

PeekabooAV – der Weg zu Version 2.0

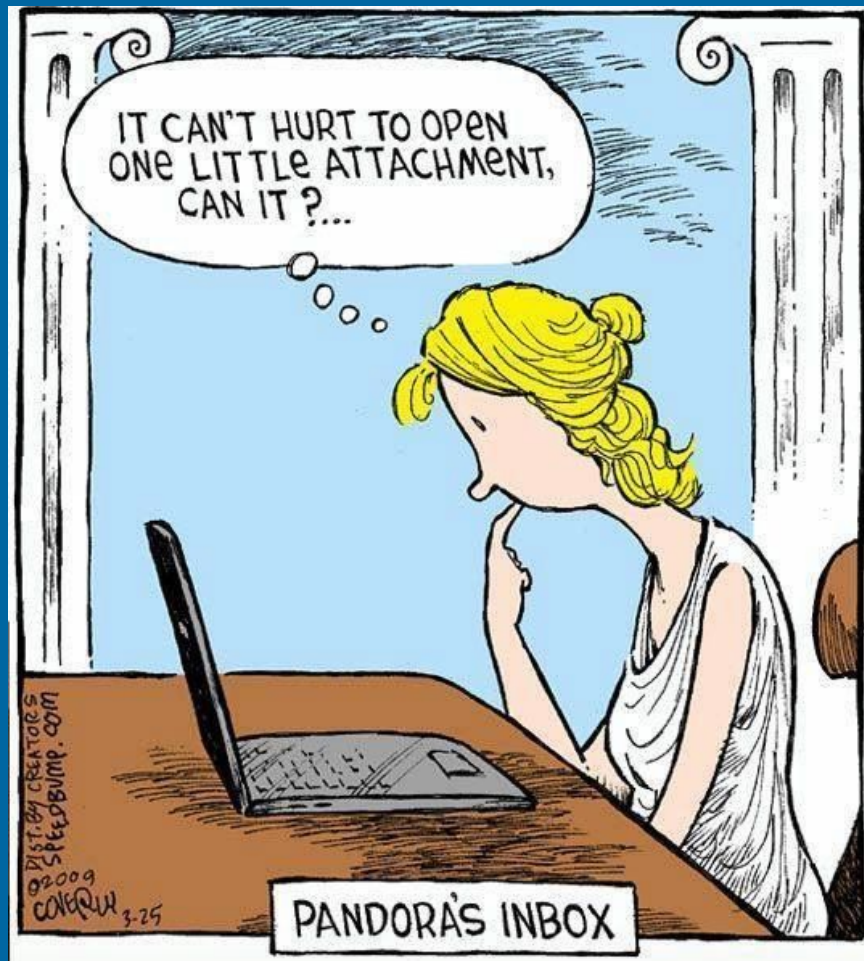
Open Source Behavioral Analysis of Email Attachments

06.07.2019

Trusted partner for your Digital Journey



Atos



Deswegen PeekabooAV

PeekabooAV, the link between amavis and cuckoo

„auditable state of the art Malware detection with OpenSource Software“

„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 Things PeekabooAV does

Avoid analysis to save resources

```
graph TD; A[Avoid analysis to save resources] --> B[Submit to Cuckoo for behavior analysis]; B --> C[Report evaluation]; C --> D[Decision making (good / bad / very bad)]
```

Submit to Cuckoo for behavior analysis

Report evaluation

Decision making (good / bad / very bad)

Prerequisites for PeekabooAV

- ▶ Any Linux, preferred Ubuntu 18.04 or Proxmox
- ▶ Any Hypervisor, preferred VirtualBox or Proxmox
- ▶ Standard SMTP server (preferred Postfix)
- ▶ PeekabooAV + Cuckoo will run in VMs on the host
- ▶ MySQL Database (can run on the host or in a VM)
- ▶ Client VM Image from the customer, which needs to be modified a bit
 - PeekabooAV does not provide scan clients
 - Uses images provided by the customer which provide the best adapted protection: we see what possibly could happen on customer clients
- ▶ PeekabooAV communicates via SMTP, it can easily be integrated in any SMTP stream (e.g. between external MTAs in a DMZ and internal Exchange servers)

Wie alles begann!

- E-Mail
- Anhänge
- Problem

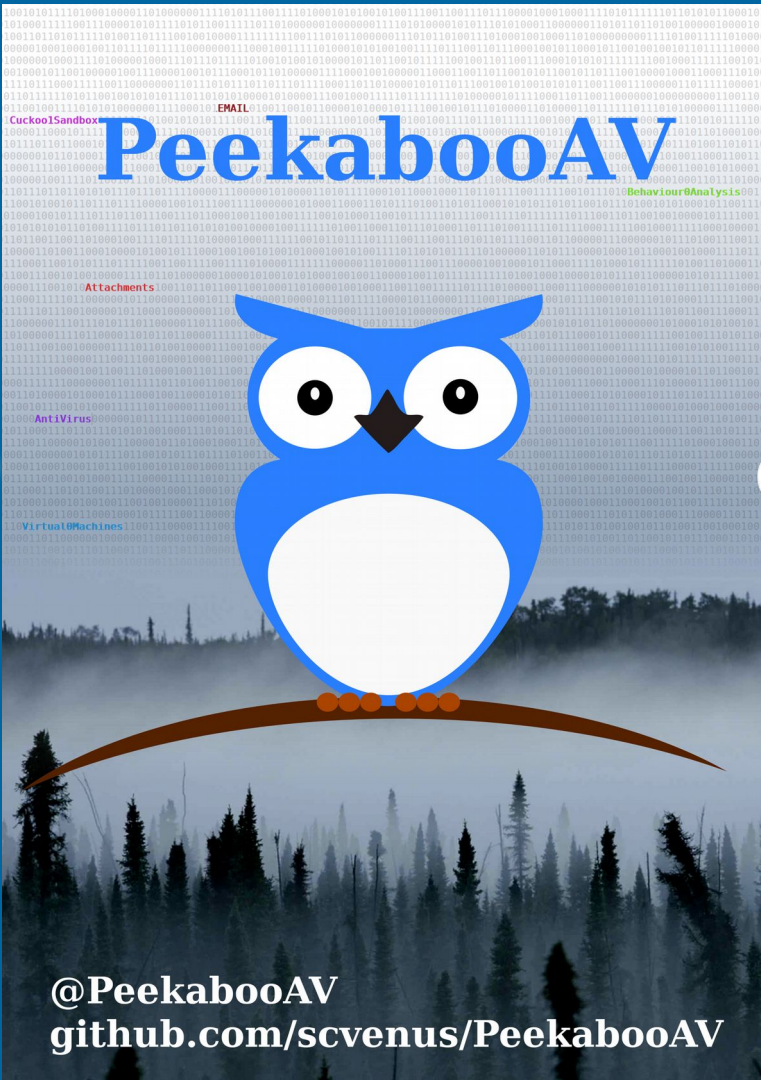
?



ein lieber
Kunde







@PeekabooAV
github.com/scvenus/PeekabooAV



Heinlein



Akademie



Consulting



Hosting



Heinlein Akademie: Unsere Schulungen & Kurse

/ Unser Kursangebot

/ Die Kurse im Zusammenspiel

/ Unsere Dozenten

/ Details und Rabatte

/ Meinungen der Teilnehmer

/ Online-Anmeldung

Inhouse-Schulungen

Mailserver-Konferenz

Secure Linux Administration Conference

/ Programm 2019

/ Bilder der SLAC 2019

/ Meinungen der Teilnehmer

/ Anmeldung & Infos

/ Ort, Hotel und Anreise

DER CUCKOO SANDBOX-SCANNER FÜR AMAVIS

Das Erkennen von Schadsoftware ist heutzutage extrem schwer geworden. Traditionelle Virens Scanner arbeiten mit Pattern. Polymorphie verhindert die Erkennung durch Pattern. Um dieser modernen Schadsoftware nicht komplett schutzlos ausgeliefert zu sein, werden neue Verfahren benötigt.

Die Verhaltensanalyse ist eines dieser modernen Verfahren, um größere Mengen an Informationen zu einem gegebenen Sample zu produzieren und darauf erweiterte Tests auszuführen. Cuckoo ist ein OpenSource Projekt zur Verhaltensanalyse von Samplen.

Es gibt bis jetzt noch keine Möglichkeit, cuckoo in ein Mailsystem einzubinden. Diese Aufgabe soll Peekaboo übernehmen. Peekaboo ist eine Schnittstelle von amavis zu cuckoo.

Der Vortrag ist die öffentliche Premiere von Peekaboo.

Referent:

Christoph Herrmann ist Solution Architect bei der Atos BDS in Berlin und betreut dort als Schwerpunkt OpenSource Software, auch und vor allem OpenSource Mailsysteme, bei Enterprise Kunden.

Felix Bauer ist IT-Security Engineer und Consultant bei Atos in Tübingen, er entwirft und erstellt Security-Lösungen im Bereich Netzwerk, Malware und Hacking, er ist IT-Security-

Haben Sie Fragen?

Simone Rosenberg
Tel. 030/40 50 51-40
mail@heinlein-akademie.de

Anfrage

CompetenceCall



Blog: Heinlein Support

→ Rspamd – Neuigkeiten in 1.9.0

o to...



[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)

 **scVENUS / PeekabooAV**

 Unwatch ▾

14

 Unstar

29

 Fork

8

 Code

 Issues **12**

 Pull requests **1**

 Projects **0**

 Wiki

 Security


 Insights

 Settings

Import from our internal VCS

[Browse files](#)

 master  v1.7  bt-test-1.0.b

 **Sebastian Deiss** committed on 23 May 2017

1 parent [620029c](#)

commit [6dc0dbb6fc0f59b454d6f384f348d4a8634b6d06](#)

 Showing **37 changed files** with 4,088 additions and 102 deletions.

Unified

Split

Sonder-OSBAR – Public Sector für PeekabooAV

Die Entwicklung von [PeekabooAV](#) wurde maßgeblich von einer großen Bundesbehörde gefördert und folgt so dem Kredo und Wunsch

der OSB Alliance: Software, die mit öffentlichen Geldern finanziert und entwickelt wird, muss auch im Quelltext der Öffentlichkeit

zur Verfügung gestellt werden. Für diese Quasi-Pionierrolle gibt es den Sonder-OSBAR Public-Sektor für PeekabooAV.



8. Dezember 2017

Christoph Herrmann, Felix Bauer, Sebastian Deiss

Suche

OSB Alliance Trust matters.



STAY CONNECTED



325 Fans

GEFÄLLT MIR



1,059 Follower

FOLGEN



NEWSLETTER-ANMELDUNG

Anstehende Veranstaltungen

Podiumsdiskussion „Von Fake News zu Deep Fake – was Journalisten wissen sollten“

10. Juli

Nürnberg Digital Festival 2019



@PEEKABOO AV 1.4

Vorschau *Februar 2018*

Auf Malware-Fang

E-Mail-Anhänge sind heute ein Haupteinfallstor für Schadsoftware. Klassische Virens Scanner haben gerade bei neuer Ransomware Schwierigkeiten mit der Erkennung. Peekaboo verbessert dies, indem die Software eine Brücke zwischen AMaViS und einer Cuckoo-Sandbox zur Analyse von E-Mail-Attachments baut.



Stucki (2018) - IPA Proof of Concept
(PoC) Mail-Security Gateway mit
Verhaltensanalyse von Mailanhängen
mittels Sandboxing

PeekabooAV



1.6

@PeekabooAV
github.com/scvenus/PeekabooAV



Evaluierung und Erweiterung von PeekabooAV zur Detektierung von Malware in E-Mail Anhängen

Studienarbeit

des Studiengangs Informationstechnik

an der Dualen Hochschule Baden-Württemberg Stuttgart

von

Raphael Nonnenmann und Jan-Ruben Schmid

04.06.2018

PeekabooAV



1.7

Happy Easter



Peekaboo AV

Workshop and Developers meeting

2.5.2019



```
182 class CuckooRule(Rule):
183     """ A common base class for rules that evaluate Cuckoo reports. """
184     def evaluate(self, sample):
185         """ If a report is present for the sample in question we call method
186         evaluate_report() implemented by the subclasses to evaluate it for
187         findings. Otherwise we submit the sample to Cuckoo and raise
188         PeekabooAnalysisDeferred: if the sample was submitted to Cuckoo
189         until the report arrives. If submission to Cuckoo fails we will
190         ourselves report the sample as failed.
191         @param sample: The sample to evaluate.
192         @raises PeekabooAnalysisDeferred: if the sample was submitted to Cuckoo
193         @returns: RuleResult containing verdict.
194         """
195         report = sample.cuckoo_report
196         if report is None:
197             try:
198                 job_id = sample.submit_to_cuckoo()
199             except CuckooSubmitFailedException:
200                 logger.error("Submit to Cuckoo failed: %s", failed)
201                 # exception message intentionally not present in message
202                 # delivered back to client as to not disclose internal
203                 # information, should request user to contact admin instead
204                 return self.result(
205                     Result.failed,
206                     ("Behavioral analysis by Cuckoo has produced an error "
207                     "and did not finish successfully"),
208                     False)
209             logger.info('Sample submitted to Cuckoo. Job ID: %s.',
210                         'Sample: %s', job_id, sample)
211             raise PeekabooAnalysisDeferred()
212         # call report evaluation function if we get here
213         return self.evaluate_report(report)
214
215 def evaluate_report(self, report):
216     """ Evaluate a Cuckoo report.
217     @param report: The Cuckoo report.
218     @returns: RuleResult containing verdict.
219     """
220     raise NotImplementedError
221
222 class CuckooEvilSigRule(CuckooRule):
223     """ A rule evaluating the signatures from the Cuckoo report against a
224     of signatures considered bad. """
```

PeekabooAV

–

**Erweiterung eines Open-Source-Projektes aus dem
IT-Security- und Malware-Bereich**

Studienarbeit 5. und 6. Theoriephase

des Studienganges Angewandte Informatik

an der Dualen Hochschule Baden-Württemberg Stuttgart

von

Sandra Fischer

03.06.2019

Heute



ANSIBLE



VAGRANT

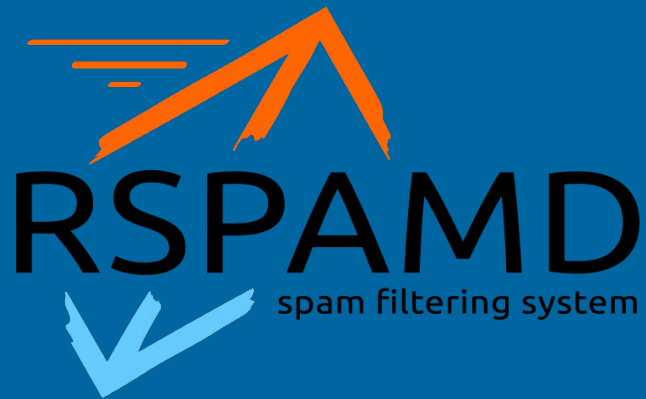


dnsmasq



INetSim

Morgen



github.com/scvenus/PeekabooAV

github.com/scvenus/PeekabooAV-Installer

twitter.com/PeekabooAV

← Links

`pip install PeekabooAV`

gitter.im/PeekabooAV/Lobby

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



Atos