Forensischer Untersuchungbericht

Tobias Krieg va08kyqy

4. Juni 2021

Inhaltsverzeichnis

Teil I

Untersuchungsbericht

Kapitel 1

Prolog

1.1 Beweismittel

1.1.1 Identifikation

TODO access LOg Konfigurationsdatei Die Beweismittel zwei Datenträger mit den Namen und SHA256-Summen
ex A.dd a01b1963c1c6b1636242b72ab3423e310186d554c079e288abd3ea5a9f22b55f (Asservat A) und ex B.dd ea2fb3488e11f6426a27bcee054c2629c55334f565d0ed1a2346c0d32f2c3d80 (Asservat B) wurden persönlich bei der Staatsanwaltschaft abgeholt mit Identitätskontrolle der anwesenden Personen. Ebenfalls abgeholt wurden die von der Spurensicherung erstellten Hash-Summen zur Überprüfung der Echtheit der Datenträger. Die Echtheit der Datenträger konnte somit erfolgreich verifiziert werden. Daraufhin wurde eine 1 zu 1 Kopie der Datenträger angefertigt, welche für die folgende Analyse verwendet wurden. Die orginalen Datenträger wurden bis auf die Kopie für nichts anderes benutzt. Ebenfalls wurde nur auf einem Passwort gesicherten Computer ohne Internet Anschluss in einem Raum gearbeitet, welcher nach Verwendung abgesperrt wurde. Manipulation der Beweise durch dritte ist somit ausschließbar.

1.1.2 Verlauf

Der Ermittlungsverlauf des Falles sah wie folgt aus:
Festplatte 1:

- Nachweis der Integrität des Asservats
- Anfertigung einer Kopie
- Analyse des Datenträgers und Suche nach möglichen Beweisen

Festplatte 2:

- Nachweis der Integrität des Asservats
- Anfertigung einer Kopie
- Analyse des Datenträgers und Suche nach möglichen Beweisen

1.2 Auftrag

Die Staatsanwaltschaft ermittelt zur Zeit gegen die zwei Brüder John und Frank Doe aus Erlangen. Sie stehen im Verdacht, am 8.10.2015 zwischen 23 und 24 Uhr einen Webserver an der Universität Erlangen angegriffen, kompromittiert und in der Folge Daten aus gespäht zu haben. Neben §202a StGB sieht die Staatsanwaltschaft den Tatbestand der Datenveränderung gemäß §303a StGB als erfüllt an.Beider Analyse des Webservers wurde die IP-Adresse 131.188.31.68 ermittelt. Es ist davon auszugehen, dass die Angriffe auf den Webserver von dieser IP-Adresse aus erfolgten. Übereine Abfragegemäß §100j Abs.2 StPO wurde Frank Doe als Anschlussinhaber dieser IP-Adresse zum oben genannten Zeitpunkt ermittelt. Im Rahmen einer Hausdurchsuchung wurden zwei Computersysteme vorgefunden und beschlagnahmt. Es wurde festgestellt, dass sowohl John als auch Frank Doe aber keine weiteren Personen die Wohnung bewohnen. Eine Zuordnung der beiden Rechner zu

den beiden Personen war im Rahmen der Beschlagnahme nicht möglich. Beide Brüder haben ausgesagt, im fraglichen Zeitraum auf die Webseite zugegriffen zu haben. Weitere Angaben zur Sache haben sie allerdings gemäß §55 StPO nicht gemacht. Die Kriminalinspektion 5(Cybercrime und digitale Spuren) hat im Zuge der Ermittlungen bereits eine Analyse des Webservers durchgeführt. Die vorläufigen Untersuchungsergebnisse sind unten beigefügt. Die Staatsanwaltschaft erbittet Antworten auf folgende Fragen:
1. Können Sie die beiden Rechner den beiden Brüdern persönlich zuordnen?
2. Wurde von einem der beiden Rechner der Angriff durchgeführt? Fallsja, von welchem Rechner?

1.3 Arbeitsumgebung

Die komplette Untersuchung wurde ausschließlich unter folgenden Arbeitsbedingungen ausgeführt, wobei eine virtuelle Maschine benutzt wurde um externe Einflüsse zu minimieren:

- Oracle VM-Virtualbox 6.0.24 mit Standardeinstellungen
- Kali-Linux-2021.1-vbox-amd64
- Host OS Windows 10 Pro Intel Core i5-4670K CPU@ 3.40GHz, x64-Bit-Betriebssystem, 8 GB RAM
- The Sleuth Kit ver 4.10.1
- TestDisk 7.1, Data Recovery Utility, July 2019
- PhotoRec 7.1, Data Recovery Utility, July 2019

Kapitel 2

Ergebniszusammenfassung

Kapitel 3

Analyse des Datenträgers

3.1 Sleuthkit

3.2 Photorec

3.3 Testdisk

3.3.1 Untersuchung der ersten Partition

3.3.2 Untersuchung der zweiten Partition

3.3.3 Untersuchung der dritten Partition

Teil II

Anhang

Kapitel 4

Beweismittel

4.1 Bild des Beweismittels

Kapitel 5

Konsolenausgaben

5.1 Sleuhtkit

5.2 Testdisk

5.3 File Carving