2.1
- Erste Sichtung: April 2019
- Ransomware-as-a-Service (RaaS)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.revil

Sodinokibi / REvil – Sample

SHA256 Hash

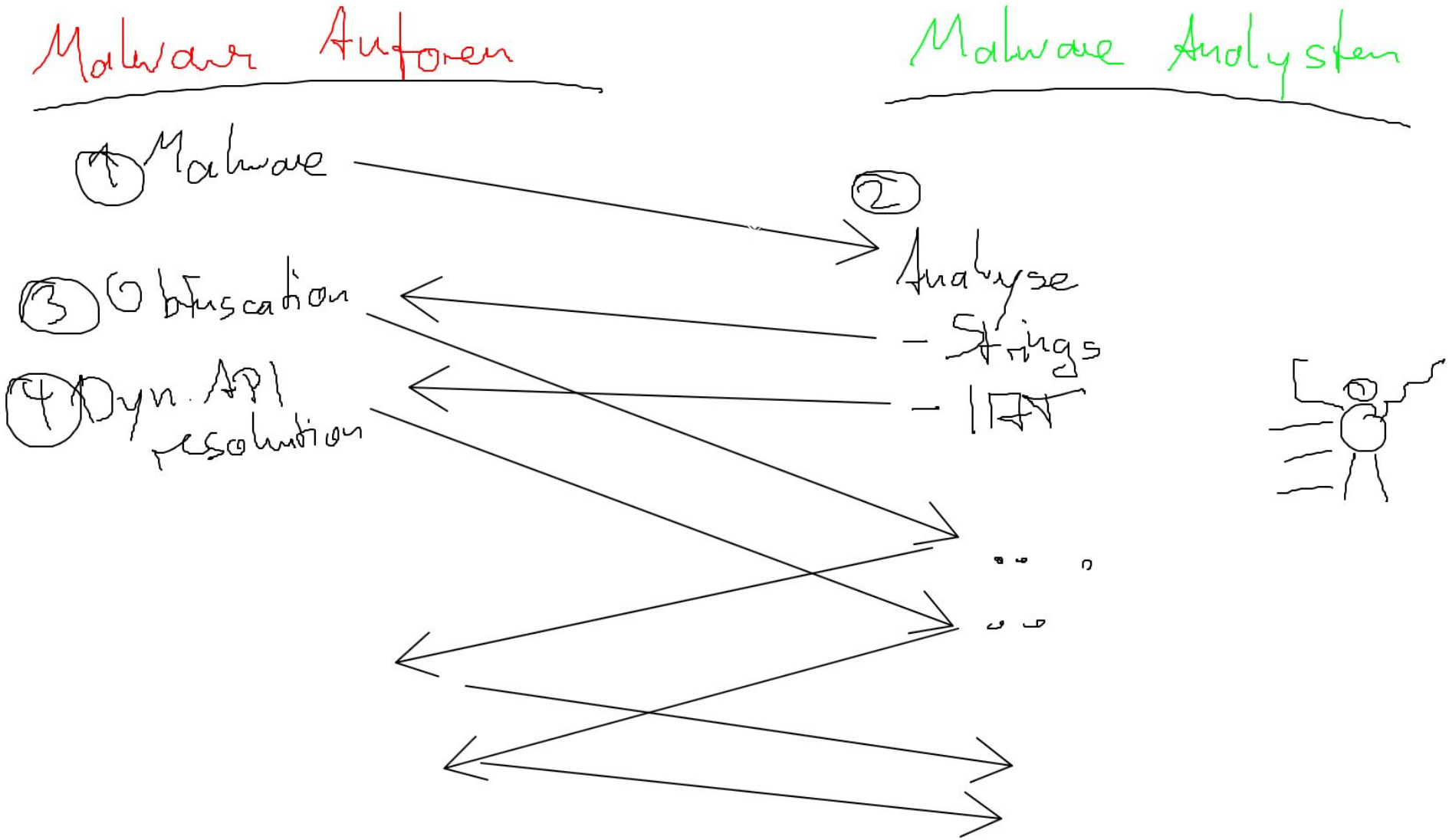
`ef6a96bf68ec54d78f4f4cd304acc671`
`8f9dfe398f368bc1e5b127bd746302f2`

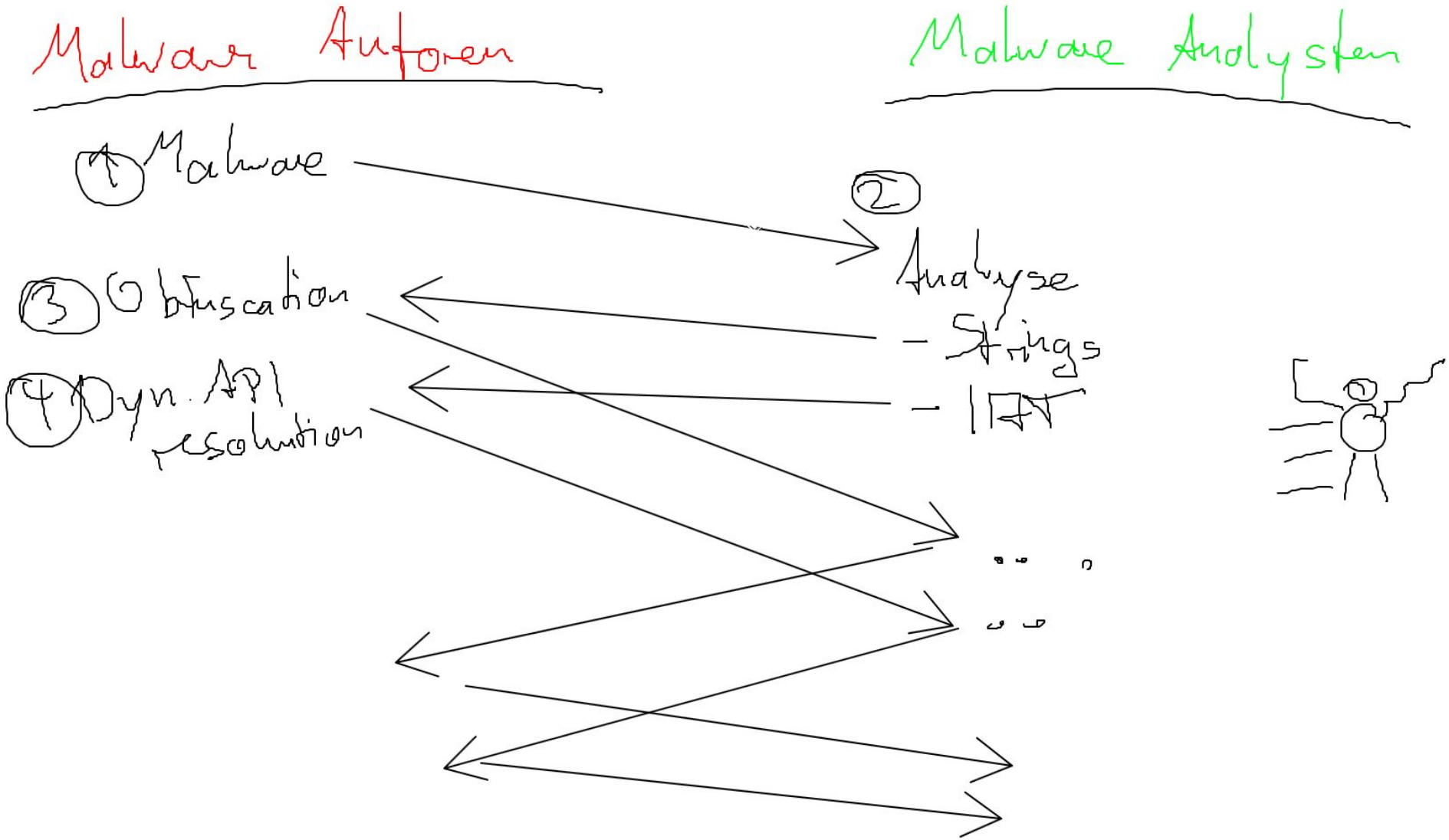
Timestamp 2020-03-14 19:08:12

Lernziel String-Deobfuscation verstehen

Download https://mal.re/tmp/coole-leute/

Passwort `infected`


Malware Autoren
Malware Analysten
1 Malware
2
Analyse
- Strings
- IAT
3 Obfuscation
4 Dyn. API resolution


Malware Autoren
Malware Analysten
1 Malware
2
Analyse
- Strings
- IAT
3 Obfuscation
4 Dyn. API resolution

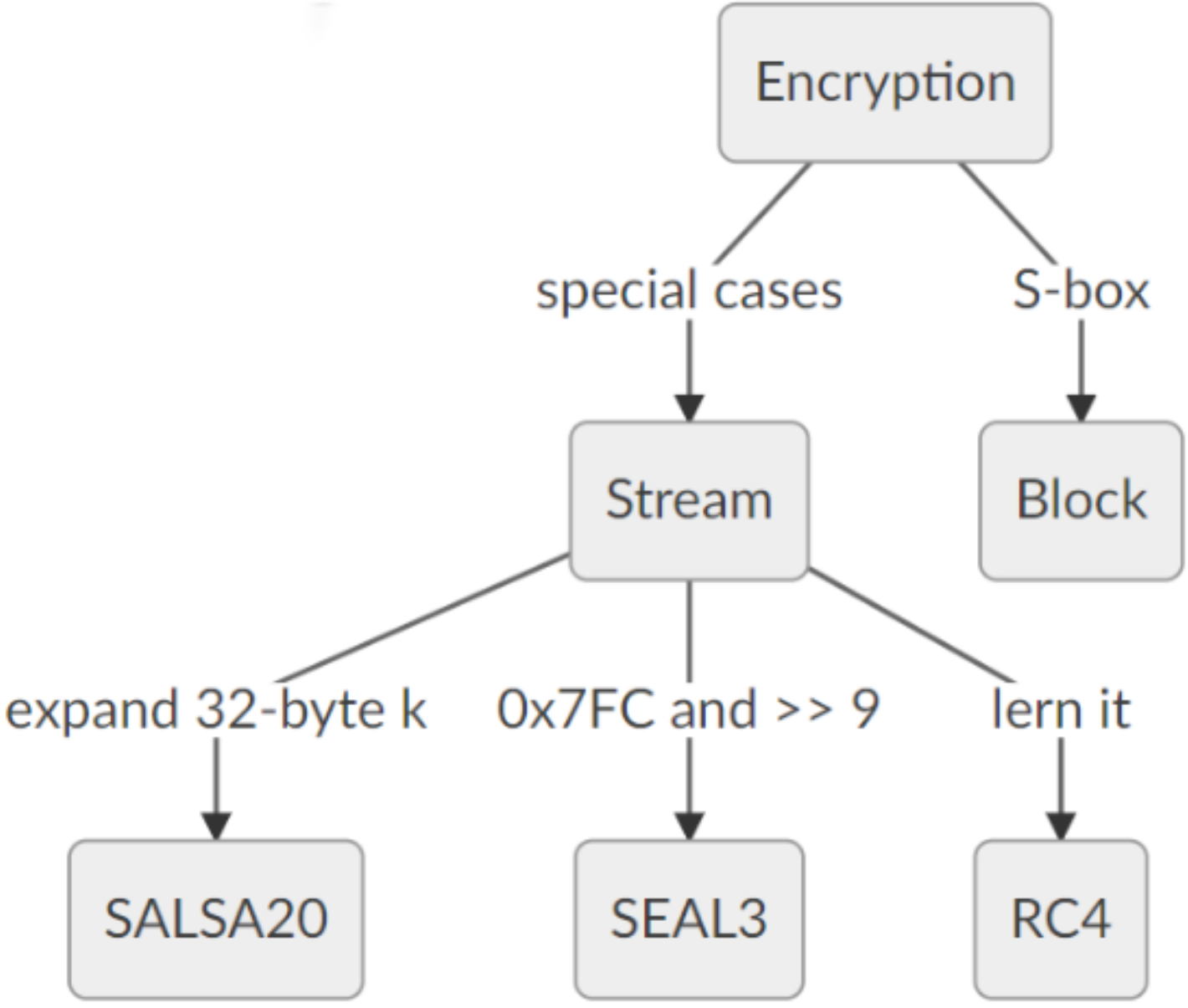
Anti-Analyse

- Strings liefern einen sehr guten Einstiegspunkt für statische Bottom-Up Analyse.
- Also haben Malware-Authoren ein Interesse daran, dass Strings nicht mehr direkt in der Binary vorkommen.

```
char s[10];
fun(s, "3816320013131C1B", 8, 0x75);
printf("%s", s);
```

Kryptographische Algorithmen identifizieren

- Gibt es eine S-Box? (das ist ein langes Array mit vorberechneten Werten)
  $\Rightarrow$ Block-Cipher (Anfang der S-Box googeln)
- Permutations-Array mit 256 Einträgen. Initialisierung dieses Arrays mit den Zahlen von 0 bis 255. Drei aufeinanderfolgende Schleifen.
  $\Rightarrow$ RC4
- Kommt die Zeichenkette `expand 32-byte k` vor?
  $\Rightarrow$ SALSA20
- Kommt der Wert `0x7FC` und viele rechts-shifts um 9 vor?
  $\Rightarrow$ SEAL3


Encryption
special cases
S-box
Stream
Block
expand 32-byte k
0x7FC and >> 9
lern it
SALSA20
SEAL3
RC4

How To Ghidra (1/3) – Überblick

- Sample in Ghidra ziehen, dann auf den Drachen droppen.
- Immer weiter auf ”Ja” und ”Ok” und ”Weiter” klicken.
- Im ”Symbol Tree” unter ”Exports” zum `entry` point gehen.
- Google benutzen um Windows API Funktionen nachzuschlagen.
- Doppelklick um einer Referenzen (z.B. einem Funktionsaufruf) zu folgen.

How To Ghidra (2/3) – Shortcuts

- `ESC` um ”zurück” zu gehen.
- `N` um eine Variable oder Funktion umzubenennen.
- `Y` um einen Datentypen anzupassen.
- `P` (im Disassembly) falls Ghidra nicht verstanden hat, dass irgendetwas eine Funktion ist.
- `G` (im Disassembly) um an eine bestimmte Stelle im Speicher zu springen, arithmetische Ausdrücke sind erlaubt.
- Im Zweifelsfall: Rechtsklick!

How To Ghidra (3/3) – Einstellungen

- ”Options” → ”Key Bindings”, klicke ”Import...” und importiere `ghIDA.kbxml` (von https://mal.re/tmp/ghIDA.kbxml)
- ”Edit” → ”Tool Options” → ”Listing Fields” → ”Cursor Text Highlight”, setze ”Mouse Button To Activate” auf ”LEFT”
- Bereich im Disassembly markieren und `Shift-E` und ”Byte String (No Spaces)” um die Markierung, hex-encoded, in die Zwischenablage zu kopieren.
- http://cyberchef.nullteilerfrei.de/ falls ihr mal schnell mit Daten rum spielen wollt.

How To Workshop

- Lade Sample (`ef6a96...6302f2.7z`) und Handout von https://mal.re/tmp/coole-leute runter.
- Wir teilen uns in Break-Out Räume mit je 4 Leuten auf.
- Helft einander!
- Jesko und ich ”laufen rum” und beantworten Fragen.
- Wer will, kann uns Privatnachrichten schicken.
- Traut euch, es gibt keien dummen Fragen, es gibt nur dumm Studenten.
- Um 20:00 treffen wir uns wieder hier und machen ein Quiz (10 Fragen). Jeder kann jederzeit gehen. Wenn ihr vor der letzten Frage geht, lasst uns doch bitte Feedback da.
- Übungszettel zum angeleiteten Reverse-Engineering: https://mal.re/tmp/coole-leute/uebungszettel/index.html

Das war’s, letzte Fragen?