



Fakultät für Informatik

FWPM Penetrationstests und Forensik

Abschlussbericht Forensik

von

Daniel Böning

Jonathan Hamberger

Osman Güloglu

Karl Herzog

# Inhaltsverzeichnis

<b>1</b>	<b>Analyse des kompromittierten Systems</b>	<b>1</b>
1.1	Einleitung . . . . .	1
<b>2</b>	<b>Analyse des Systems</b>	<b>2</b>
2.1	Vorbereitung . . . . .	2
2.2	File Records in Master File Table (MFT) . . . . .	2
2.3	Prefetch-Files . . . . .	3
2.4	Registry-Analyse . . . . .	3
2.5	Wireshark Analyse . . . . .	5
2.6	Prozessliste . . . . .	6
<b>3</b>	<b>Weitere Aktivität des Angreifers</b>	<b>7</b>
<b>4</b>	<b>Möglicher Datendiebstahl</b>	<b>9</b>
	<b>Literaturverzeichnis</b>	<b>10</b>

# **1 Analyse des kompromittierten Systems**

## **1.1 Einleitung**

Beim Reiseveranstalter „hVs-Reisen“, der auf Reisen nach Nordkorea spezialisiert ist, kam es am Nachmittag des 14.11.2017 zu einem Security Incident, nachdem der Virens Scanner auf dem virtuellen Client des Mitarbeiters Lars Walter eine Malware erkannt hatte.

Das Forensik Team wurde daraufhin beauftragt, das betroffene System einer forensischen Analyse zu unterziehen. Der vorliegende Bericht gliedert sich in eine sog. Management Summary, in welcher die wichtigsten Ergebnisse der Untersuchung in kompakter Form dargestellt sind. Im Anschluss daran folgt eine detaillierte Aufstellung der Vorgehensweise und Ergebnisse, in der speziell auf die Fragen des Kunden eingegangen wird. Abgeschlossen wird der Bericht mit Handlungsempfehlungen für den Kunden von Seiten des Forensik Teams.

## 2 Analyse des Systems

### 2.1 Vorbereitung

Zur Durchführung der forensischen Analyse wurden dem Team zwei Sicherungsdateien des betroffenen Clients des Mitarbeiters Lars Walter zur Verfügung gestellt. Dabei handelt es sich zum Einen um die Sicherung des Arbeitsspeichers *client-walter.vmem* und zum Anderen um ein Image der Festplatte (*client-walter.vmem*). Zu Beginn wurde die Integrität der Images überprüft. Dabei wurden vom Team die Hashwerte der beiden Dateien mit dem CertUtil Befehl ermittelt und mit den vom Kunden zur Verfügung gestellten Hashwerten verglichen.

Datei	Sicherungszeitpunkt	MD5	SHA1	SHA256
client-walter.vmem	14.11.17 16:00 Uhr	korrekt	korrekt	korrekt
client-walter.e01	27.11.17 14:00 Uhr	korrekt	korrekt	korrekt

Da eine Übereinstimmung der Hashwerte festgestellt wurde, konnte davon ausgegangen werden, dass die Daten korrekt übermittelt wurden. Sie konnten daher zur weiteren forensischen Analyse herangezogen werden.

### 2.2 File Records in Master File Table (MFT)

Die MFT-Datei des betroffenen Clients wurde mithilfe von FTK Imager extrahiert und anschließend mithilfe von Mft2csv in eine CSV-Datei umgewandelt. Als Ergebnis lässt sich Folgendes festhalten: Im Cache für Email-Anhänge konnte die Existenz einer .zip- Datei Temp1\_171110\_NorthKorea-DiploimaticUpdate.zip nachgewiesen werden, in der die eigentliche Malware enthalten war. 171110\_NorthKorea-DiploimaticUpdate.pdf.exe Darüber hinaus konnte eine entsprechende Prefetch-Datei 171110\_NORTHKOREA-DIPLOIMATIC-3B19E785.pf nachgewiesen werden. Dies ist in Abbildung 2.1 ersichtlich.

99164	4	171110~1.LNK	:\Users\walter\AppData\Roaming\Microsoft\Windows\Recent\171110_NorthKorea-DiploimaticUpdate.lnk	FILE	ALLOCATED
125028	5	171110~1.EXE	:\Users\walter\Documents\Work\E-Mails\Attachment-Export\171110_NorthKorea-DiploimaticUpdate.pdf.exe	FILE	ALLOCATED
99301	2	TEMP1_~1.ZIP	:\Users\walter\AppData\Local\Temp\Temp1_171110_NorthKorea-DiploimaticUpdate.zip	FOLDER	ALLOCATED
110382	28	PLATF~1	:\Users\walter\AppData\Local\Google\Chrome\User Data\CertificateTransparency\570\_platform_specific	FOLDER	ALLOCATED
92917	1	171110~1.PF	:\Windows\Prefetch\171110_NORTHKOREA-DIPLOIMATIC-3B19E785.pf	FILE	ALLOCATED

Abbildung 2.1 MFT

### 2.3 Prefetch-Files

Mithilfe des Tools PECmd wurde das zur Malware gehörende Prefetch-File `/Windows/Prefetch/171110_NORTHKOREA-DIPLOIMATIC-3B19E785.pf` analysiert. Das Ergebnis ist in Abbildung 2.2. Es konnte nachgewiesen werden, dass die Malware zuletzt am 13.11.17 um 16:27 Uhr ausgeführt wurde. Dies lässt den Schluss zu, dass der Client des Mitarbeiters schon einen Tag vor dem Security Incident am 14.11.17 kompromittiert war.

```
PECmd version 1.3.4.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd
Command line: -d C:\Users\forensics\Desktop\ptf2021-evidences\CLIENT-WALTER\Prüfungsaufgabe\Export\
Warning: Administrator privileges not found!
Keywords: temp, tmp
Looking for prefetch files in 'C:\Users\forensics\Desktop\ptf2021-evidences\CLIENT-WALTER\Prüfungsaufgabe\Export\'
Found 1 Prefetch files
Processing 'C:\Users\forensics\Desktop\ptf2021-evidences\CLIENT-WALTER\Prüfungsaufgabe\Export\171110_NORTHKOREA-DIPLOIMATIC-3B19E785.pf'
Created on: 2020-11-06 13:16:20
Modified on: 2020-11-06 13:16:20
Last accessed on: 2020-11-06 13:16:20
Executable name: 171110_NORTHKOREA-DIPLOIMATIC
Hash: 3B19E785
File size (bytes): 36.358
Version: Windows 10
Run count: 1
Last run: 2017-11-13 16:27:38
```

Abbildung 2.2 MFT

### 2.4 Registry-Analyse

Es wurde eine Analyse der Registry Dateien NTUSER.dat, SYSTEM.dat, SAM.dat, SECURITY.dat und SOFTWARE.dat durchgeführt. Diese Dateien wurden aus dem Dateisystem des kompromittierten Rechners extrahiert und mit dem Programm RegRipper analysiert.

Die NTUSER Datei enthielt folgenden Eintrag unter dem Abschnitt UserAssist:

*Mon Nov 13 16:27:38 2017*

*C:\Users\walter\Documents\Work\EMails\Attachment-Export\171110\_NorthKorea-DiploimaticUpdate.pdf.exe (1)*

Abbildung 2.3 Pfad zur verdächtigen Datei

Diese Datei konnte aus dem Dateisystem des betroffenen Rechners extrahiert werden und wurde mit VirusTotal analysiert. In Abbildung 2.4 sind die Ergebnisse von VirusTotal zu sehen.

## 2 Analyse des Systems

49 / 71

49 engines detected this file

657776945c92874342f15fa2456dd80ad76eace94ce20b901d58c31fcd5018a  
171110\_NorthKorea-DiploimaticUpdate.pdf.exe

3.41 MB Size | 2020-10-29 14:05:41 UTC a moment ago

Community Score: ☒ peexe

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis	Suspicious	Ad-Aware	Generic.Exploit.Shellcode.2.50EF6B94
ALYac	Generic.Exploit.Shellcode.2.50EF6B94	Antiy-AVL	Trojan/Win64.Shelma
SecureAge APEX	Malicious	Arcabit	Generic.Exploit.Shellcode.2.50EF6B94
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Crypt.XPACK.Gen7	BitDefender	Generic.Exploit.Shellcode.2.50EF6B94
BitDefenderTheta	Gen:NN.ZexaF.34590.AtW@aOOVjnk	ClamAV	Win.Trojan.PupyRat-5710268-0
Comodo	TrojWare.Win32.Patpoopy.E@8152t0	CrowdStrike Falcon	Win/malicious_confidence_80% (D)
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Python.PuPy.17	eGambit	RAT.Pupy

Abbildung 2.4 VirusTotal der prefetch Datei

Zusätzlich wurde in der *NTUSER.dat* Datei der Key RecentDocs analysiert. Es stellte sich dabei heraus, dass diese Datei zum letzten am am 01.01.1970 um 00:00 Uhr geschrieben wurde. Es ist zu vermuten, dass der Angreifer den Attribut LastWrite auf Beginn der Unixzeit 1. Januar 1970, 00:00 Uhr bewusst gesetzt hat und somit eine Manipulation zur Verschleierung von Spuren hindeuten könnte.

Ein Ausschnitt aus der RecentDocs-Analyse ist in Abbildung ?? zu sehen.

```
LastWrite Time Thu Jan 1 00:00:00 1970 (UTC)
22 = 171110_NorthKorea-DiploimaticUpdate.zip

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.zip
LastWrite Time Thu Jan 1 00:00:00 1970 (UTC)
MRUListEx = 0
0 = 171110_NorthKorea-DiploimaticUpdate.zip
```

Abbildung 2.5 Ausschnitt aus der RecentDocs-Analyse

Die *SECURITY.dat* und *SAM.dat* Dateien enthielten keine aufschlussreichen Einträge.

Um den letzten Login im System festzustellen, wurde die Datei *SOFTWARE.dat* analysiert. Dabei stellte sich ebenfalls raus, dass der Eintrag Winlogon überschrieben wurde. Auch hier ist davon auszugehen, dass der Angreifer diesen Eintrag überschrieben hat, um seine Spuren zu verwischen. Der zuletzt eingeloggte User sowie der Zeitpunkt des Logins konnten somit nicht ermittelt werden. Dies ist in Abbildung 2.6 zu sehen.

```
Microsoft\Windows NT\CurrentVersion\Winlogon
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
```

**Abbildung 2.6** Ein Ausschnitt aus der Software.dat Analyse

Die Ermittlungen ergaben, dass neben den bereits erwähnten Manipulationen, weitere Zugriffszeiten in allen Registry-Einträgen zurückgesetzt wurden.

## 2.5 Wireshark Analyse

Wireshark wurde am 13.11.17 um 16:24 Uhr heruntergeladen und eine Minute vor der eigentlichen Malware um 16:26 Uhr gestartet. Es deutet darauf hin, dass der Mitarbeiter aufgrund eines ersten Verdachts das Sniffing-Tool selbst heruntergeladen hat, um den Netzwerkverkehr von seinem Rechner zu überwachen. Außerdem wurde eine Wireshark-Erweiterung **Solarwinds Response Time Viewer** installiert. Dies ist in Abbildung 2.7 und 2.8 zu sehen. Im Image des Users findet sicher unter `/root/Install` zwei Wireshark Dumps `dump_a.pcapng` und `dump_b.pcapng`. Bei der Analyse der Wireshark Dumps fiel auf, dass die IP Adresse 192.168.8.131, welche zu Router Admin Interfaces gehört, oft aufgerufen wurde und dabei verschiedene Ports ausprobiert wurden. Dies wirkt, als sollte sich Zugang zur Admin-Konsole verschafft werden. Es konnte kein Beweis gefunden werden, dass der Virus den Router kompromittieren konnte, es ist aber trotzdem dringend empfohlen den Router zu untersuchen.

History	<a href="http://tracker.marinnm.com/?cid=26u0u0K06nwid=s...">http://tracker.marinnm.com/?cid=26u0u0K06nwid=s...</a>	2017-11-13 16:24:47 UTC	<a href="http://tracker.marinnm.com/?cid=26u0u0K06nwid=s...">http://tracker.marinnm.com/?cid=26u0u0K06nwid=s...</a>	Chrome	tracker.marinnm.com	client-wat...
History	<a href="http://go.solarwinds.com/free-tools-response-time-viewer...">http://go.solarwinds.com/free-tools-response-time-viewer...</a>	2017-11-13 16:24:47 UTC	<a href="http://go.solarwinds.com/free-tools-response-time-viewer...">http://go.solarwinds.com/free-tools-response-time-viewer...</a>	Chrome	go.solarwinds.com	client-wat...
History	<a href="https://www.google.de/search?source=hp&amp;ie=8BcWnGUL...">https://www.google.de/search?source=hp&amp;ie=8BcWnGUL...</a>	2017-11-13 16:24:47 UTC	<a href="https://www.google.de/search?source=hp&amp;ie=8BcWnGUL...">https://www.google.de/search?source=hp&amp;ie=8BcWnGUL...</a>	Chrome	www.google.de	client-wat...
History	<a href="https://www.wireshark.org/">https://www.wireshark.org/</a>	2017-11-13 16:24:50 UTC	<a href="https://www.wireshark.org/">https://www.wireshark.org/</a>	Chrome	www.wireshark.org	client-wat...
History	<a href="https://www.wireshark.org/#download">https://www.wireshark.org/#download</a>	2017-11-13 16:24:53 UTC	<a href="https://www.wireshark.org/#download">https://www.wireshark.org/#download</a>	Chrome	www.wireshark.org	client-wat...

### Abbildung 2.7 Analyse der aufgerufenen Webseiten

```
Tue Nov 14 12:43:00 2017 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mmc.exe (1)
Mon Nov 13 16:41:23 2017 Z
  Microsoft.Windows.Explorer (26)
Mon Nov 13 16:27:38 2017 Z
  C:\Users\walter\Documents\Work\E-Mails\Attachment-Export\171110_NorthKorea-DiploimaticUpdate.pdf.exe (1)
Mon Nov 13 16:26:33 2017 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Wireshark\Wireshark.exe (1)
Mon Nov 13 16:23:40 2017 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (4)
Mon Nov 13 08:06:04 2017 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\UserAccountControlSettings.exe (2)
Sun Nov 12 19:08:39 2017 Z
  Microsoft.Office.OUTLOOK.EXE.16 (3)
Sun Nov 12 18:55:10 2017 Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (7)
Fri Nov 10 15:37:54 2017 Z
  Chrome (6)
```

**Abbildung 2.8** Dateipfade zu analysierten Dateien

## 2.6 Prozessliste

Mithilfe von Volatility 2.6.1 konnten aus dem Arbeitsspeicher die aktiven und beendeten Prozesse ausgewertet werden. Dabei fiel auf, dass der verdächtige Prozess 171110\_NorthKo um 13.11.17 16:27 Uhr gestartet wurde und bis zur Extraktion bzw. der forensischen Sicherung des Arbeitsspeichers nicht beendet wurde. Dies bestätigt den Security Incident. Die Ausgabe von Volatility pslist ist in Abbildung X zu sehen.

Eine Minute davor um 16:26 Uhr wurde das Netzwerk Sniffing Tool Wireshark gestartet und am nächsten Tag, den 14.11.17 um 16:01 Uhr beendet. Es ist zu vermuten, dass Wireshark vom Nutzer selbst ausgeführt wurde, da es vor dem Virus gestartet wurde. Der User könnte einen verdacht gehabt haben und sicherheitshalber den Netzwerktraffic tracken wollte. Es ist zu empfehlen, den Mitarbeiter Lars Walter dazu zu befragen.

Es wurde in der Prozessanalyse mit Volatility der Prozess 171110\_NorthKo mit der Prozess-ID 6580 gefunden. Wie in Abbildung X zu sehen ist, hat diese Datei die cmd.exe Prozesse gestartet. Diese Prozesse weisen alle die bereits oben erwähnte PID 6580 der Malware als Parent-PID auf. Diese Prozesse sind verdächtig, wobei jedoch die Absicht dahinter nicht eindeutig festgestellt werden kann.

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
18446673171499102000	171110_NorthKo	6580	4012	6	0	1	1	2017-11-13 16:27:38 UTC+0000	
18446673171539012000	cmd.exe	12520	6580	0	-1	1	1	2017-11-14 12:28:58 UTC+0000	2017-11-14 12:31:31 UTC+0000
18446673171517130000	cmd.exe	14860	6580	0	-1	1	1	2017-11-14 12:38:59 UTC+0000	2017-11-14 12:45:43 UTC+0000
18446673171505164000	cmd.exe	14764	6580	0	-1	1	1	2017-11-14 12:48:14 UTC+0000	2017-11-14 12:49:49 UTC+0000
18446673171521907000	cmd.exe	3440	6580	0	-1	1	1	2017-11-14 12:50:57 UTC+0000	2017-11-14 12:52:40 UTC+0000
18446673171541084000	cmd.exe	16508	6580	0	-1	1	1	2017-11-14 12:57:29 UTC+0000	2017-11-14 12:59:01 UTC+0000
18446673171543828000	cmd.exe	1500	6580	0	-1	1	1	2017-11-14 15:37:16 UTC+0000	2017-11-14 15:39:01 UTC+0000
18446673171543005000	cmd.exe	19224	6580	3	0	1	1	2017-11-14 15:47:39 UTC+0000	

Showing 1 to 8 of 8 entries (filtered from 188 total entries)



Previous **1** Next

**Abbildung 2.9** Prozessübersicht aus der Arbeitsspeicheranalyse



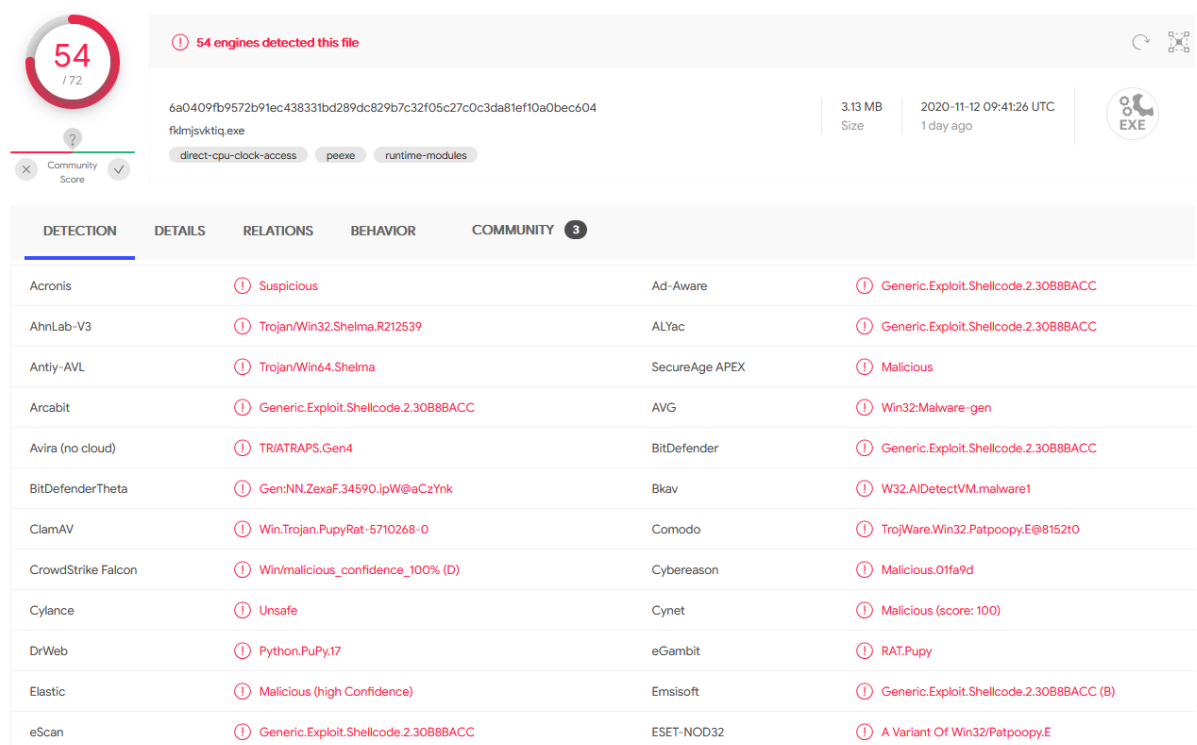
### 3 Weitere Aktivität des Angreifers

Mithilfe der Timeline-Funktionalität des Forensik-Tools Autopsy wurde die verdächtig wirkende Datei fklmjsvktiq.exe wie in Abbildung 3.1 gefunden. Diese Datei wurde am 13.11.17 um 16:53 Uhr im Dateisystem angelegt und ausgeführt.

	2017-11-13 16:53:58	File Accessed	/img_client-walter.e01/ProgramData/fklmjsvktiq.exe	File System	UNKNOWN
	2017-11-13 16:53:58	File Created	/img_client-walter.e01/ProgramData/fklmjsvktiq.exe	File System	UNKNOWN

**Abbildung 3.1** Nachweis der fklmjsvktiq.exe

Zur weiteren Analyse wurde die Datei wie in Abbildung 3.2 auf [www.virustotal.com](http://www.virustotal.com) hochgeladen. Dabei stellte sich heraus, dass die Datei als Schadsoftware eingestuft wird. Anhand VirusTotal konnte außerdem das grobe Verhalten der Schadsoftware abgelesen werden.



DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Acronis		① Suspicious	Ad-Aware	① Generic.Exploit.Shellcode.2.30B8BACC
AhnLab-V3		① Trojan.Win32.Shelma.R212539	ALYac	① Generic.Exploit.Shellcode.2.30B8BACC
Antiy-AVL		① Trojan.Win64.Shelma	SecureAge APEX	① Malicious
Arcabit		① Generic.Exploit.Shellcode.2.30B8BACC	AVG	① Win32:Malware-gen
Avira (no cloud)		① TRI/ATRAP.Gen4	BitDefender	① Generic.Exploit.Shellcode.2.30B8BACC
BitDefenderTheta		① Gen:NN.Zexaf.34590.jpW@aCzYnk	Bkav	① W32.AIDetectVM.malware1
ClamAV		① Win.Trojan.PupyRat-5710268-0	Comodo	① TrojWare.Win32.Patpoopy.E@6152t0
CrowdStrike Falcon		① Win/malicious_confidence_100% (D)	Cybereason	① Malicious.0Tfa9d
Cylance		① Unsafe	Cynet	① Malicious (score: 100)
DrWeb		① Python.PuPy.17	eGambit	① RAT.Pupy
Elastic		① Malicious (high Confidence)	Emsisoft	① Generic.Exploit.Shellcode.2.30B8BACC (B)
eScan		① Generic.Exploit.Shellcode.2.30B8BACC	ESET-NOD32	① A Variant Of Win32/Patpoopy.E

**Abbildung 3.2** VirusTotal Auswertung zu fklmjsvktiq.exe

Es stellte sich dabei heraus, dass die Maleware in der Lage ist, wichtige .dll Libraries wie kernel32.dll (Verwaltung von Speicher und Ein-/Ausgabefunktionen) und

### 3 Weitere Aktivität des Angreifers

user32.dll zu importieren, welche möglicherweise zu weitreichenden Eingriffen ins System genutzt wurden. Des Weiteren werden verschiedene IP-Adressen aufgerufen wie in Abbildung 3.3 zu sehen ist, wobei die Adresse 210.122.17.27 auf einen koreanischen Server verweist und in vorliegenden Kontext daher besonders verdächtig erscheint.

**Contacted IPs** ⓘ

IP	Detections	Autonomous System	Country
210.122.17.27	0 / 76	3786	KR
23.12.145.26	0 / 83	20940	US
23.12.145.33	0 / 83	20940	US
104.111.87.125	0 / 85	35994	US
23.33.181.181	0 / 76	6762	NL
64.4.10.255	0 / 76	8075	US
23.200.147.17	0 / 76	35994	NL
23.200.147.16	0 / 88	35994	NL
40.91.72.206	0 / 84	8075	US

**Abbildung 3.3** VirusTotal Analyse der aufgerufenen IP Adressen der fklmjsvktiq.exe

## 4 Möglicher Datendiebstahl

Die auf VirusTotal aufgeführten IP Adressen des Virus wie in Abbildung 4.1 zu sehen, wurden in den Wireshark Dumps analysiert. Dabei wurde eine der Verbindungen auf die IP Adresse 210.122.17.27:80 gefunden. Es fiel auf, dass sehr viele Calls auf diese IP Adresse durchgeführt wurden. Dabei wurden auch Daten übertragen, da die Calls teilweise eine sehr hohe Größe hatten.

</

Abbildung 4.1 Wireshark Analyse der Calls auf 210.122.17.27:80

In Abbildung 4.1 ist zu sehen, dass es insgesamt über 67000 Pakete mit Ziel oder Absenderadresse dieser IP Adresse hat und dass das größte Paket eine Länge von über 52000 Bytes hat. Dies deutet darauf hin, dass Daten hochgeladen wurden.

Auf *who is* konnte ermittelt werden, dass sie einem asiatischen Provider zuzuordnen ist, allerdings sind durch das hohe Alter, keine genaueren Angaben möglich. Es könnte mittlerweile neu vergeben worden sein oder dieser Server war auch betroffen und wurde nur als Mittelsmann genutzt.

Aufzählung bla bla

1. bla bla

# **Literaturverzeichnis**