Zentrale Ansprechstelle Cybercrime für die nds. Wirtschaft (ZAC)
Landeskriminalamt Niedersachsen
0511 / 262 62 - 3804
zac@lka.polizei.niedersachsen.de

Entschlüsselungstool für Petya-Ransomware veröffentlicht

Die Entwickler der Ransomware-Varianten „GoldenEye“, „Mischa“ und „Petya“ haben via Twitter den Master-Schlüssel veröffentlicht. Mit diesem Schlüssel ist es möglich, befallene Systeme wieder zu entschlüsseln. Die Schadsoftware „NotPetya“ ist hiervon nicht betroffen. Sicherheitsforscher von Malwarebytes haben ein Entschlüsselungstool herausgebracht, das Daten wiederherstellen kann. Betroffene Unternehmen sowie Privatpersonen, die jene Festplatten aufgehoben haben, sollten nun gute Chancen haben, wieder Zugriff auf ihre verschlüsselten Daten zu erlangen.

Anleitung zur Entschlüsselung

Diese Anleitung basiert auf die Anleitung der Firma ***Malwarebytes*** [1]. Die originale Anleitung wurde hier ergänzt und in die deutsche Sprache übersetzt.

ACHTUNG: Die Benutzung des Entschlüsselungstools erfolgt auf eigene Gefahr! Es wird ausdrücklich empfohlen, bevor Beginn ein Backup der verschlüsselten Festplatte bzw. Dateien zu erzeugen.

Anwendungsmöglichkeit

Das veröffentlichte Werkzeug von Malwarebytes zur Entschlüsselung von Rechnern, die mit Petya oder Goldeneye verschlüsselt worden, eignet sich laut den Autoren nur für folgende Versionen der Malware:

- Red Petya (roter Schrift bzw. Hintergrund)
- Green Petya + Mischa (grüner Schrift)
- Goldeneye (goldener Schrift bzw. Hintergrund)

Das Entschlüsselungstool funktioniert *NICHT* mit NotPetya.

Vorbereitung

1) Erstellen Sie ein Backup der zu entschlüsselnden Festplatte (für den Fall, dass die Entschlüsselung scheitert) bzw. der zu entschlüsselnden Dateien.

2) Besuchen Sie die Webseite von Malwarebytes und laden Sie die beiden Tools herunter:

- Live-CD:
  https://github.com/hasherezade/petya_key/releases/download/0.2/antipetya_ultimate.iso
- Windows Executable:
  https://github.com/hasherezade/petya_key/releases/download/0.2/petya_key_v0.2_win32.zip

Zentrale Ansprechstelle Cybercrime für die nds. Wirtschaft (ZAC)
Landeskriminalamt Niedersachsen
0511 / 262 62 - 3804
zac@lka.polizei.niedersachsen.de

Einordnung der Version

Verschiedene Versionen von Petya existieren. Diese können anhand deren Schriftfarbe unterschieden werden [3]:

- **Rot:** Die rote Version verschlüsselt nur die Master File Table [2] der Festplatte und nicht die Dateien. Für diese Version ist nur Schritt 3 auszuführen.
- **Grün:** Green Petya verschlüsselt entweder die MFT *oder* Dateien [1]. Ob nur Schritt 4 oder beide Schritte (3 und 4) auszuführen sind, kann man sofort erkennen: startet der Rechner nicht mehr normal (Text mit Aufforderung zur Zahlung), sind beide Schritte auszuführen. Sind lediglich Dateien verschlüsselt und der Rechner an sich startet normal, ist nur Schritt 4 nötig.
- **Goldeneye:** Da Goldeneye sowohl die MFT als auch Dateien verschlüsselt, sind beide Schritt 3 und Schritt 4 auszuführen.

Entschlüsselung der MFT

3) Zur Entschlüsselung der MFT muss die Live-CD benutzt werden (wie man eine boot-fähige CD oder USB-Disk von einer .iso Image macht, findet man über Google). Wenn von der Live-CD gebootet wird, kommt in englischer Sprache eine Reihe von Anweisungen. Bei der Eingabe ist zu beachten, dass das Programm die Eingabe von einer US-Tastatur erwartet (Bilder einer US Tastatur und die zu der deutschen Tastatur unterschiedliche Tasten findet man ebenfalls über Google).

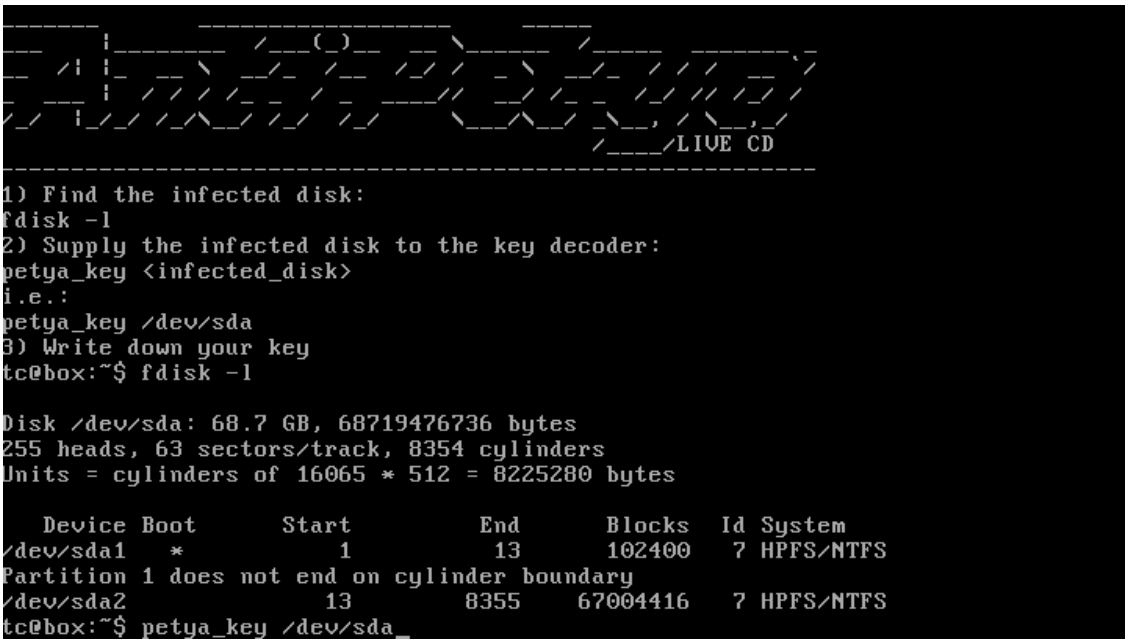

Abbildung 1: Live-CD

a) Mit dem Befehl „fdisk -l“ listet man alle Festplatten bzw. Partitionen auf. Die Bezeichnung der Partition ist zu notieren (z.B. „/dev/sda“).
b) Bei Eingabe „petya_key <disk>“ prüft das Programm, ob die angegebene Festplatte von Peyta infiziert ist. Ist das der Fall, wird gefragt, welche Version (anhand der Farbe) vorhanden ist. Drückt man die entsprechende Taste, bekommt man die Victim ID und der Schlüssel ausgegeben („Your key:“). Der Schlüssel sollte notiert werden.

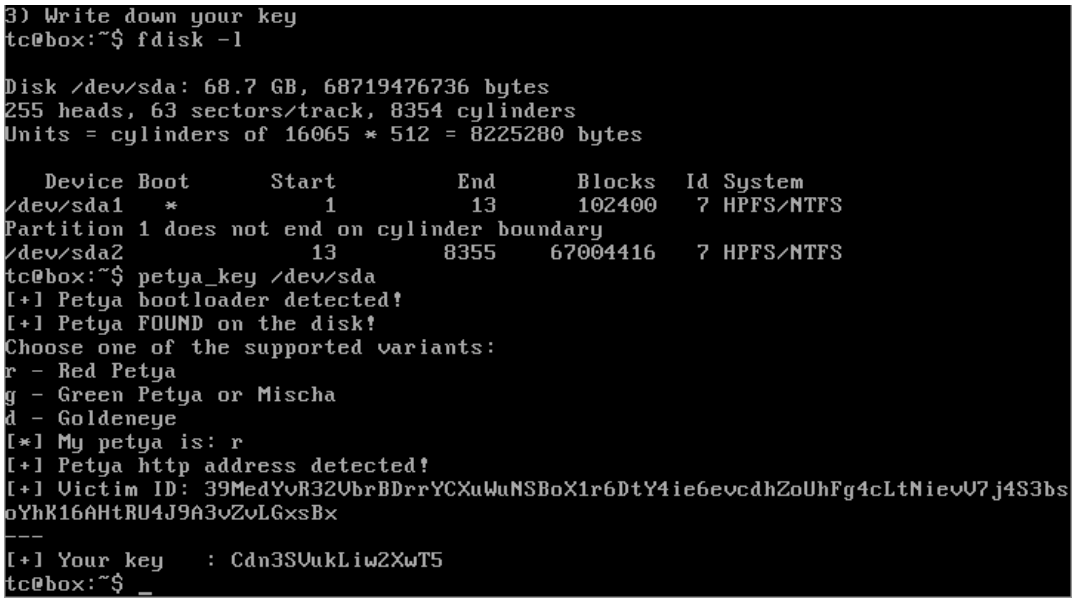

Abbildung 2: Erfolgreiche Ausgabe des Schlüssels zur MFT Entschlüsselung

c) Nach einem Neustart des Rechners (ohne Live-CD) wird man mit der üblichen Zahlungsaufforderung konfrontiert. Unten kann der Schlüssel jetzt eingegeben werden.
d) Nach Eingabe des Schlüssels wird die Entschlüsselung der MFT durchgeführt. Ist diese erfolgreich, kann man den Rechner danach normal neustarten. Je nach Version sind Dateien möglicherweise noch verschlüsselt.

Abbildung 3: Eingabe des Schlüssels bei Petya

Entschlüsselung der Dateien

4) Sind Dateien verschlüsselt, kann das Windows Tool benutzt werden, um den entsprechenden Schlüssel für die verschlüsselten Dateien zu finden.

a) Das Tool braucht die Victim ID, die sich unter anderem in der Datei „YOUR_FILES_ARE_ENCRYPTED“ o.ä. zu finden ist. Kopiert man diese ID in eine neue Text-Datei (z.B. mit dem Namen „id.txt“) und speichert man diese in dem selben Verzeichnis wie das Tool, kann man jetzt über die Kommandozeile das Tool (mit zusätzlicher Angabe des ID-Dateinames) ausführen:

$ petya_key.exe id.txt

Abbildung 4: Gewinnung des Schlüssels mit dem Windows-Tool „petya_key.exe“

b) Ist der vorherige Schritt erfolgreich gewesen, wird der Schlüssel zur Entschlüsselung unter „Your key:“ ausgegeben. Mit diesem Schlüssel kann man nun unter Benutzung des originalen Entschlüsselungstool der jeweiligen Petya Version die verschlüsselten Dateien mit hoher Wahrscheinlichkeit erfolgreich entschlüsseln.

- Mischa: https://drive.google.com/open?id=0Bzb5kQFOXkiSWUZ6dndxZkN1YlE
- Goldeneye: https://drive.google.com/open?id=0Bzb5kQFOXkiSdTZkUUYxZ0xEeDg

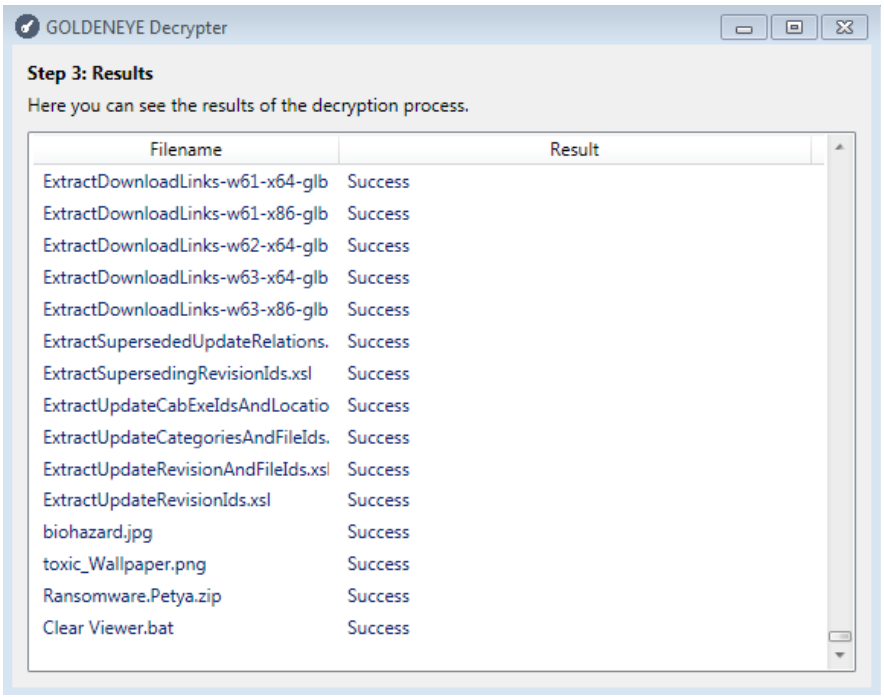

Abbildung 5: Erfolgreiche Ausführung des Goldeneye Entschlüsselungstool

[1] https://blog.malwarebytes.com/malwarebytes-news/2017/07/bye-bye-petya-decryptor-old versions-released/

[2] https://de.wikipedia.org/wiki/NTFS#Aufbau_.E2.80.93_MFT

[3] https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/