PeekabooAV – Vom PoC zur Anwendung

OpenSource Verhaltensanalyse von E-Mail-Anhängen

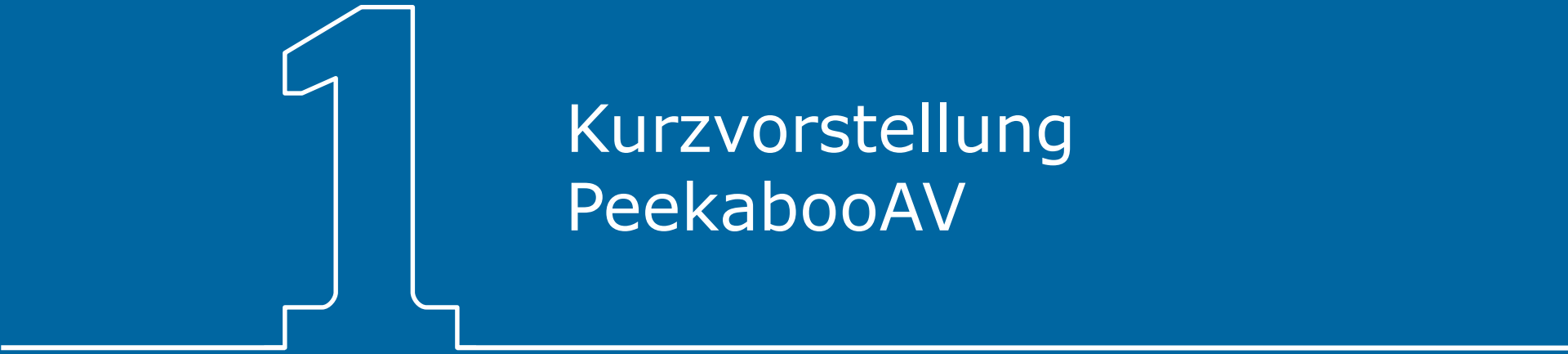
28.05.2019

Trusted partner for your **Digital Journey**

Atos

Übersicht

I. Kurzvorstellung PeekabooAV
II. Anforderungen an ein Mailsystem
III. Situation vor zwei Jahren
IV. Erfahrungen im Test- und Pilotbetrieb
V. Anpassungen an PeekabooAV (und auch an amavis und cuckoo)
VI. Aktueller Stand von PeekabooAV
VII. offene Punkte und Zukunft von PeekabooAV
VIII. Fragen



Kurzvorstellung PeekabooAV

PEEKABOO

Extend
Email
K
Attachment
Behavior
Observation
Owl

Die Idee von PeekabooAV

- Wir hätten gerne einen OpenSource Stack zur Verhaltensanalyse von E-Mail-Anhängen!
- Was gibt es schon an Software?
  - postfix
  - amavis
  - cuckoo
- Aber: Wie kommen die Attachments von amavis ins cuckoo?

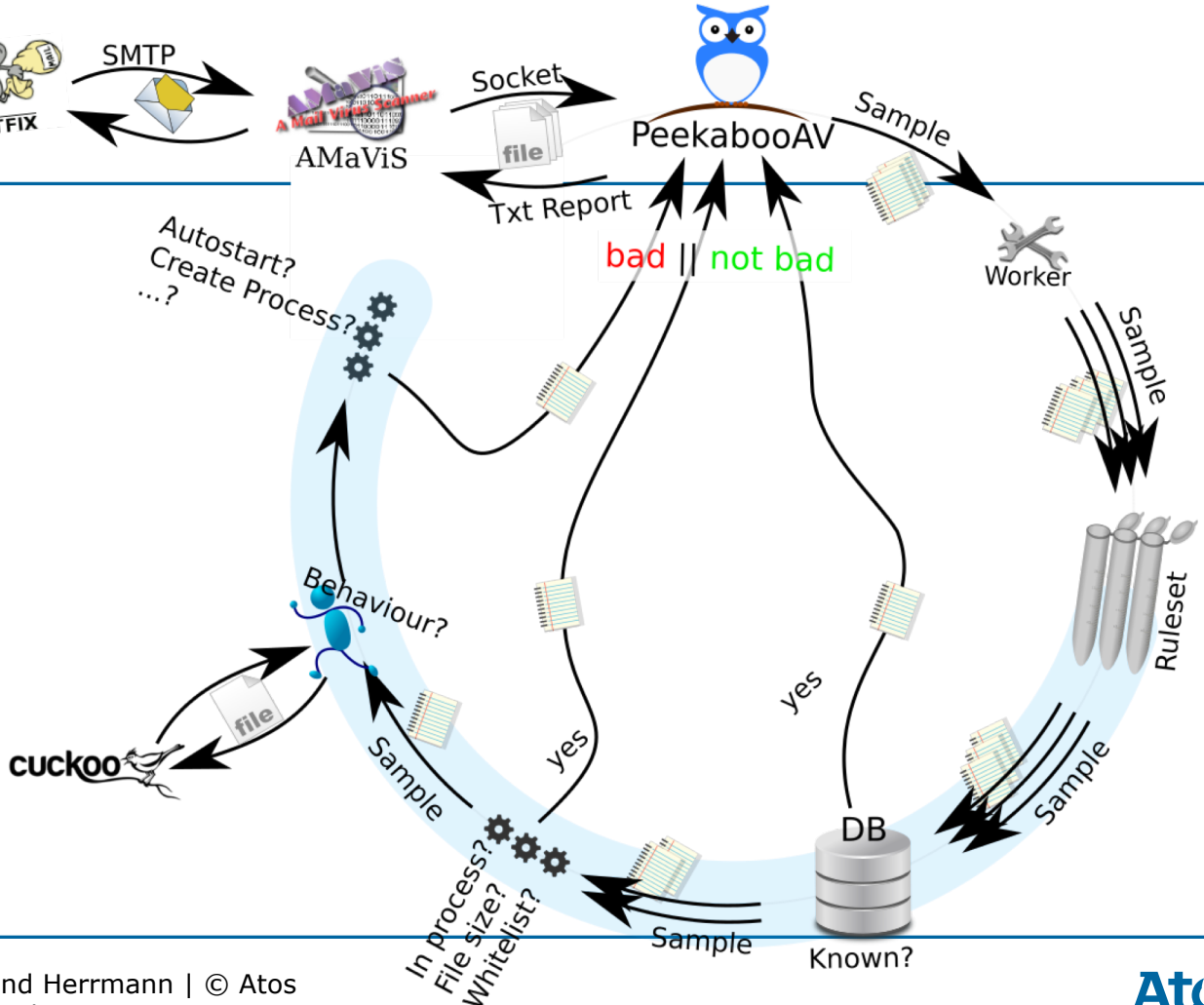
Da schreiben wir mal schnell ein Script :-).

Anforderugen an PeekabooAV

- muss sich amavis gebenüber wie ein Virenscanner verhalten
- braucht ein Regelwerk, welche Dateien in der Sandbox untersucht werden sollen und welche nicht
- muss eine Datenbank mit schon gescannten und in Bearbeitung befindlichen Dateien führen, um identisch Anhänge nicht mehrfach zu scannen
- braucht ein Regelwerk, um mit dem cuckoo report die Entscheidung BLOCKEN oder WEITERLEITEN zu treffen

Ablauf

- 1 Texteil
- 2 Anhang1
- 3 Anhang2
- Analyse:
- 1 ist auf whitelist
- 2 ist bekannt
- 3 started Powershell und ist **gefährlich**



Anforderungen an ein Mailsystem

Zuverlässigkeit

- Mailsysteme arbeiten autonom
- ein zuverlässiger Betrieb ohne manuelle Intervention muss gerwährleistet werden
- postfix und amavis sind stabil und erprobt
- cuckoo hat einen anderen Fokus (manuelles Hochladen von Samples)
- eine Fehlerrate von 1 zu 1000 ist für cuckoo o.k.
- **Aber nicht in einem Mailsystem!**
- PekabooAV muss mit Fehlern in cuckoo umgehen!

Skalierbarkeit

- PeekabooAV (das komplette System) skaliert nicht mit der Anzahl der Mails, sondern mit der Anzahl der Anhänge
- es gibt Mails mit mehreren hundert Anhängen
- das Untersuchen einer unbekannten Datei in cuckoo dauert ca. 1 min.
- ohne white/grey/blacklist und Datenbank mit laufenden und den Ergebnissen der abgeschlossenen Analysen nur schwer realisierbar
- wir brauchen Skalierung auf allen Ebenen:
  - paralleler Betrieb mehrerer PeekabooAV Instanzen mit einer DB ist notwendig
  - paralleler Betrieb mehrerer cuckoo Instanzen mit einer PeekabooAV Instanz wäre auch wünschenswert

3

Situation vor zwei Jahren

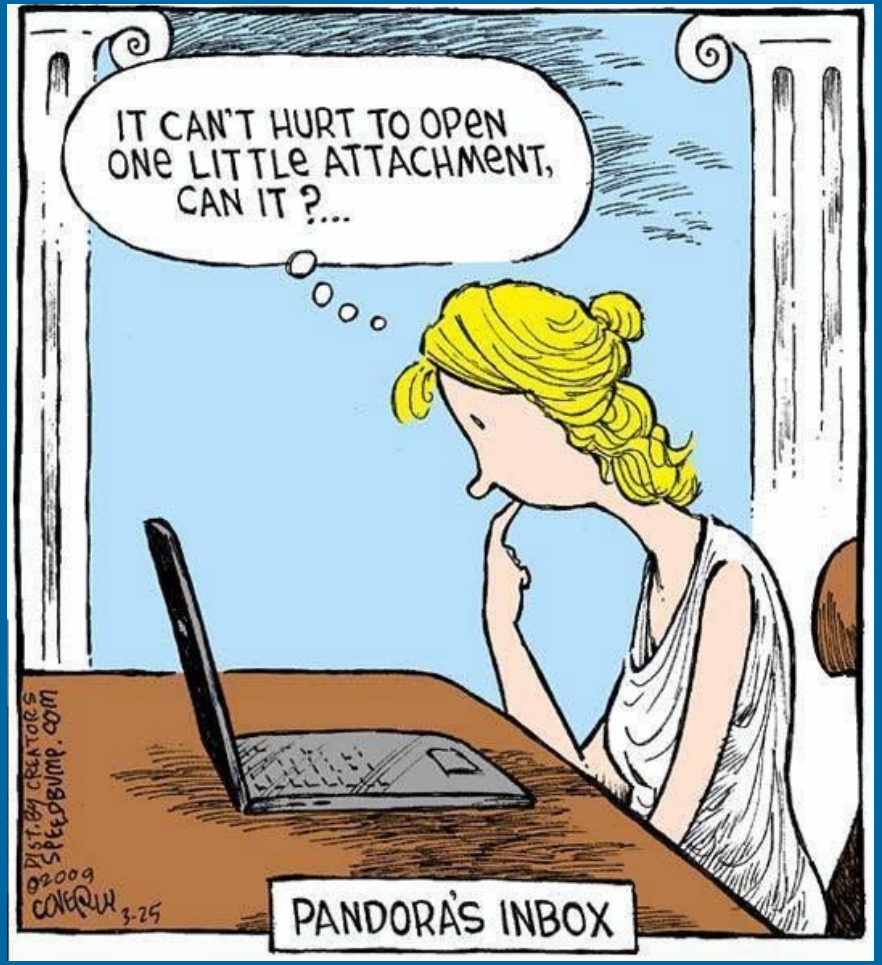
Proof of Concept

- SLAC 2017 :-)
- wir hatten einen (nahezu) featurekompletten PoC
- Verhaltenspattern ohne praktische Überprüfung
- das serielle Untersuchen von E-Mail-Anhängen hat funktioniert
- keine praktische Erfahrung mit realen E-Mails
- Das Prinzip funktioniert!

Erfahrungen im Test- und Pilotbetrieb

Beginn Testbetrieb

- Start mit 20 Mailadressen, eingebunden über recipient_bcc
- schneller Anstieg auf 100 Mailadressen
- sehr viele false postives wegen falscher Verhaltensmuster (ja, auch hier gibt es Muster, aber auf einer anderen Abstraktionsebene)
- die Verhaltensmuster müssen auch an den Kunden angepasst werden
- bei 200 Mailadressen erste Skalierungsprobleme
- Probleme mit dem Encoding der Dateinamen der Anhänge
- Bestätigung, daß E-Mail ein häßliches Format hat
- wie viele verschiedene MIME Types findet Ihr in einer Woche im Maillog?


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

Startseite Über uns Twitter durchsuchen Hast du einen Account? Anmelden

BSI @BSI_Presse · 14. Jan.

Nach einer Weihnachtspause wird seit heute Morgen wieder massenhaft #emotet-Spam verschickt. Achtung: Standard-AV erkennt die Malware oft (noch) nicht! Unternehmen und Privatanwender sollten sich unbedingt die BSI-Empfehlungen anschauen:
bsi.bund.de/DE/Presse/Pres…
(1/2)

7 111 69

BSI
@BSI_Presse

Folgen

… oder PeekabooAV verwenden

- beim Auftraggeber für die PeekabooAV Entwicklung hat PeekabooAV gezeigt, daß es diese Viren findet
- Traditionelle Virenscanner arbeiten mit Mustererkennung auf Dateiebene und versagen damit beim Erkennen polymorpher Viren
- PeekabooAV arbeitet mit Mustererkennung auf Verhaltensebene
- damit findet PeekabooAV auch polymorphe Viren wie Emotet zuverlässig
- **erste Probe erfolgreich bestanden!**

Anpassungen an PeekabooAV

Probleme mit PeekabooAV im Test- und Pilotbetrieb

- false positives
- Versagen bei bestimmten Mails/Anhängen
- Skalierung
- Encoding
- Stabilität (Abstürze von cuckoo oder PeekabooAV)

Anpassungen an (und um) PeekabooAV

- amavis plugin anstelle eines Patches/Forks von amavis
- Auslagern des Umgangs mit verschlüsselten Attachments an amavis
- Parallelbetrieb mehrerer PeekabooAV Instanzen mit einer zentralen DB und locking von Dateien, die gerade untersucht werden
- Verbesserter Umgang mit Encoding
- Verbesserung der Rückgabewerte für amavis (good/bad/unchecked)
- stark verbesserte Fehlerbehandlung im ganzen Code
- generell grosse Verbesserungen der Codequalität (git-lint)
- Lokalisierung der Kommunikation mit amavis
- Beginn Testsuite / Continuous Integration

Fortsetzung Anpassungen an PeekabooAV

- Python 3 Support (cuckoo ist in Python 2 geschrieben)
- Programmieren/Verbessern des Installers:
  - Verwendung von Ansible
  - seperate virtualenvs (getrennte Abhängigkeiten für cuckoo und PeekabooAV)
  - Vorbereitung für verteilte Installation
- Umstellung auf cuckoo REST API für den Jobsubmit
- Beginn Programmierung von Regeln mit logischen Verknüpfungen
- Programmierung Proxmox Anbindung für cuckoo (offener Mergerequest bei cuckoo)

Aktueller Stand von PeekabooAV

Testbetrieb

- 5200 Teilnehmer
- es werden nur eingehende Mails gescannt
- ca. 15.000 Mails/35.000 Attachments am Tag
- weniger als ein false positive im Monat
- Weniger als 10 Mails im Monat, die “Hängen bleiben“
- Verbesserungen im letzten Jahr:
  - Steigerung des Durchsatzes um einen Faktor 100 (gleiche HW)
  - Reduzierung false positves um mehr als einen Faktor 1.000
  - Reduzierung hängende Mails um einen Faktor 30
- **Umstellung auf Produktivbetrieb möglich und geplant**

Why GitHub? Enterprise Explore Marketplace Pricing Search / Sign in Sign up

scVENUS / PeekabooAV

Watch 14 Star 28 Fork 8

Code Issues 14 Pull requests 1 Projects 0 Wiki Security Insights

- Pulse
- Contributors
- Commits
- Code frequency
- Dependency graph
- Network
- Forks

April 27, 2019 – May 27, 2019

Period: 1 month

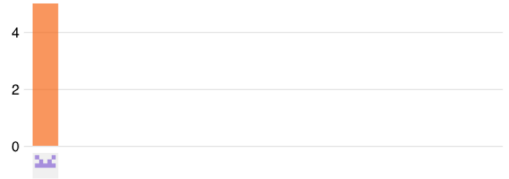
Overview

3 Active Pull Requests

4 Active Issues

2	1	3	1
Merged Pull Requests	Proposed Pull Request	Closed Issues	New Issue

Excluding merges, **1 author** has pushed **5 commits** to master and **5 commits** to all branches. On master, **16 files** have changed and there have been 1,079 **additions** and 614 **deletions**.



2 Pull requests merged by **1** person

Merged #84 Orig filename 19 days ago

Why GitHub? Enterprise Explore Marketplace Pricing Search / Sign in Sign up

scVENUS / PeekabooAV

Watch 14 Star 28 Fork 8

Code Issues 14 Pull requests 1 Projects 0 Wiki Security Insights

- Pulse
- **Contributors**
- Commits
- Code frequency
- Dependency graph
- Network
- Forks

May 14, 2017 – May 28, 2019

Contributions: **Commits**

Contributions to master, excluding merge commits

Offene Punkte und Zukunft von PeekabooAV

Offene Punkte

- Unterstützung von rspamd
- REST API für PeekabooAV
- Verbesserte Testsuite
- Verbessern Continuous Integration
- Implementierung eines verbesserten Regelwerkes mit logischen Verknüpfungen
- Erkennung von Angriffen auf den Mailclient
- Offene Punkte cuckoo:
  - Geplanter Umstieg auf Proxmox als Hypervisor
  - Tests mit ESX

Ein Wort zum Scanclient

- cuckoo benötigt clients (bevorzugt VMs) in denen die Anhänge untersucht werden
- das muss nicht in jedem Fall Windows+MS Office sein
- wieviel verschiedene PDF Viewer gibt es?
- kundenspezifische Spezialsoftware
- diese Scanclients sind nicht Bestandteil von PeekabooAV sondern sollten vom Endanwender/Kunde kommen
- dann wird das Verhalten des Anhangs in genau der Umgebung getestet, in der Anwender den Anhang öffnen
- Teilweise werden Lizenzen für den Scanclient und dessen Software benötigt

Zukunft von PeekabooAV

- PeekabooAV ist OpenSource!
- Wie freuen uns über Verwendung, Anregungen, Unterstützung, Mitarbeit, Patches, Merge Requests, ...
- PeekabooAV hängt an cuckoo
  - leider scheint die Entwicklung von cuckoo eingeschlafen zu sein
- Vielleicht mag sich jemand bei cuckoo engagieren?

Fragen

Vielen Dank

Atos BDS
science + computing ag
Hagellocher Weg 73
72070 Tübingen

T+ 49 7071 9457 0

@PeekabooAV
felix.bauer@atos.net
michael.weiser@atos.net
christoph.herrmann@atos.net