

Anti-Forensik

Martin Morgenstern

12.05.2023

Gliederung

- **Grundlagen und Ziele AF**
- **Vorbereitende AF-Maßnahmen**
- **AF-Maßnahmen während der Tat**
- **Nachbereitende AF-Maßnahmen**
- **Juristische AF-Maßnahmen**
- **Self Anti-Forensik**

Ziele

- **Sie sollen gängigen Anti-Forensik-Maßnahmen kennen.**
- **Sie sollen Maßnahmen Erkennung und Verhinderung von Anti-Forensik-Maßnahmen kennen.**

Definition AF

In der Praxis mehrere ähnliche Definitionen. Hier wird die Definition von Wundram und Siegel von 2014 verwendet.

Jeder Versuch, die Verfügbarkeit oder Brauchbarkeit von Beweisen für die IT-forensische Untersuchung zu beeinträchtigen.

Durchführung von AF

- **AF kann als Angriffsversuch gewertet werden**
- **Vergleichbar mit klassischen IT-Angriffen**
 - 1. Informationsgewinnung**
 - 2. Finden von Schwachstellen**
 - 3. Ausnutzen der Schwachstellen**

Offene und versteckte AF

**AF kann in 2 Arten unterschieden werden,
offene und versteckte AF**

**Offen: der Analyst sieht sofort das AF-
Maßnahmen durchgeführt werden**

**Versteckt: AF-Maßnahmen sollen nicht oder
nur schwer identifizierbar sein.**

Kombination möglich

Vorbereitende AF

- **Eigene Überlegung welche Ziele erreicht werden sollen**
- **Offene, versteckte oder kombinierte AF**
- **Sammeln möglichst vieler Informationen über den „Gegner“**

Vorbereitende AF

- **Ziele sind meistens:**
 - **Möglichst wenig Rückschlüsse auf Tat**
 - **Vermeidung auffälliger Spuren → offene AF kann dem entgegen stehen!**
 - **Ermittlungsansätze im Keim ersticken**

Vorbereitende AF

Mögliche vorbereitende Maßnahmen:

- Tat nicht zuhause ausführen
- Vermeidung auffälliger Spuren → offene AF kann dem entgegen stehen!
- Ermittlungsansätze im Keim ersticken
- Logging deaktivieren

Vorbereitende AF

Mögliche vorbereitende Informationen:

- **Wie funktioniert Forensik-Software, was wird ausgewertet?**
- **Was sind technische / juristische Anforderungen an einen Beweis?**

AF-Maßnahmen während der Tat

- **VPN, Proxy, Tor...**
- **Falsche Spuren (auch hinterher möglich)**
- **Manipulation von Log-Daten**
- **Nutzung falscher Identitäten**
- **...**

„Härten“ des Systems gegen Auswertungen

- **Klassisch: „Datenträger- bzw. Dateiverschlüsselung“**
- **„Fallen“ für Live-Analysten**
- **Erschweren einer Datenträger-Analyse**

Nutzung von virtuellen Maschinen

- **Nutzung von VMs um keine Spuren im Host-System zu hinterlassen**
 - **Kann eingestellt werden, dass durch Snap-Shots bzw. sonstigen zurücksetzen keine Spuren hinterlassen werden sollen**
- Könnten Sie darauf Hinweise finden?**

Nutzung von Live-Systemen

- **Nutzung von Live-Systemen um keine Spuren im Host-System zu hinterlassen**
 - **In der Praxis bisher zum Glück eher selten**
- Könnten Sie darauf Hinweise finden?**

Falsche Spuren

- Bei Malware und ähnlichem: falsche Hinweise auf Programmierer z.B. durch:

- Variablennamen in bestimmter Sprache
- Kopieren eines Programmierstils
- Identifizierungsmerkmale von Compiler
- ...

Fake-Identitäten nutzen

- **Alternative zur Nutzung von Pseudonymen (z.B. in sozialen Netzwerken)**
- **Ziel entweder Ablenkung von einem selbst oder bewusst jemanden anderen Verdächtigen**

Verstecken von Daten

- Täter muss Aufwand und Nutzen abschätzen
- Wenn Daten benötigt werden müssen diese auch Zugreifbar sein!

Alternate Data-Streams

- **Daten können in mehreren sog. Streams gespeichert werden**
- **Muss vom Dateisystem unterstützt werden (z.B. NTFS)**
- **Praktisch handelt es sich um eine zweite Datei, die nichtt von Windows angezeigt wird**

Alternate Data-Streams

- Schema ist **Dateiname.Endung:Streamname**

z.B. Text.txt:Stream1

- Nur für „schnelles“ verstecken geeignet, Forensikprogramme finden ADS sehr schnell
- Selbst mit Nicht-Forensik-Tools können ADS sichtbar gemacht werden

Alternate Data-Streams

- **ADS können nahezu alle Daten Speichern**
- **Dateigröße wird nicht angezeigt → Auffällig wenn Datenträger voll ist, aber nur wenige kleine Daten enthält**

Nutzung verschlüsselter Container

- Neben einer Kompletterschlüsselung können auch verschlüsselte Container genutzt werden
- In der Praxis geschieht das wenn Daten getauscht oder fremde Rechner für die Tat genutzt werden

Änderung der Speicherorte

- **Daten können in nicht dafür vorgesehenen Orten gespeichert werden**
- **HPO und DCO sind Klassiker dafür, jedoch werden diese heute standardmäßig durchsucht**

Versteckte Partitionen

- **Mit entsprechenden Tools können versteckte Partitionen angelegt werden → Übungsaufgabe**
- **Eine sehr simple Methode wäre es einfach Laufwerke nicht einzubinden**

Nachbereitende AF

- Vermutlich die meisten AF-Maßnahmen sind nachbereitend
- Nachbereitende AF kann auf allen Ebenen stattfinden (Software, Betriebssystem, Hardware, Mensch, Umgebung)

Zerstörung von Hardware

- **Versuch Datenträger bzw. Geräte vor Auswertung zu schützen**
- **Häufig als Spontan-Handlung während polizeilicher Maßnahmen**
- **In IuK-Werkstätten oder forensischen Abteilungen ist oft eine Wiederherstellung möglich**

Verstecken von Asservaten

- **Fast alle Kriminellen versuchen Beweismittel zu verstecken**
- **Der Kreativität von Verstecken sind keine Grenzen gesetzt**
- **Beispielhafte verstecke: Hinter Steckdosen/Lichtschaltern, Kinderzimmer, Sex-Toys...**

Schutzmaßnahmen vor Auswertungen

- Schutzmaßnahmen sind zu unterscheiden zwischen
 - Live-Forensik
 - Post-Mortem-Forensik

Erkennung einer forensischen Auswertung

- Die Nutzung forensischer Tools kann erkannt werden
- Hierfür ist die Entwicklung von Skripten möglich, die permanent im Hintergrund überwachen welche Prozesse ausgeführt werden → Bsp. Wenn FTK.exe erkannt wird fährt das System runter oder löscht Daten

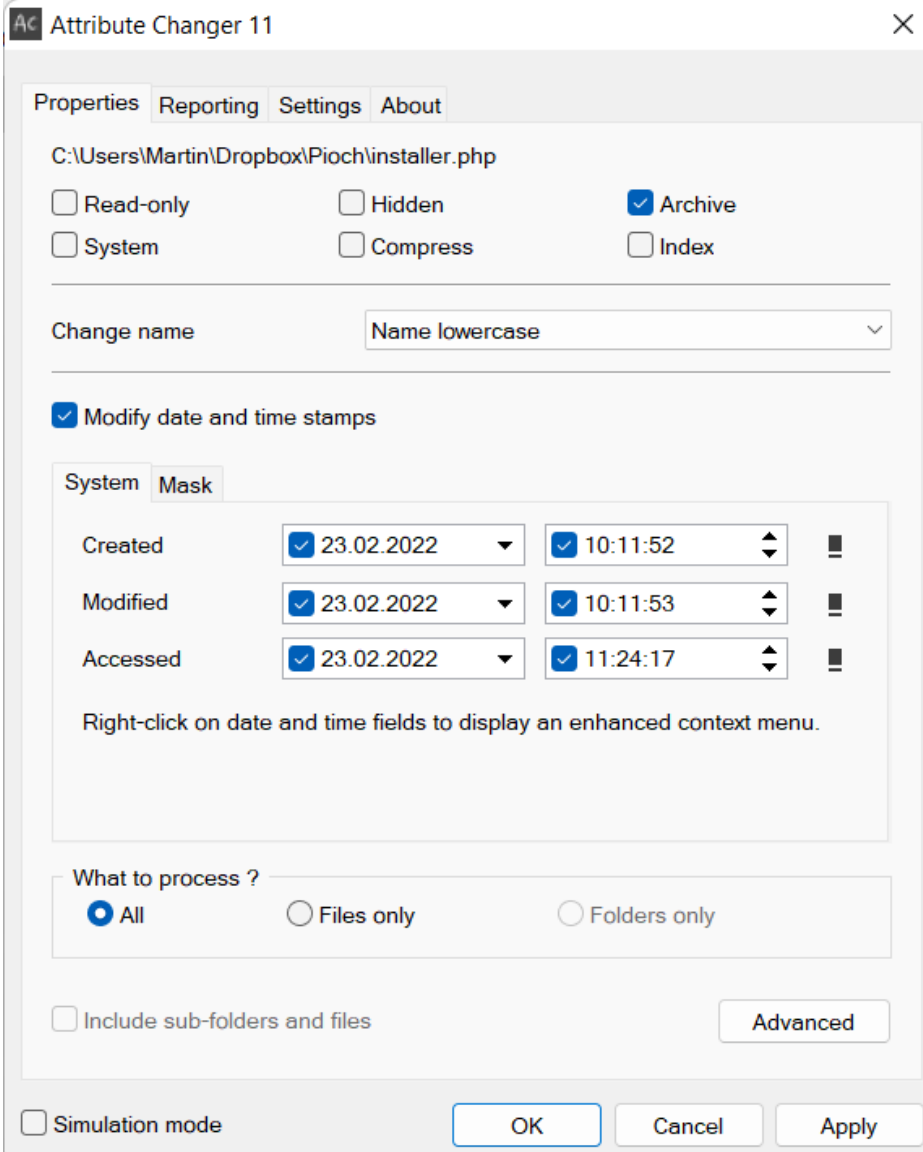
Erschweren der Auswertung

- **Der Anschluss von USB-Geräten, wie etwa Festplatten kann über Gruppenrichtlinien verhindert werden**
- **Über ein Skript kann eine erwartete Aktion in definierten Zeiträumen verlangt werden; bei Nichtausführung der Aktion werden Daten gelöscht o.ä.**

Fälschen von Spuren

- **Forensische Tools und Gutachten basieren oft auf Zeitstempeln**
- **Zeitstempel können gefälscht werden, z.B. mit Attribut**

Zeitstempel fälschen



The screenshot shows the 'Attribute Changer 11' window. The 'Properties' tab is active, displaying the file path 'C:\Users\Martin\Dropbox\Pioch\installer.php'. Under the 'Properties' section, there are checkboxes for 'Read-only', 'Hidden', 'Archive' (checked), 'System', 'Compress', and 'Index'. Below this is a 'Change name' section with a dropdown menu set to 'Name lowercase'. The 'Modify date and time stamps' checkbox is checked. Under the 'System' tab, there are three rows for 'Created', 'Modified', and 'Accessed'. Each row has a date dropdown (all set to '23.02.2022') and a time dropdown (set to '10:11:52', '10:11:53', and '11:24:17' respectively). A note below states: 'Right-click on date and time fields to display an enhanced context menu.' At the bottom, there is a 'What to process ?' section with radio buttons for 'All' (selected), 'Files only', and 'Folders only'. There is also an 'Include sub-folders and files' checkbox and an 'Advanced' button. At the very bottom, there is a 'Simulation mode' checkbox and 'OK', 'Cancel', and 'Apply' buttons.

Attribute Changer 11

Properties Reporting Settings About

C:\Users\Martin\Dropbox\Pioch\installer.php

☐ Read-only ☐ Hidden ☒ Archive

☐ System ☐ Compress ☐ Index

Change name Name lowercase

☒ Modify date and time stamps

System Mask

Created ☒ 23.02.2022 ☒ 10:11:52

Modified ☒ 23.02.2022 ☒ 10:11:53

Accessed ☒ 23.02.2022 ☒ 11:24:17

Right-click on date and time fields to display an enhanced context menu.

What to process ?

☒ All ☐ Files only ☐ Folders only

☐ Include sub-folders and files

Advanced

☐ Simulation mode

OK Cancel Apply

Erkennung von VM-Umgebungen

- **Anhand von Hardware-Informationen oder ähnlichen können VMs erkannt werden**
- **Was könnte dagegen helfen?**

Weitere AF-Maßnahmen

- **Erzeugung von Datenmüll**
- **Ändern von File-Headern und Endungen →
Probieren sie deren Analyse danach mit
Autopsy**
- **Fernzugriff bei Live-Forensik**

**Danke für Ihre
Aufmerksamkeit!**