Technische Hochschule Rosenheim

Fakultät für Informatik

FWPM Penetrationstests und Forensik

Abschlussbericht Forensik

von

Daniel Böning

Jonathan Hamberger

Osman Güloglu

Karl Herzog

Inhaltsverzeichnis

1 Management Summary **1**

2 Analyse des Systems **2**
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 Arbeitsspeicheranalyse 6

3 Art des Angriffs **8**

4 Weitere Aktivität des Angreifers **10**

5 Möglicher Datendiebstahl **12**

6 Empfohlene nächste Schritte für hVs-Reisen **13**

1 Management Summary

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 Virenscanner 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 E-Mail-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-Datei

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 Prefetch-Datei

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.

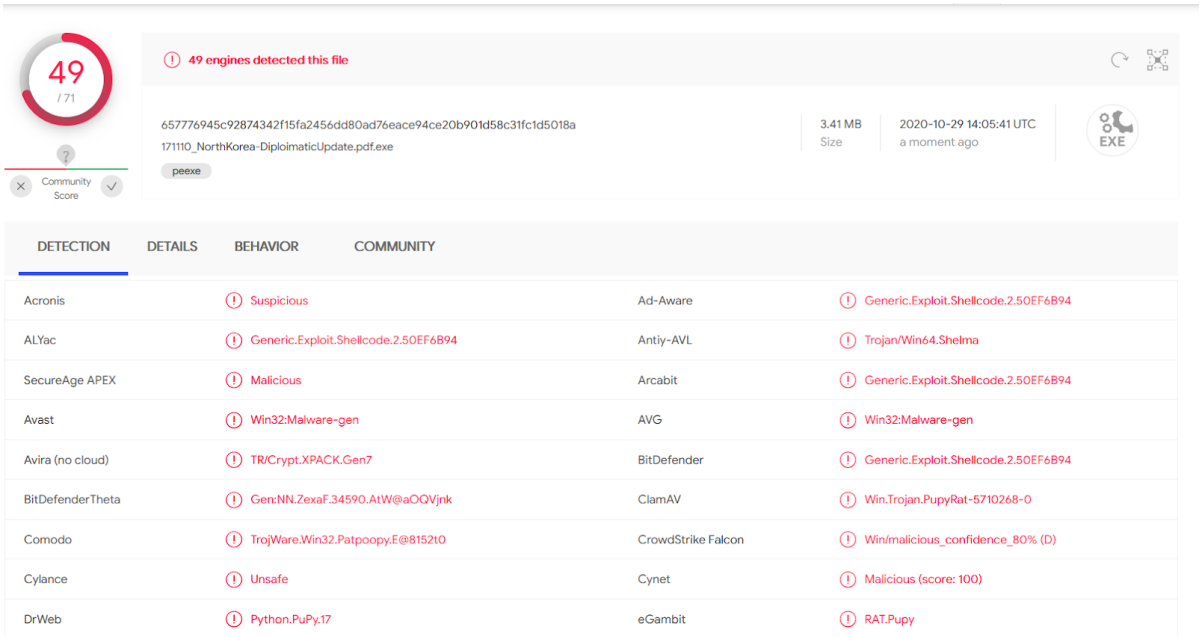

Abbildung 2.4 VirusTotal Scan der Malware 17110_NorthKorea-DiploimaticUpdate.pdf.exe

Zusätzlich wurde in der *NTUSER.dat* Datei der Key *RecentDocs* analysiert. Es stellte sich dabei heraus, dass diese Datei zum letzten Mal am *1. Januar 1970, 00:00 Uhr* geschrieben wurde. Es ist zu vermuten, dass der Angreifer das Attribut *LastWrite* bewusst auf den Beginn der Unixzeit gesetzt hat, was auf eine Manipulation zur Verschleierung von Spuren hindeuten könnte. Ein Ausschnitt aus der RecentDocs-Analyse ist in Abbildung 2.5 zu sehen. Die SECURITY.dat und SAM.dat Dateien enthielten keine aufschlussreichen Einträge.

```
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

Um den letzten Login im System festzustellen, wurde die Registry-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 herunterladen und eine Minute vor der eigentlichen Malware um 16:26 Uhr gestartet. Dies geht aus der Analyse der Registry-Einträge hervor (siehe Abbildung 2.7).

```
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 2.7 Ausschnitt der Registry-Einträge

Es deutet darauf hin, dass der Mitarbeiter aufgrund eines ersten Verdachts das Sniffing-Tool selbst heruntergeladen hat, um den Netzwerkverkehr seines Rechners zu überwachen. Die Browser-History zeigt, dass die Wireshark-Erweiterung *Solarwinds Response Time Viewer* installiert wurde (siehe Abbildung 2.8). 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 eine gängige Adresse für Admin Interfaces ist, häufig aufgerufen wurde und dabei verschiedene Ports angesprochen wurden. Dies deutet darauf hin, dass sich der Angreifer Zugang zur Admin-Konsole des Routers verschaffen wollte. Es konnte kein Beweis gefunden werden, dass der Virus den Router kompromittieren konnte, es ist aber trotzdem dringend empfohlen den Router zu untersuchen.

History			http://tracker.marinsm.com/rd?cid=26xu0nx0k08mkwid=s...	2017-11-13 16:24:47 UTC	http://tracker.marinsm.com/rd?cid=26xu0nx0k08mkwid=s...		Chrome	tracker.marinsm.com	client-walter.(
History			http://go.solarwinds.com/free-tools-response-time-viewer-...	2017-11-13 16:24:47 UTC	http://go.solarwinds.com/free-tools-response-time-viewer-...		Chrome	go.solarwinds.com	client-walter.(
History			https://www.google.de/search?source=hp&ei=R8cJWrG0L...	2017-11-13 16:24:47 UTC	https://www.google.de/search?source=hp&ei=R8cJWrG0L...	wireshark - Google-Suche	Chrome	www.google.de	client-walter.(
History			https://www.wireshark.org/	2017-11-13 16:24:50 UTC	https://www.wireshark.org/	Wireshark · Go Deep.	Chrome	www.wireshark.org	client-walter.(
History			https://www.wireshark.org/#download	2017-11-13 16:24:53 UTC	https://www.wireshark.org/#download		Chrome	www.wireshark.org	client-walter.(

Abbildung 2.8 Ausschnitt der Browser-History mit Autopsy

2.6 Arbeitsspeicheranalyse

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` am 13.11.17 um 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 2.9 zu sehen. Eine Minute davor, um 16:26 Uhr, wurde 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. 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 2.9 zu erkennen ist, hat dieser Prozess weitere Prozesse mit der Bezeichnung *cmd.exe* gestartet. Diese weisen alle die oben erwähnte PID 6580 der Malware als Parent-PID auf. Obwohl diese Prozesse als verdächtig zu betrachten sind, konnte nicht eindeutig festgestellt werden, welche Funktion sie erfüllen.

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

Wie in Abbildung 2.10 ersichtlich, konnte mit dem Plugin *netscan* von Volatility herausgefunden werden, dass die Malware auf die IP-Adresse `210.122.17.27:80` zugreift. Eine Whois-Abfrage der IP Adresse ergab, dass es sich um eine südkoreanische Adresse handelt. Dies wird im Kapitel 5 weiter untersucht.

```
0xbf83ca569cc0    TCPv4    192.168.8.131:54599    210.122.17.27:80    ESTABLISHED    6580    171110_NorthKo
```

Abbildung 2.10 Ausschnitt aus dem Volatility-Plugin netscan

Bei der Analyse mit dem Volatility Plugin *handles* konnte herausgefunden werden, auf welche Registry-Schlüssel der besagte Prozess ein Handle besitzt (siehe Abbildung 2.11). Nach dem Auslesen der jeweiligen Registry-Schlüssel konnten jedoch keine verdächtigen Einträge nachgewiesen werden. Möglicherweise wurden auf diese Weise die Zeitstempel der Registry-Einträge zurückgesetzt.

```
PS C:\Forensics\01_Tools\06_Memory-Analysis\volatility-2.6.1> python .\vol.py -f "C:\Users\forensics\Desktop\ptf2021-evidences\CLIENT-WALTER\client-walter.vmem" --profile=Win10x64_15063 handles -p 6580 --object-type=key
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Pid      Handle     Access Type        Details
---------- -------- ---------- ---------- ---------- -------
0xffff9b877a231540   6580      0xa4   0x20019 Key        MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
0xffff9b877a9f21e0   6580      0xa8       0x1 Key        MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE
0xffff9b877abefd40   6580      0xc4   0x f003f Key        MACHINE
0xffff9b8779e4ad70   6580     0x104       0x9 Key        MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
0xffff9b8776 9f26b0  6580     0x240   0x20019 Key        MACHINE\SYSTEM\CONTROLSET001\CONTROL\NETWORKPROVIDER\HWORDER
0xffff9b8777fa29a0   6580     0x27c       0x9 Key        MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS\DLLNXOPTIONS
0xffff9b877ab15d30   6580     0x298   0xf003f Key        USER\S-1-5-21-75241813-3417798221-1742485458-1004
0xffff9b877af562b0   6580     0x2cc   0xf003f Key        MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9
0xffff9b877886fd50   6580     0x2d4   0xf003f Key        MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5
0xffff9b876fff71b0   6580     0x388       0x1 Key        MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
0xffff9b8776f72d60   6580     0x3a4   0x20019 Key        MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\IDS
0xffff9b8778b9a3f0   6580     0x554       0x8 Key        USER\S-1-5-21-75241813-3417798221-1742485458-1004\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION
0xffff9b877adaf960   6580     0x848   0xf003f Key        MACHINE\SOFTWARE\CLASSES
0xffff9b877b659750   6580     0x880   0xf003f Key        MACHINE\SOFTWARE\CLASSES
```

Abbildung 2.11 Ausschnitt aus dem Volatility-Plugin handles

3 Art des Angriffs

Mithilfe von *Autopsy* wurde der Browserverlauf sowie die E-Mail-Nachrichten des betroffenen Systems auf verdächtige Aktivitäten und Nachrichten analysiert. Im Posteingang (lokale Sicherung von Outlook) konnte dabei die Existenz einer Phishing-Mail nachgewiesen werden, welche am 13.11.17 um 16:19 Uhr empfangen wurde (siehe Abbildungen 3.1 und 3.2).

Abbildung 3.1 Ausschnitt des Posteingangs in Autopsy

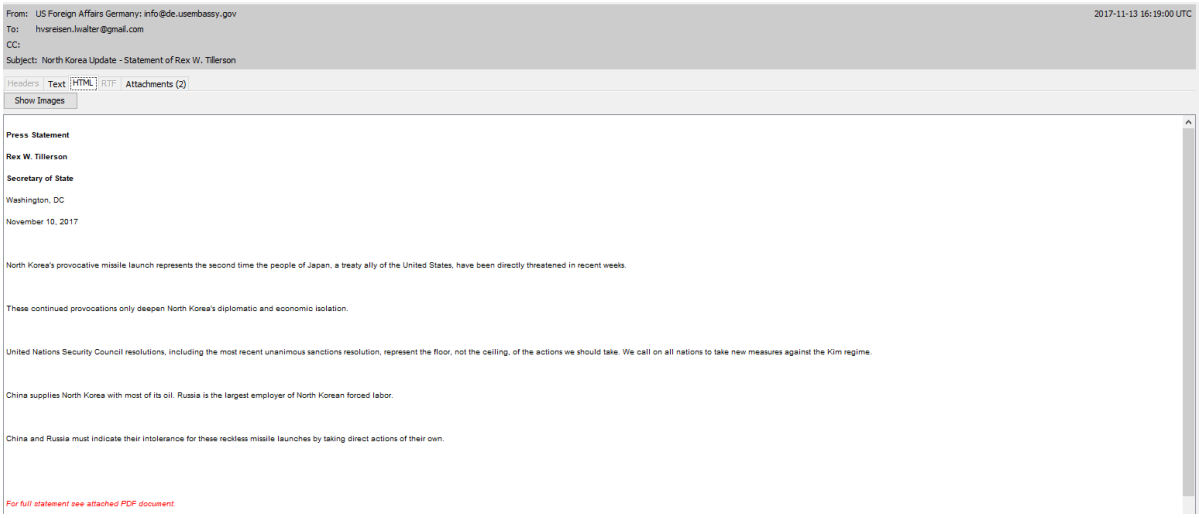

Abbildung 3.2 Ausschnitt der Phishing-Mail

Im Mail-Anhang befand sich eine Zip-Datei, welche die auf dem System nachgewiesene Malware `171110_NorthKorea-DiploimaticUpdate.pdf.exe` enthielt (siehe Abbildung 3.3). Mit großer Wahrscheinlichkeit ist anzunehmen, dass es sich bei der Phishing-Mail um einen gezielten Angriff auf hVs-reisen handelte. Die Nachricht sollte dabei den Eindruck erwecken, sie stamme von einem hochrangigen Beamten des US-Außenministeriums und liefere wichtige Informationen über Änderungen der diplomatischen Beziehungen zu Nordkorea. Vor dem Hintergrund des Geschäftsmodells von hVs-reisen (Reisen nach Nordkorea), ist anzunehmen, dass der betroffene Mitarbeiter sich dazu verleiten ließ, die E-Mail als seriös zu betrachten und den Anhang zu öffnen.

From: US Foreign Affairs Germany: info@de.usembassy.gov 2017-11-13 16:19:00 UTC
To: hvsreisen.lwalter@gmail.com
CC:
Subject: North Korea Update - Statement of Rex W. Tillerson

Headers | Text | HTML | RTF | Attachments (2)

View in New Window

2 Results

Table | Thumbnail

Name	S	C	O	Size	Known	MIME Type
171110_NorthKorea-DiploimaticUpdate.zip				3273776	unknown	application/zip
OutlookConvertMSG2EMLSetup.exe				310800	unknown	application/x-dosexec

Abbildung 3.3 Ausschnitt des Anhangs der Phishing-Mail

Ferner konnte nachgewiesen werden, dass am 12.11.2017 ab 18:55 Uhr mehrfach über den Webbrowser des Mitarbeiters auf dessen E-Mail-Postfach `hvsreisen.lwalter@gmail.com` zugegriffen wurde. Dabei wurde um 19:47 Uhr der Zugriff für weniger sichere Apps auf den Google E-Mail Account des Mitarbeiters aktiviert (siehe Abbildung 3.4). Ob diese Änderung absichtlich erfolgte, kann nur durch weitere Befragung des Mitarbeiters ermittelt werden. Sollte sich dabei herausstellen, dass die Einstellung nicht von ihm selbst durchgeführt wurde, liegt die Vermutung nahe, dass der Angreifer bereits vor der Phishing-Attacke Zugriff auf das E-Mail Konto des Mitarbeiters hatte, was die Bedrohungslage als Ganzes massiv erhöhen würde. Für eine endgültige Bestätigung müsste dieser Annahme in einem separaten Projekt weiter nachgegangen werden.

Unabhängig von der Frage, wer die konkrete Änderung durchführte, wurde dadurch die Sicherheit des Systems gefährdet. Die Einstellung erlaubt nämlich Anwendungen, die nicht dem Sicherheitsstandard von Google entsprechen, den Zugriff auf das Postfach.

History				https://mail.google.com/mail/	2017-11-12 18:56:11 UTC	https://mail.google.com/mail/	Posteingang - hvsreisen.lwalter@gmail.com - Gmail	Chrome	mail.google.com	client-walter.
History				https://mail.google.com/mail/	2017-11-12 18:56:11 UTC	https://mail.google.com/mail/	Posteingang - hvsreisen.lwalter@gmail.com - Gmail	Chrome	mail.google.com	client-walter.
History				https://mail.google.com/mail/	2017-11-12 18:56:11 UTC	https://mail.google.com/mail/	Posteingang - hvsreisen.lwalter@gmail.com - Gmail	Chrome	mail.google.com	client-walter.
History				https://mail.google.com/mail/	2017-11-12 18:56:11 UTC	https://mail.google.com/mail/	Posteingang - hvsreisen.lwalter@gmail.com - Gmail	Chrome	mail.google.com	client-walter.
History				https://mail.google.com/mail/	2017-11-12 18:56:11 UTC	https://mail.google.com/mail/	Posteingang - hvsreisen.lwalter@gmail.com - Gmail	Chrome	mail.google.com	client-walter.
History				https://mail.google.com/mail/	2017-11-12 18:56:11 UTC	https://mail.google.com/mail/	Posteingang - hvsreisen.lwalter@gmail.com - Gmail	Chrome	mail.google.com	client-walter.
History				https://mail.google.com/mail/	2017-11-12 18:56:11 UTC	https://mail.google.com/mail/	Posteingang - hvsreisen.lwalter@gmail.com - Gmail	Chrome	mail.google.com	client-walter.
History				https://mail.google.com/mail/	2017-11-12 18:56:11 UTC	https://mail.google.com/mail/	Posteingang - hvsreisen.lwalter@gmail.com - Gmail	Chrome	mail.google.com	client-walter.
History				https://www.google.com/settings/security/lesssecureapps	2017-11-12 19:08:31 UTC	https://www.google.com/settings/security/lesssecureapps	Weniger sichere Apps	Chrome	www.google.com	client-walter.
History				https://myaccount.google.com/lesssecureapps	2017-11-12 19:46:47 UTC	https://myaccount.google.com/lesssecureapps	Weniger sichere Apps	Chrome	myaccount.google.com	client-walter.
History				https://myaccount.google.com/lesssecureapps	2017-11-12 19:46:47 UTC	https://myaccount.google.com/lesssecureapps	Weniger sichere Apps	Chrome	myaccount.google.com	client-walter.
History				https://myaccount.google.com/lesssecureapps	2017-11-12 19:46:47 UTC	https://myaccount.google.com/lesssecureapps	Weniger sichere Apps	Chrome	myaccount.google.com	client-walter.
History				https://myaccount.google.com/lesssecureapps	2017-11-12 19:46:47 UTC	https://myaccount.google.com/lesssecureapps	Weniger sichere Apps	Chrome	myaccount.google.com	client-walter.
History				https://myaccount.google.com/lesssecureapps	2017-11-12 19:46:47 UTC	https://myaccount.google.com/lesssecureapps	Weniger sichere Apps	Chrome	myaccount.google.com	client-walter.
History				https://myaccount.google.com/lesssecureapps	2017-11-12 19:46:47 UTC	https://myaccount.google.com/lesssecureapps	Weniger sichere Apps	Chrome	myaccount.google.com	client-walter.
History				https://mail.google.com/mail/#inbox/15fb19666219573c	2017-11-12 19:47:36 UTC	https://mail.google.com/mail/#inbox/15fb19666219573c	Zugriff für weniger sichere Apps wurde aktiviert - hvsreise...	Chrome	mail.google.com	client-walter.
History				https://mail.google.com/mail/#inbox/15fb19666219573c	2017-11-12 19:47:36 UTC	https://mail.google.com/mail/#inbox/15fb19666219573c	Zugriff für weniger sichere Apps wurde aktiviert - hvsreise...	Chrome	mail.google.com	client-walter.
History				https://mail.google.com/mail/#inbox/15fb19666219573c	2017-11-12 19:47:36 UTC	https://mail.google.com/mail/#inbox/15fb19666219573c	Zugriff für weniger sichere Apps wurde aktiviert - hvsreise...	Chrome	mail.google.com	client-walter.

Abbildung 3.4 Ausschnitt des Browser-Verlaufs mit Aufruf der Einstellung *less secure apps*

4 Weitere Aktivität des Angreifers

Mithilfe der Timeline-Funktionalität des Forensik-Tools *Autopsy* wurde die verdächtig wirkende Datei *fklmjsvktiq.exe* gefunden (siehe Abbildung 4.1). Diese Datei wurde am 13.11.17 um 16:53 Uhr im Dateisystem angelegt und ausgeführt.

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

Abbildung 4.1 Nachweis der Existenz von fklmjsvktiq.exe

Zur weiteren Analyse wurde die Datei auf `www.virustotal.com` hochgeladen. Das Ergebnis des Scans ist in Abbildung 4.2 zu sehen. Dabei stellte sich heraus, dass die Datei als Schadsoftware eingestuft wird. Anhand VirusTotal konnte außerdem das grobe Verhalten der Schadsoftware abgelesen werden.

54 / 72

Community Score

54 engines detected this file

6a0409fb9572b91ec438331bd289dc829b7c32f05c27c0c3da81ef10a0bec604

fklmjsvktiq.exe

direct-cpu-clock-access | peexe | runtime-modules

3.13 MB Size | 2020-11-12 09:41:26 UTC 1 day ago | EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 3

Acronis	Suspicious	Ad-Aware	Generic.Exploit.Shellcode.2.30B8BACC
AhnLab-V3	Trojan/Win32.Shelma.R212539	ALYac	Generic.Exploit.Shellcode.2.30B8BACC
Antiy-AVL	Trojan/Win64.Shelma	SecureAge APEX	Malicious
Arcabit	Generic.Exploit.Shellcode.2.30B8BACC	AVG	Win32:Malware-gen
Avira (no cloud)	TR/ATRAPS.Gen4	BitDefender	Generic.Exploit.Shellcode.2.30B8BACC
BitDefenderTheta	Gen:NN.ZexaF.34590.jpW@aCzYnk	Bkav	W32.AIDetectVM.malware1
ClamAV	Win.Trojan.PupyRat-5710268-0	Comodo	TrojWare.Win32.Patpoopy.E@8152t0
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.01fa9d
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Python.PuPy.17	eGambit	RAT.Pupy
Elastic	Malicious (high Confidence)	Emsisoft	Generic.Exploit.Shellcode.2.30B8BACC (B)
eScan	Generic.Exploit.Shellcode.2.30B8BACC	ESET-NOD32	A Variant Of Win32/Patpoopy.E

Abbildung 4.2 VirusTotal Auswertung zu fklmjsvktiq.exe

Es stellte sich dabei heraus, dass die Malware in der Lage ist, wichtige .dll Libraries wie kernel32.dll (Verwaltung von Speicher und Ein-/Ausgabefunktionen) und user32.dll zu importieren, welche möglicherweise zu weitreichenden Eingriffen ins System genutzt wurden. Des Weiteren werden verschiedene IP-Adressen aufgerufen wie in Abbildung 4.3 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 4.3 VirusTotal Analyse der aufgerufenen IP Adressen der fklmjsvktiq.exe

Laut VirusTotal ist die Schadsoftware außerdem in der Lage, eine ausführbare Datei mit dem Namen oewjeya.exe zu erstellen (siehe Abbildung 4.4). Diese konnte allerdings nicht im System des Mitarbeiters nachgewiesen werden.

Files Written

C:\Users\<USER>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\oewjeya.exe

Abbildung 4.4 Ausschnitt aus VirusTotal für fklmjsvktiq.exe

5 Möglicher Datendiebstahl

Die auf VirusTotal aufgeführten IP Adressen des Viruses wie in Abbildung 5.1 zu sehen, wurden in den Wireshark Dumps analysiert. Dabei wurde eine der Verbindungen auf die IP Addresse 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.

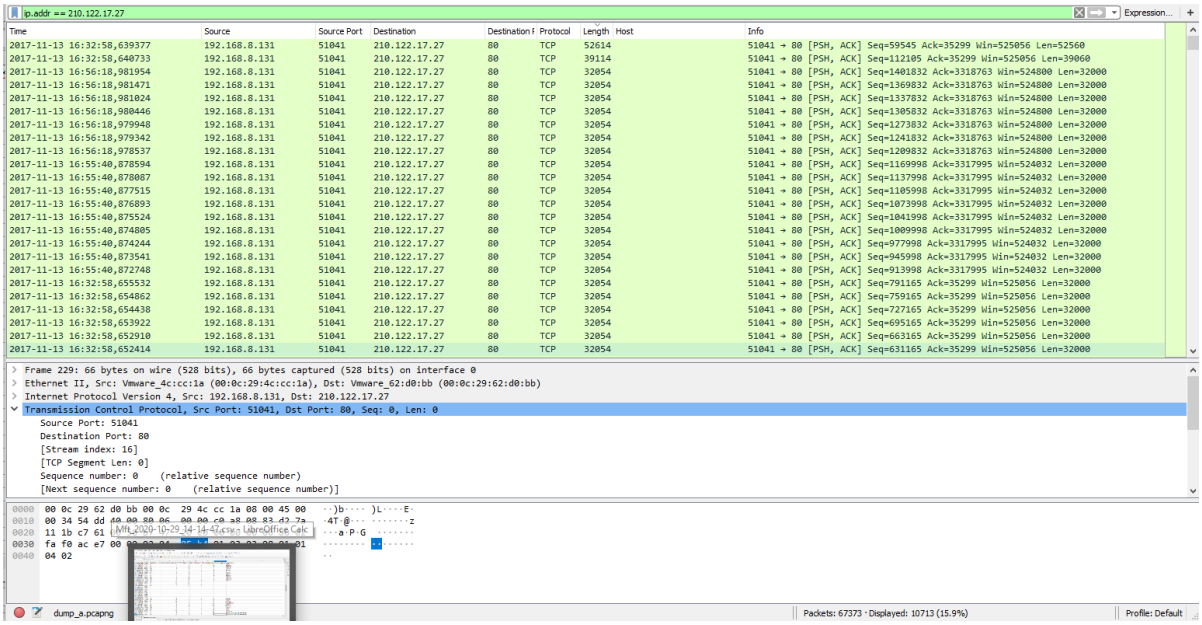

Abbildung 5.1 Wireshark Analyse der Calls auf 210.122.17.27:80

In Abbildung 5.1 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.

Per *whois*-Abfrage 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.

6 Empfohlene nächste Schritte für hVs-Reisen

Dem betroffenen Mitarbeiter Lars Walter wird empfohlen, die Passwörter für sämtliche Accounts und Dienste zu ändern, bei denen er sich seit der Ausführung der Malware am 13.11.17 um 16:27 Uhr vom betroffenen Rechner aus eingeloggt hat. Dringend geändert werden sollte das Passwort für den Google E-Mail Account, da nachgewiesen werden konnte, dass sich der Mitarbeiter nach dem Malware-Befall noch mehrfach bei diesem Dienst angemeldet hatte (siehe Abbildungen 6.1 und 6.2)

2017-11-13 16:28:00 to 2017-11-13 16:29:00

Table | Thumbnail

Icon	Date/Time	Sub Type	Description	Base Type	Known
	2017-11-13 16:28:58	Web History	google.com : https://mail.google.com/mail/#inbox/15fb195...	Web Activity	UNKNOWN
	2017-11-13 16:28:58	Web History	google.com : https://mail.google.com/mail/#inbox/15fb195...	Web Activity	UNKNOWN

Abbildung 6.1 Browserhistory des Nutzers

2017-11-14 10:00:00 to 2017-11-14 11:00:00

Table | Thumbnail

Icon	Date/Time	Sub Type	Description	Base Type	Known
	2017-11-14 10:52:32	Web History	google.com : https://mail.google.com/mail/#inbox/15fa61b49ef...	Web Activity	UNKNOWN
	2017-11-14 10:52:32	Web History	google.com : https://mail.google.com/mail/#inbox/15fa61b49ef...	Web Activity	UNKNOWN
	2017-11-14 10:52:32	Web History	google.com : https://mail.google.com/mail/#inbox/15fa61b49ef...	Web Activity	UNKNOWN
	2017-11-14 10:52:32	Web History	google.com : https://mail.google.com/mail/#inbox/15fa61b49ef...	Web Activity	UNKNOWN

Abbildung 6.2 Browserhistory des Nutzers

Der kompromittierte Rechner sollte vollständig neu aufgesetzt werden, da nicht auszuschließen ist, dass neben der gefundenen Malware noch weitere Schadsoftware installiert wurde. Weiterhin sollte auch der Netzwerk-Router untersucht werden, um festzustellen, ob es dem Angreifer gelang, auf diesen Zugriff zu erlangen. Auch das Passwort des Netzwerk-Routers sollte von der IT-Administration geändert werden. Es empfiehlt sich, alle Passwörter der Mitarbeiter von hVs-Reisen zu ändern, da wir einen Zugriff auf weitere Accounts derzeit nicht ausschließen können. Zudem sollten alle E-Mail Accounts der Mitarbeiter auf Aktivierung der *Less secure apps* untersucht werden.

Zuletzt sollten alle Mitarbeiter für die IT-Sicherheit sensibilisiert werden, damit ein solcher Angriff auf hVs-Reisen in Zukunft vermieden werden kann. Es sollte

vor allem darauf hingewiesen werden, dass nicht direkt auf die Links der erhalten E-Mails geklickt wird. Die Mitarbeiter sollen sich erst vergewissern, dass die E-Mail vertraulich ist.