Ausführende:
Jill Kleiber
Benedikt Völker
Alexander Reuter
Simon Bergedieck

Forensischer Bericht der M57.biz-Untersuchungen

Aktenzeichen 2
Version 1.0

Aachen, 27. Juni 2017

Inhaltsverzeichnis

1 Prolog

1.1 Auftrag

Nachdem auf einer kürzlich verkauften Workstation, die ehemals im Besitz der Firma M57.biz war, illegale Daten gefunden wurden, soll der Besitzer der Daten ermittelt werden. Ebenfalls ist herauszufinden, wie es zum Verkauf des Geräts kam, ob es sich dabei um Diebstahl handelt und wer daran beteiligt war. Da das Gerät ursprünglich die Workstation des Mitarbeiters Jo Smith war, wird die Hypothese aufgestellt, dass dieser der Verantwortliche im oben beschriebenen Sachverhalt ist.

Bei den Untersuchungen fielen weitere Sachverhalte auf, die darüber hinaus untersucht werden sollten. Zum einen war dies, dass Firmengeheimnisse veruntreut wurden, zum anderen, dass der CEO Pat MacGoo von einem der Mitarbeitern ausspioniert wurde.

In Bezug auf die Veruntreuung sollte der Verantwortliche gefunden werden, welche Daten weitergegeben wurden und wer die Daten erhalten hat.

Bei der Spionage soll ermittelt werden von wem und aus welchem Grund sie durchgeführt wird sowie welche Methoden angewandt wurden.

1.2 Beweismittel

Als Beweismittel wurden jeweils vier Festplattenimages, USB-Stick-Images und RAM-Images erhalten.

Tabelle 1.1: Images

Nr.	Image	Größe in GB	MD5-Hash
1	charlie_harddrive	10,2	3017c4188553d7423cd6646a7ff1c1a9
2	jo_harddrive	15,4	872e38f83628f2c3a203457c90e57fdb
3	pat_harddrive	13,0	8f39599fc63bdda285158ea20ee3d567
4	terry_harddrive	41,1	f945f4e23fe82868547cada9868c48c0
5	charlie-2009-12-11	2,1	38067CC457546B3156975D9A52D4229F
6	jo-2009-12-11	1,1	E929219719211F51267C5DFB5406A5AB
7	pat-2009-12-11	0,5348	CE9D8A9979F2BADE5228393B8AC1E3FD
8	terry-2009-12-11	2,1	6B43EB293D85BDD6AD5EF2B2F84F8584
9	charlie_work_usbdrive	1,1	f7f625f56b0337d4d23e423f2ead119e
10	jo_private_usbdrive	1,0	b1ea0a9edae0b3558bb43566ef20e90d
11	jo_work_usbdrive	0,131	59a3620fdd4210b6e909ada29a340877
12	terry_work_usbrive	2,1	9d84f913f3d056e45bd82ed78aa9ba6f

1.3 Beweismittelkette

Die Beweismittel wurden am 20. Juni 2017 um 12:26 im Raum E124 der FH Aachen Eupenerstraße von Chief Inspektor Benedikt Paffen an Ermittler Benedikt Völker ausgehändigt. Bezeugt wurde diese Übergabe von Jill Kleiber.

Im Anschluss wurden die Beweismittel vervielfältigt und zur Unterstützung bei den Untersuchungen an die weiteren Teammitglieder übergeben. Eine Vervielfältigung aller Beweismittel erhielt Alexander Reuter am 20. Juni 2017. Ebenfalls an diesem Tag wurden Simon Bergedieck eine Kopie der Beweismittel 1,5 und 9 übergeben. Jill Kleiber erhielt ein Duplikat aller Beweismittel am 23. Juni 2016. Die Orginalbeweise verblieben bei Benedikt Völker, der sie so verwahrte, dass eine Manipulation der Daten ausgeschlossen ist. Die Integrität der Beweismittel wird durch die Bereitstellung und regelmäßige Überprüfung der Hash-Werte gewährleistet.

1.4 Arbeitsumbgebung

Alle Ermittler nutzten eine Windows 10 64 Bit Version. Als Analyseprogramme wurden Autopsy Version 4.4.0 mit Sleuth Kit Version 4.4.1 und Volatility Version 2.6 verwendet.

Die Untersuchungen fanden im Zeitraum zwischen dem 20. Juni 2017 und dem 27. Juni 2017 in dafür geeigneten Räumlichkeiten des forensischen Trakts der FH Aachen Eupenerstraße (Besucherraum der Mensa) statt.

2 Zusammenfassung für Nicht-Techniker

2.1 Illegale Daten

- einschlägige Daten auf Jos privatem USB-Stick
- identische Daten auf Jos Festplatte (als gelöschte Daten)
- Jos Computer musste ausgetauscht werden
- Terry hat Kontaktdaten von Aaron Green (Käuferin der Workstation) im Handy

2.2 Datenveruntreuung

- Charlie hat Daten in Steganographie-Bildern als E-Mail verschickt
- Daten über Patentforschung von Immortality und Nitroba
- zum Auslesen wird Steganographieprogramm Invisible Secrets gebraucht (Passwort: nitro)
- Zieladressen waren andy@swaxpat.com und jamie@project2400.com (Project 2400 größter Konkurrent von M57.biz)
- mögliche Anklagepunkte Diebstahl und Wirtschaftsspionage

2.3 Wirtschaftsspionage

- Programm winvnc4 dient zum abhören
- Terry verfügt über Programm (auf USB-Stick)
- Programm wurde auf Pats Computer ausgeführt (Beweis im RAM)
- Terry hat Benutzerprofil auf Pats Computer
-

• Why is the employee spying on Pat? • Is anyone else involved? Would you characterize them as accomplices?

3 Zusammenfassung für Techniker

4. Zusammenfassung für Techniker Maximal 10 Seiten, übersichtlich gegliedert nach Schritten in der Ermittlung Technikersprache, wesentliche Spuren und Fundorte dokumentieren Bei Details auf Anhang verweisen

3.1 Alex

Jos-Katzenfetisch: Katzenbilder und Videos wurden auf dem Privaten USB-Stick gefunden. -> Existierten aber auch auf der HDD, wurden dort aber gelöscht. Auf den USB-Stick wurden die Dateien kopiert (vermutlich vom PC).

Pat Rechner: Prozess 756 Winvnc4.exe lief auf dem Rechner (Aus dem Ramimage herausgefunden). auf Patd HDD -> terry besitzt dort ein Benutzerprofil -> terry hat sich auf jeden Fall schon an dem Rechner angemeldet! vnc-4_1_3-x86_win32.exe auf dem USB-Stick gefunden.

terry hat ein Gerichtsbeschluss bzgl. eines Vorfalls der darauf schließen lässt, das er auch hier in diesem Fall involviert ist. (er will sich möglicherweise Informieren was passieren kann wenn er erwicht wird.) Der gerichtsbeschluss liegt auf der Festplatte von terry: /Users/terry/Documents/Downloads/comcast_indictment.pdf

3.2 Ben

A Details für Techniker

5. Details für Techniker (meist als Anhang) Logdateien, Bildschirmfotos, Listings, Terminalsessions, ... Jeweils durchnummeriert, damit man darauf Bezug nehmen kann in vorherigen Teilen des Berichts Beliebig lang

Abbildungsverzeichnis

Tabellenverzeichnis