PEEKABOOAV

NIGHTMARES AND FAIRYTALES

PEEKABOO EXTENDED EMAIL (K) ATTACHMENT BEHAVIOR OBSERVATION OWL

INHALTE

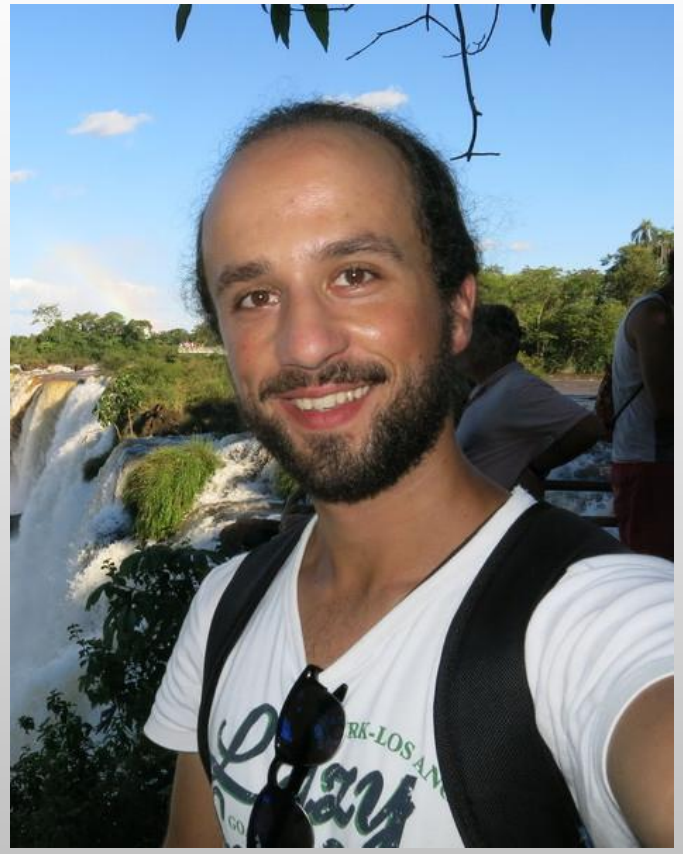
- Der Vortragende
- Was ist PeekabooAV
- Malware
- Vorgeschichte
- Herausforderungen
- Github Issues
- Zukunftspläne
- Nightmares
- Fairytales

Nightmares

Fairytales

FELIX BAUER

- IT-Sicherheitsmensch, Consultant und Engineer
- Entwickler von PeekabooAV von Tag -1
- Ethical Hacker
- Fablab Neckarälbler
- Arbeiter bei Science + computing ag an atos company



WAS IST PEEKABOO

- „PeekabooAV turns Cuckoo Sandbox into an AV.“
- „It‘s the connection between mail system and behaviour analysis.“
- „Peekaboo queues, schedules, checks, interprets and makes a decision.“

3,5 AUFGABEN

- Analysen verhindern um Ressourcen zu sparen
- Cuckoo zur Analyse veranlassen
- Report auswerten
- Entscheidung treffen

PEEKABOOAV – CUCKOO SANDBOX SCANNER FÜR AMAVIS

- Open Source Verhaltensanalyse von E-Mail-Anhängen
- Open Source Business Alliance Award Winner 2017

- Felix Bauer – Atos HPC security, s+c Security Solutions, Tübingen
- Sebastian Deiß - Security Solutions, München
- Christoph Herrmann - Services Nord, Berlin

@peekabooAV

GitHub scVENUS/PeekabooAV

YouTube Atos Tech Talks

ZIELE

- Moderne Technologie der Malware-Analyse nutzen und Viren finden
- Open Source Power nutzen und schaffen
- Den Cyber sicherer machen


PeekabooAV
1.6
@PeekabooAV
github.com/scvenus/PeekabooAV

OPEN SOURCE RELEASE

Open Source seit 19. May 2017

https://github.com/scVENUS/PeekabooAV

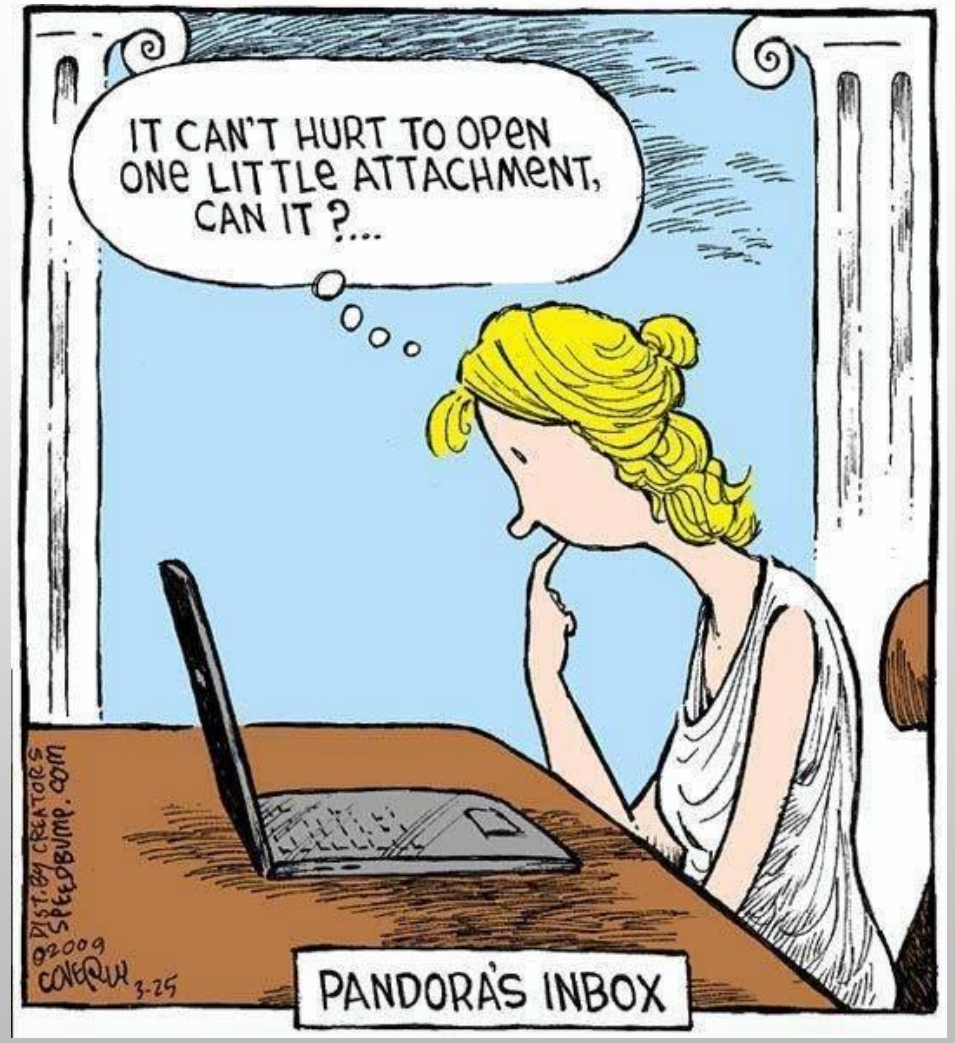
Verfügbar, nutzbar und erweiterbar von jedem!

GPLv3

Installer:
https://github.com/scVENUS/PeekabooAV-Installer

E-MAIL UND MALWARE

- Phishing
- E-Mail ist eines der Haupteinfallstore für Schadsoftware
- Bedroht Privatpersonen und Unternehmen
- Anhänge:
  - ZIP mit ausführbaren Dateien
  - JavaScript, Microsoft Office …
  - Ransomware
- Herausforderungen sind zahlreich und knifflig / hochinteressant / ZeroDays / APT


IT CAN'T HURT TO OPEN ONE LITTLE ATTACHMENT, CAN IT ?...
PANDORA'S INBOX
©2009 COVERLY 3-25
DIST. BY CREATORS SYNDICATE, INC. WWW.SPEEDBUMP.COM

DATEITYPEN VERBIETEN

exe	scr	bat	js	ps l
vbs	xls	pdf	ps	svg
jpg	png	html	docx	*

WAS BLEIBT ÜBRIG?

- [ ]
- Jede Datei kann potenziell eine Verbundbarkeit ausnutzen
- Inklusive der Mail selbst

VERHALTENSANALYSE !!

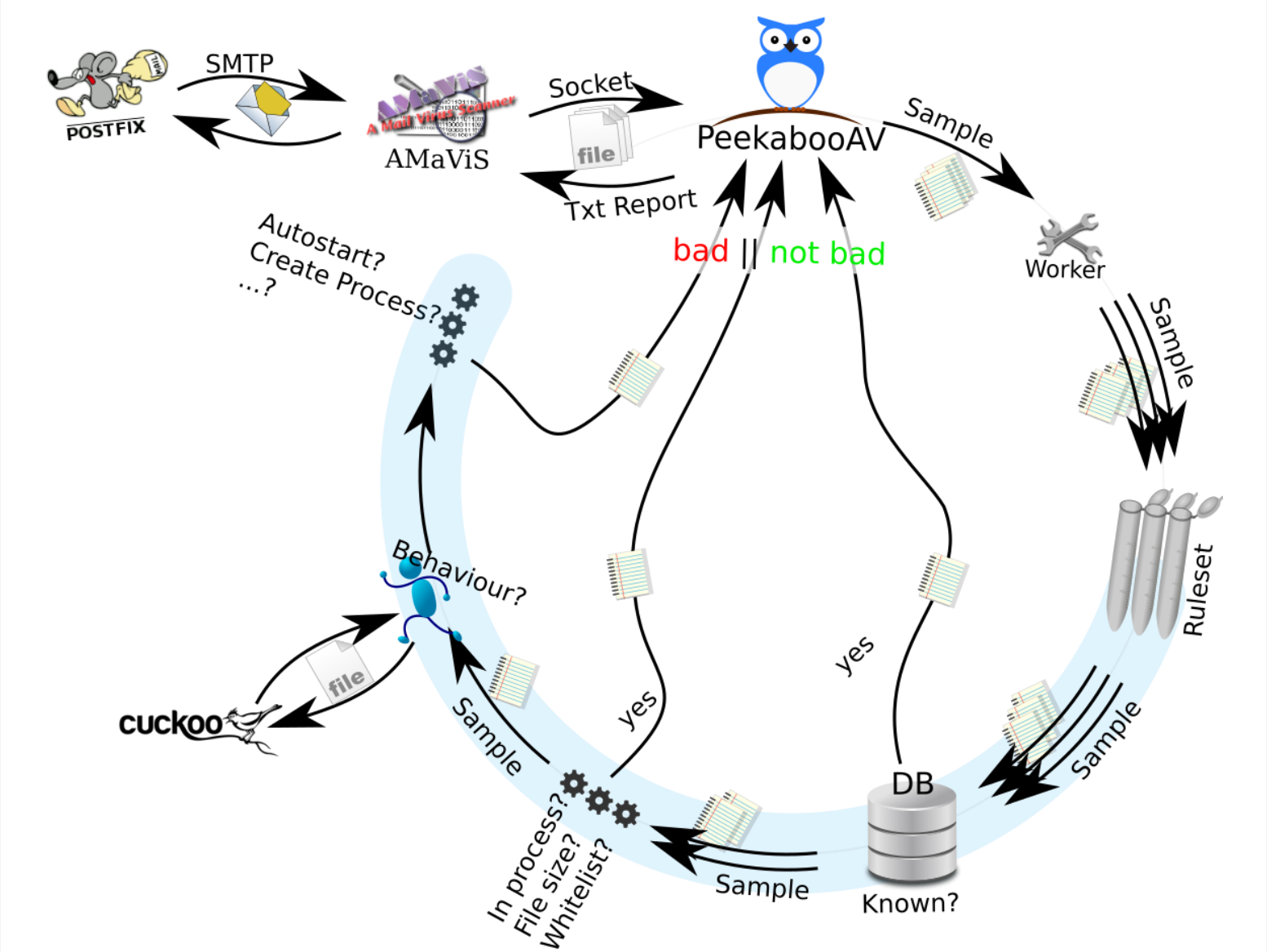
- Ausführung unter quasi normalen Bedingungen
- Beobachtung der Ausführung und Protokollierung der Ereignisse
- Auswertung

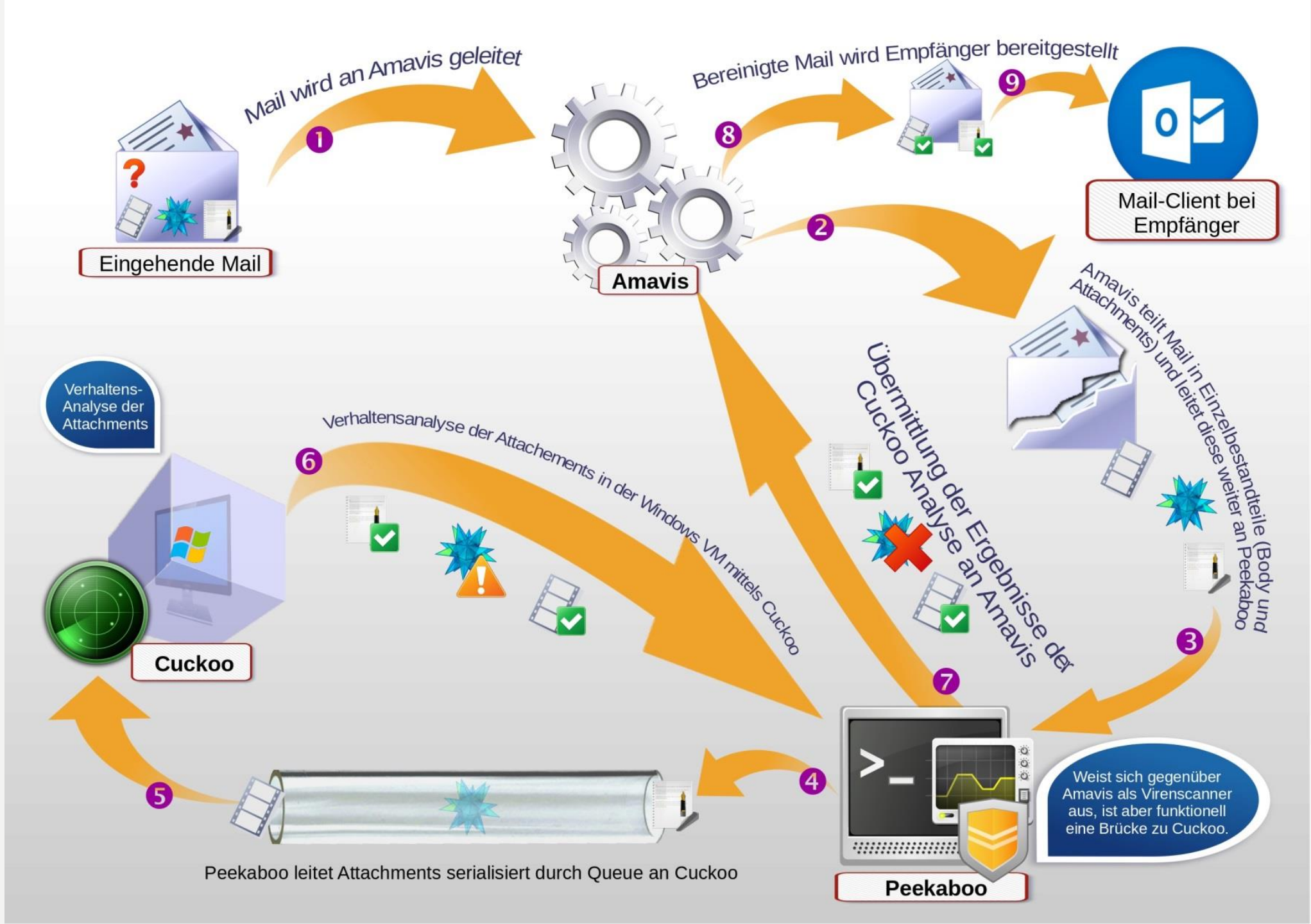
ABLAUF

- Peekaboo bekommt die nach Body und einzelnen Anhängen getrennte Mail
- Statische Tests zur Analyseverhinderung
- Übergabe an Cuckoo Sandbox
- Auswertung des Reports
- Entscheidung über die Schädlichkeit der Dateien
- Bericht an Amavis

ABLAUF

- Postifx
- SMTP
- Amavis
- File Socket
- Peekaboo
- Sample Datenstruktur
- Worker Threats
- Regelwerk
- Tests
- Informationsgewinnung
- Auswertung
- Bericht
- File Socket txt an Amavis
- Mail zurück ins Mailsystem
- Empfänger oder VirusAdmin




Mail wird an Amavis geleitet
1
Eingehende Mail
Amavis
2
Amavis teilt Mail in Einzelbestandteile (Body und Attachments) und leitet diese weiter an Peekaboo
3
Peekaboo
Weist sich gegenüber Amavis als Virenscanner aus, ist aber funktionell eine Brücke zu Cuckoo.
4
Peekaboo leitet Attachments serialisiert durch Queue an Cuckoo
5
Cuckoo
Verhaltens-Analyse der Attachments
6
Verhaltensanalyse der Attachements in der Windows VM mittels Cuckoo
7
Übermittlung der Ergebnisse der Cuckoo Analyse an Amavis
8
Bereinigte Mail wird Empfänger bereitgestellt
9
Mail-Client bei Empfänger

VIRUSMAIL

From Content-filter at turais.science-computing.de <postmaster@turais.science-computing...

Subject **VIRUS () in mail FROM [127.0.0.1]:59014 <security@turais.science-computing.de>** 10:19

To security@turais.science-computing.de

```
Content type: Virus
Internal reference code for the message is 04305-03/8eep-MkahEVZ

First upstream SMTP client IP address: [127.0.0.1] localhost

Return-Path: <security@turais.science-computing.de>
From: it-sec rulz <security@turais.science-computing.de>
Message-ID: <0087ab22-3a02-2ad4-9482-42e3faa7e662@turais.science-computing.de>
Subject: =?UTF-8?B?YsO2w7bDtsO2w7ZzZQ==?=
The message has been quarantined as: 8/virus-8eep-MkahEVZ

The message WAS NOT relayed to:
<security@turais.science-computing.de>:
   250 2.7.0 Ok, discarded, id=04305-03 - INFECTED:

Virus scanner output:
  Datei "p001":  Ergebnis "ignored" der Regel file_larger_than:188 - Datei ist nur 2 bytes lang (False)
  Die Datei "p001" wurde als "ignored" eingestuft

  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel file_larger_than:188 - Datei hat mehr als 5 bytes (True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel file_type_on_whitelist:203 - Dateityp ist nicht auf Whitelist (True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel file_type_on_greylist:227 - Dateityp ist auf der Liste der zu
analysiserenden Typen (True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel known:173 - Datei ist dem System noch nicht bekannt (True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel office_macro:318 - Die Datei beinhaltet kein erkennbares Office-Makro
(True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel file_larger_than:188 - Datei hat mehr als 5 bytes (True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel file_type_on_whitelist:203 - Dateityp ist nicht auf Whitelist (True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel file_type_on_greylist:227 - Dateityp ist auf der Liste der zu
analysiserenden Typen (True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel known:173 - Datei ist dem System noch nicht bekannt (True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel office_macro:318 - Die Datei beinhaltet kein erkennbares Office-Makro
(True)
  Datei "ccccccccccc.exe":  Ergebnis "unknown" der Regel requests_evil_domain:330 - Datei scheint keine Domains aus der Blacklist
kontaktieren zu wollen (True)
  Datei "ccccccccccc.exe":  Ergebnis "bad" der Regel cuckoo_evil_sig:264 - Folgende Signaturen wurden erkannt: ['A process
attempted to delay the analysis task.', 'Executes one or more WMI queries', 'Starts servers listening on {0}'] (False)
  Die Datei "ccccccccccc.exe" wurde als "bad" eingestuft
```

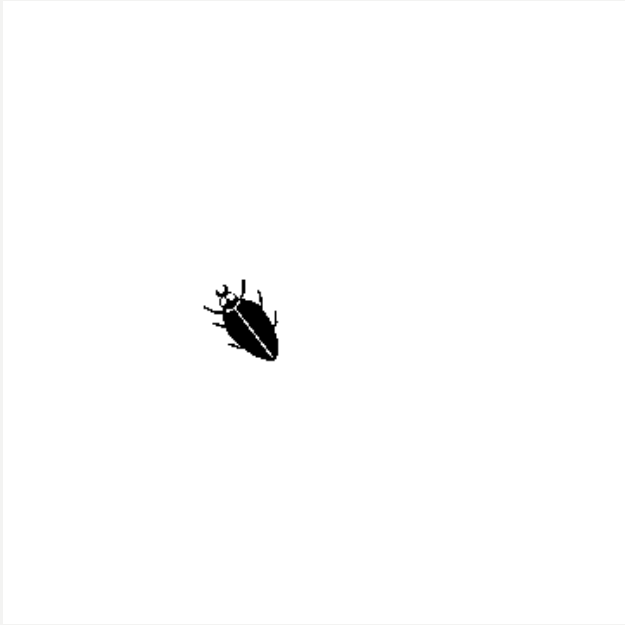
1 attachment: header.hdr 699 bytes Save

WEITERE DESASTER

AMAVIS

- „Ein Verbrechen in Perl“
- Industriestandard zur Anbindung von Virenscannern ans Mailsystem
- Unser Patch liefert mehr interne Informationen
- https://github.com/scVENUS/PeekabooAV-amavisd

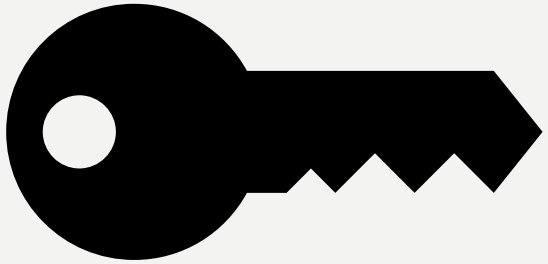
BUGS



- Bad things happen when an email has two identical attachments #
- MySQL Databank mit 170000 Einträgen kann problematisch sein (SQL Alchemy)

PKCS 7

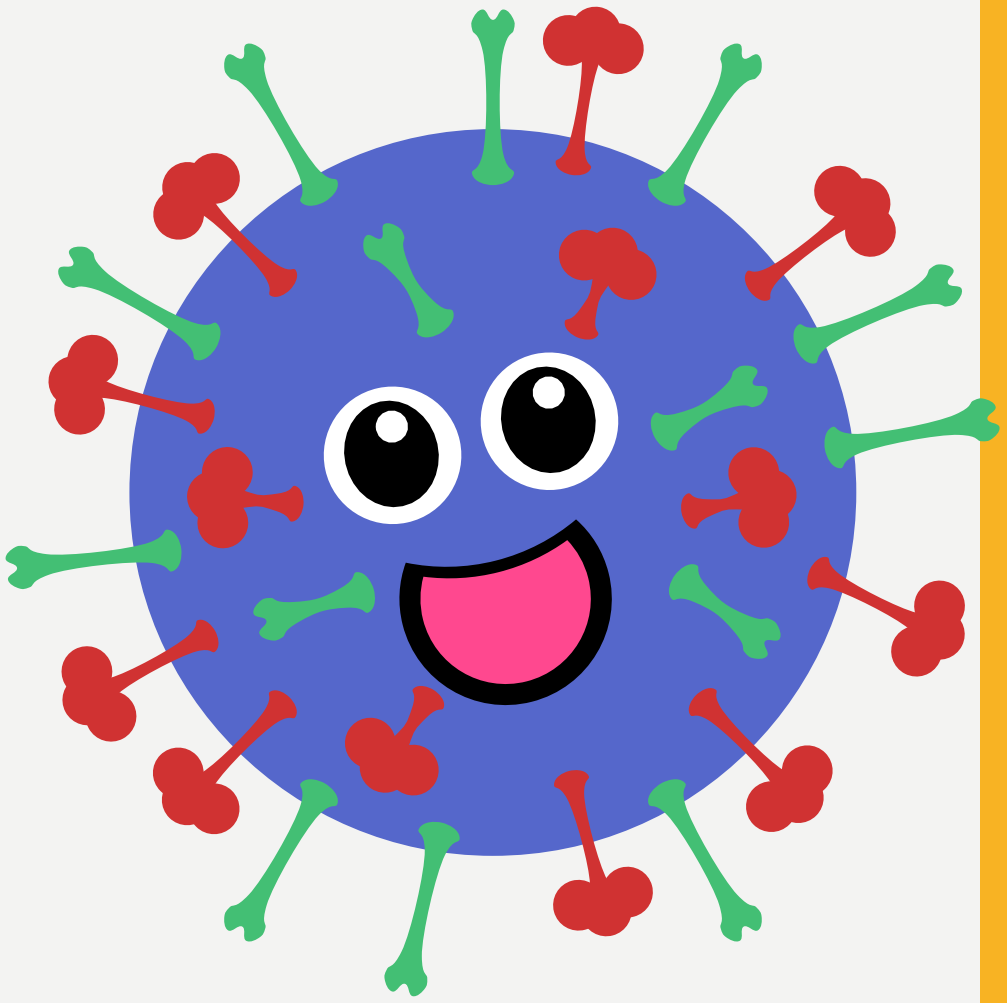
- octet-stream
- Mailsignatur (Crypto)
- smime.p7s
- Yara



MALWARE UND DEMO-MALWARE

- WanaCry

  https://asciinema.org/a/125910
- Macros
- Python Skripte
- Evil Application



WANACRY


Papierkorb
@WanaDecryptor...
@WanaDecryptor...
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
German
Was geschah mit meinem Computer?
Ihre wichtigen Dateien sind verschlüsselt.
Viele Ihrer Dokumente, Fotos, Videos, Datenbanken und andere Dateien sind nicht mehr zugänglich, weil sie verschlüsselt wurden. Vielleicht sind Sie damit beschäftigt, einen Weg zu finden, um Ihre Dateien wiederherzustellen, aber verschwenden Sie nicht Ihre Zeit. Niemand kann Ihre Dateien ohne unseren Entschlüsselungsdienst wiederherstellen.
Kann ich meine Dateien wiederherstellen?
Sicher. Wir garantieren, dass Sie alle Ihre Dateien sicher und einfach wiederherstellen können. Aber du hast nicht genug Zeit.
Sie können einige Ihrer Dateien kostenlos entschlüsseln. Versuchen Sie jetzt, indem Sie auf <Decrypt> klicken.
Aber wenn du alle deine Dateien entschlüsseln willst, musst du bezahlen.
Sie haben nur 3 Tage, um die Zahlung einzureichen. Danach wird der Preis verdoppelt.
Auch wenn du nicht in 7 Tagen bezahlt hast, kannst du deine Dateien nicht für immer wiederherstellen.
Wir haben freie Veranstaltungen für Benutzer, die so arm sind, dass sie nicht in 6 Monaten bezahlen können.
Wie bezahle ich?
Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf <About bitcoin>.
Payment will be raised on
11/20/2016 12:24:30
Time Left
02:23:59:52
Your files will be lost on
11/24/2016 12:24:30
Time Left
06:23:59:52
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt
Windows 7
Build 7601
Die Echtheit dieser Windows-Kopie wurde noch nicht bestätigt.
DE
12:24

ERSTE FUNDE

- Böse Word Dokumente …
- Andere AV-Lösung schlägt nicht an
- ClamAV und Trend Micro Office Scan 👍

SICHERHEITSLÜCKEN

SICHERHEITSLÜCKEN

- SHA256 vs. Fileextension
- Das Gleiche nochmal mit OneAnalysis ^^
- MIME-Types auf der Whitelist

DEBUGGING UND INFORMATIONFLOW

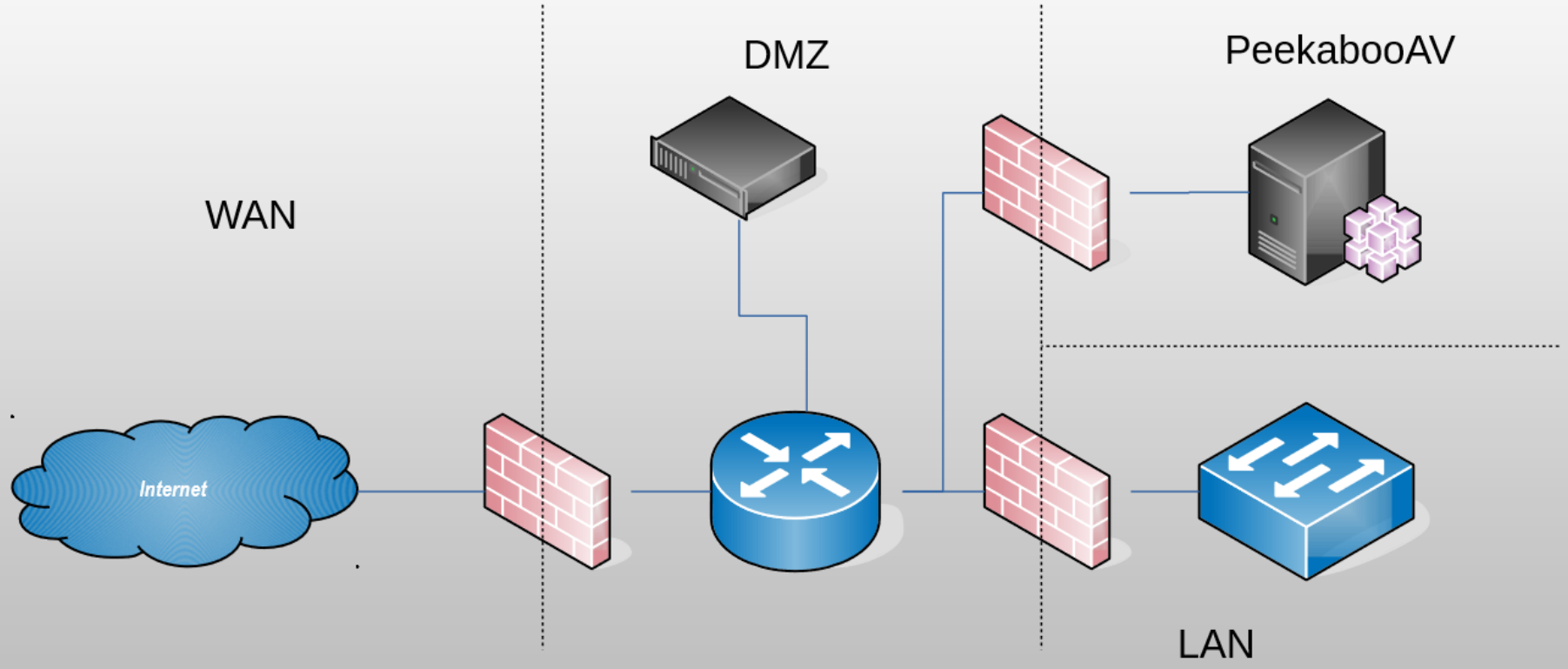
- Generelle Einführung

- From what you say I assume the mailer daemon is not configured properly and amavis can't reach peekaboo.

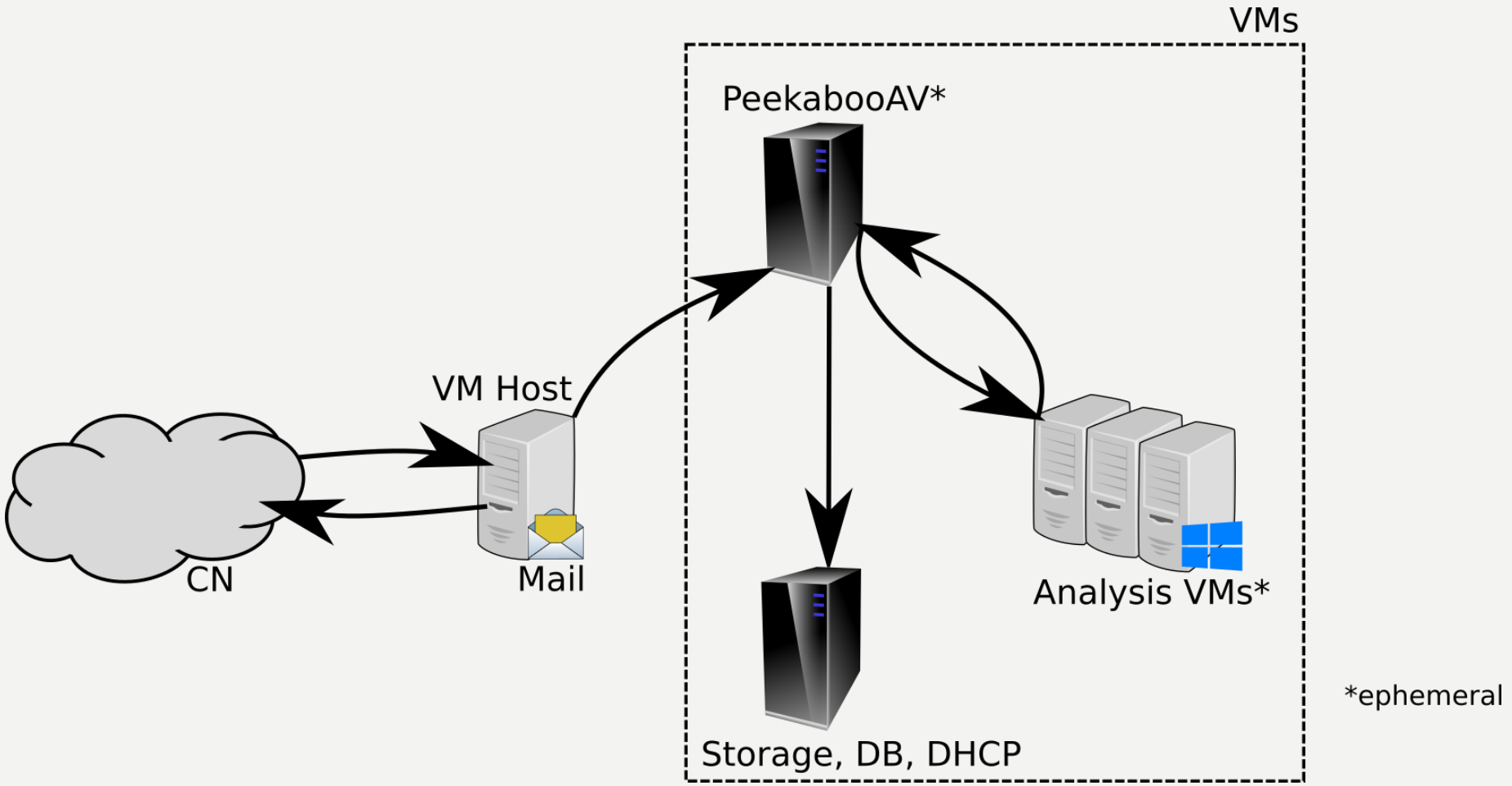
- Check paths to the peekaboo socket file in the amavis and peekaboo configuration
- Try to connect via smtp to amavis (127.0.0.1:10024) and hand in your message there
- Check local mail delivery and try again

- This way you test every step in the process and verify its correct and functional.

NETZWERKARCHITEKTUR



PEEKABOO APPLIANCE



SERVICES

- Postfix
- Amavis
- PeekabooAV
- Cuckoo Sandbox

Mehr und bessere Regeln

Weniger false positives

PeekabooAV 2.0

ALS NÄCHSTES:

ANGEBOTE

- Wir suchen:
  - Contributor
  - Neue Projekte
  - Neue Mitarbeite, Praktikanten, Abschlussarbeiten …

ZUKUNTFSMUSIK

- PeekabooAV 2.0
- MISP
- Cortex

- Neue Kollegen
- Praktika
- Abschlussarbeiten
- …

Cortex

MISP
Threat Sharing

DANKE FÜR IHRE AUFMERKSAMKEIT

- Felix Bauer

  felix@ai4me.de
- @PeekabooAV
- Github.com/scVenus/PeekabooAV

- Gerne Anfragen aller Art

- Liebe Kollegen:
  - Sebastian Deiß, Christoph Herrmann …

Grafiken von openclipart.org bzw. VRT Network Equipment Shapes, giphy, openclipart