Digitale Ermittlungen

Master Studiengang Digitale Forensik, Seminararbeit Modul 113

Gruppe 4

**Dominik Hajas, Francisco Alej. Juez Liedke , Kevin Jonas, Markus Stoll**

**Datum 16.03.2018**

2. Zwischenbericht

Inhaltsverzeichnis

1 Zwischenbericht 3

1.1 Zusammenfassung 3

1.1.1 Verdacht auf Verbreitung von Malware gem. § 202c und § 303a StGB 3

1.1.1.1 Server 3

1.1.1.2 Client 3

1.1.2 Beurteilung 4

1.2 Anhang 5

# Zwischenbericht

## Zusammenfassung

### Verdacht auf Verbreitung von Malware gem. § 202c und § 303a StGB

#### Server

|  |  |
| --- | --- |
| **Beschreibung** | **Abbildung** |
| Auf dem Server wurde die Datei Supermario.exe gefunden. |  |
| Mittels „https://www.virustotal.com“ wurde diese als Maleware erkannt. | 1 |
| Der Server war im Internet unter „http://vhost1.myflatpressserver.de/" erreichbar. |  |
| Im accesslog wurde ermittelt, dass die Datei supermario.exe wie folgt heruntergeladen wurde:  IP Adresse 192.168.178.101 am 28/Aug/2015:12:15:37 GET  IP Adresse 192.168.178.102 am 28/Aug/2015:12:19:13 GET | 2 |

#### Client

|  |  |
| --- | --- |
| **Beschreibung** | **Abbildung** |
| ***Benutzeraccounts***  Zu den Standardaccounts Administrator und Gast gibt es nur einen zusätzlichen Account mit dem Namen **vagrant**.  Letzter Login: 28/Aug/2015: 12:23:54 | 3 |
| ***IP Adresse*** 192.168.178.101 | 4 |
| ***Webhistory***  Zugriff auf die Datei supermario.exe auf dem Server.  28.8. 2015 14:23:55 UTC+2 | 5 |
| ***Prefetch***  Im Prefetch wurde ein Eintrag der supermario.exe gefunden. Dies belegt, dass die Datei ausgeführt wurde. | 6 |
| ***Trojaner-Datei itiscea.exe***  Im Autostart des User **vagrant** wurden der Eintrag der itiscea.exe gefunden.  Die Datei itiscea.exe wurde auf virustotal.com als Trojaner eingestuft. | 7  8 |
| ***Dateien mit ADS***  Die folgenden 4 Dateien wurden mit einem ADS gefunden.  ADS Ströme sind keine Malware. | 9 |
| ***Internet Explorer***  Der Server „myflatpressserver.com wurde im Internetexplorer vom Benutzer vagrant eingegeben. | 10 |
|  |  |
| ***Installierte Software***  Die folgenden Softwarepakete wurden installiert: Oracle VM virtual guest Additions. | 11, 12 |
| ***USB angeschlossene Geräte***  Ein USB Geräte VID\_80EE&PID\_0021 wurde angeschlossen. Hier bin ich noch nicht sicher was dieses war. Es gibt im Internet zwei Hinweise: USB\_Tablet und USB device treiber von virtual box | 13 |
| ***Windows Programm Kompatibilität Cache***  Der Kompatibilität Cache enthält keine Einträge. Normal bekommt jedes gestartete Programm einen Eintrag! | 14 |
| ***Windows Version***  Windows 7 Professional SP1 | 15 |
| ***Mounted Devices***  C: Harddisk  D: IDE CD ROM | 16 |
| ***Firewall Einträge für z.B. Filesharing – Programme…***  Keine Anwendungen mit erlaubtem Zugriff auf außenstehende Verbindungen durch die Firewall. | 17 |
| ***System Time***  UTC+2 | 18 |

### Beurteilung

Der Server hat die Datei supermario.exe zum Download bereitgestellt. Supermario.exe ist eine Malware und wurde zwei Mal heruntergeladen.

Der PC des Benutzers vagrant hatte auf den Server und die Datei supermario.exe Zugriff. Diese wurde auf den PC heruntergeladen und ausgeführt.

Dabei ist folgendes noch nicht klar.

1. Der letzte Login des Benutzers vagrant lag nach den Zeitstempeln jedoch nach dem Download auf dem Server.
2. Welchen Einfluss hat der Tojaner itiscea.exe und die Dateien mit ADS.

## Anhang

Abbildung 1: Server - Prüfergebnis der supermario.exe auf virustotal.com

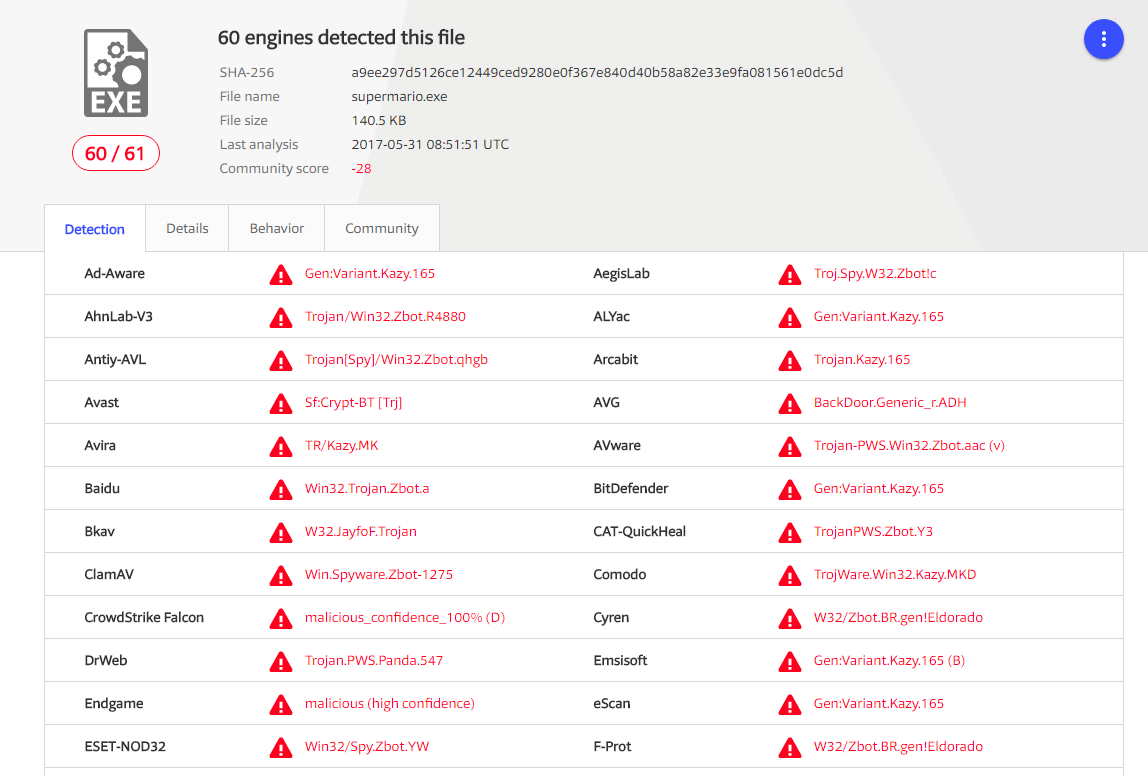


Abbildung 2: Server - accesslog

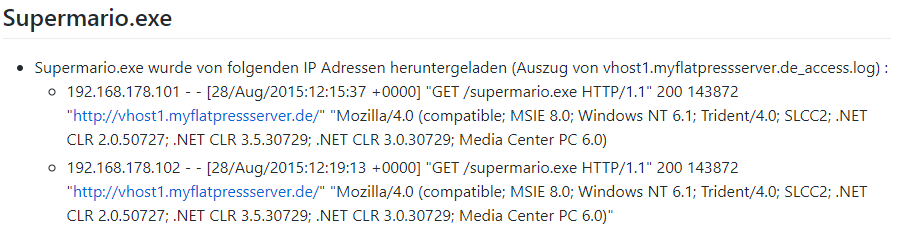


Abbildung 3: Client - Benutzeraccounts auf dem Client

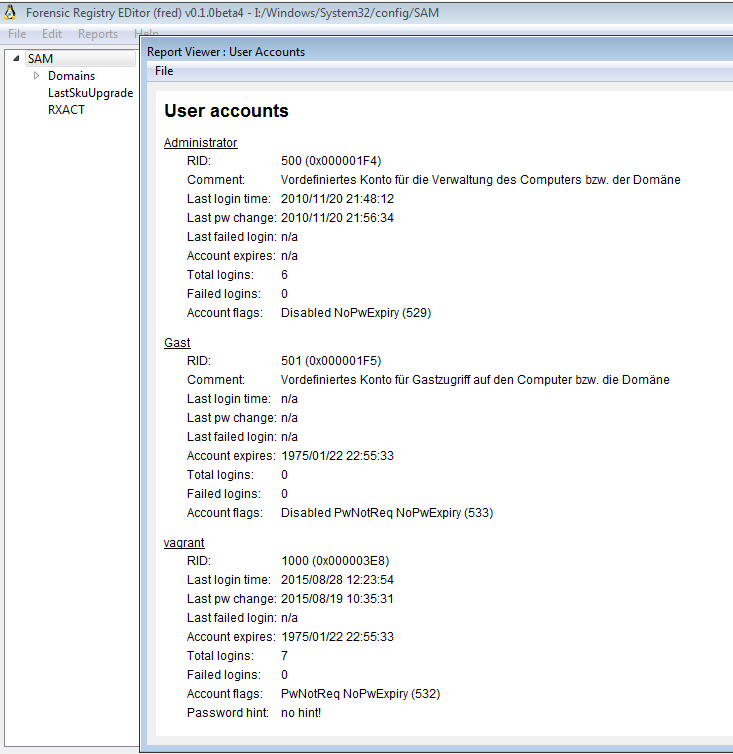


Abbildung 4: Client Netzwerkkonfiguration



Abbildung 5: Client - Zufriff auf die Datei supermario.exe auf dem Server

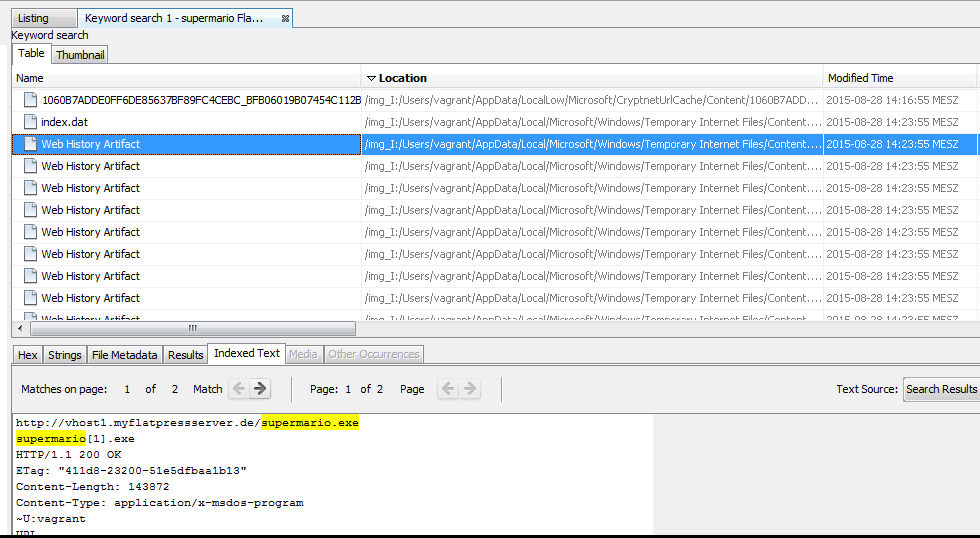


Abbildung 6: Client - Eintrag im Prefetch für den Start der Datei

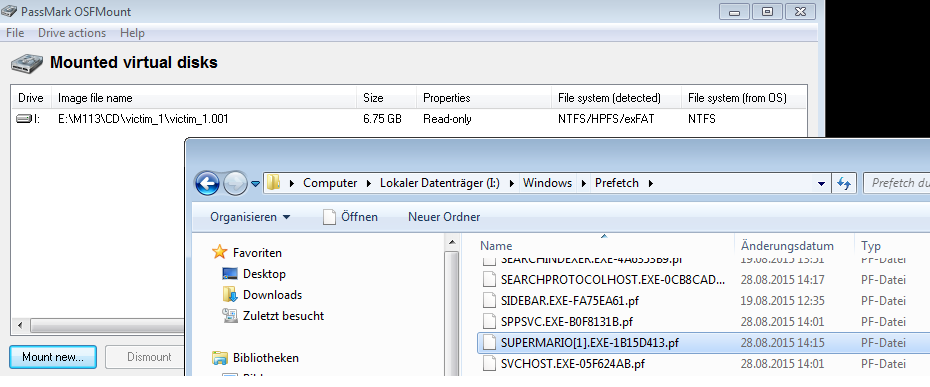


Abbildung 7: Client Autostart der Datei itiscea.exe

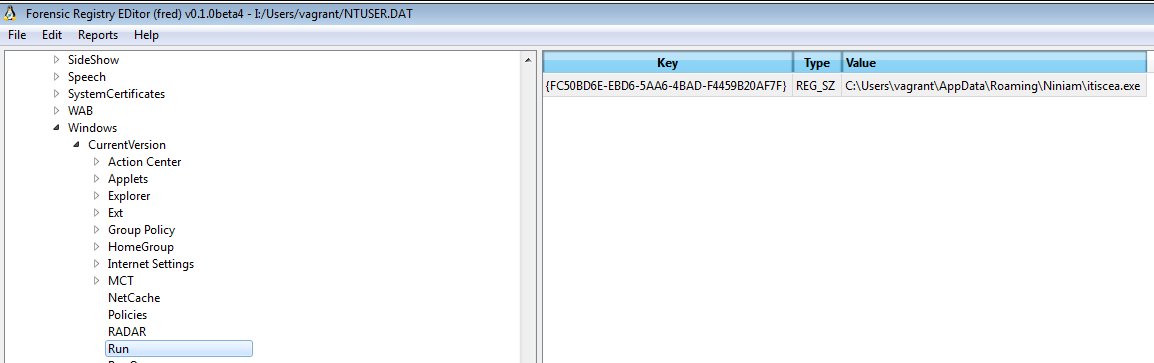


Abbildung 8: Client - Prüfergebnis der Datei itiscea.exe auf virustotal.com

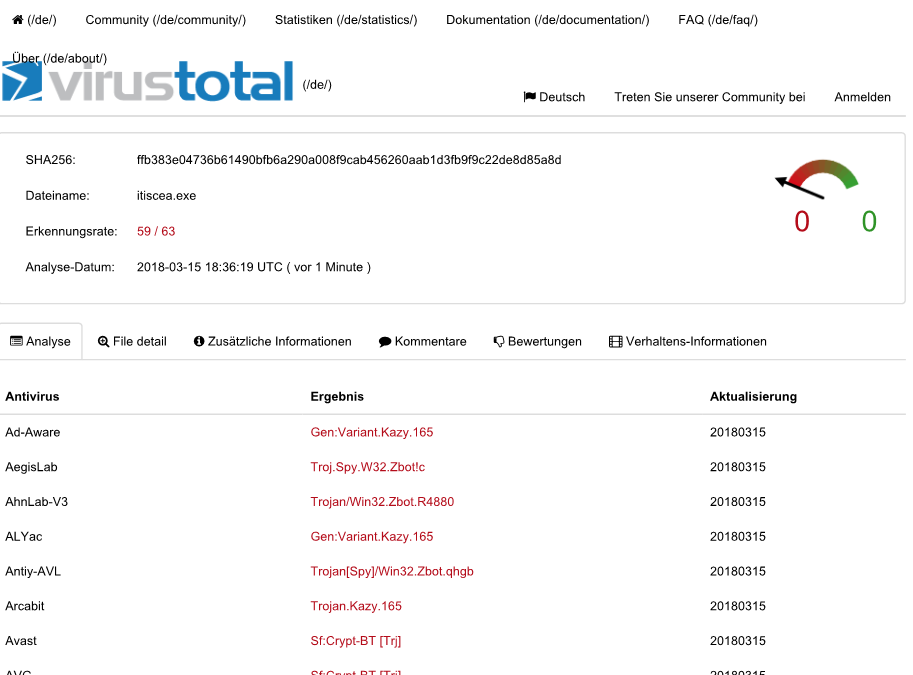


Abbildung 9: Client - Dateien mit ADS

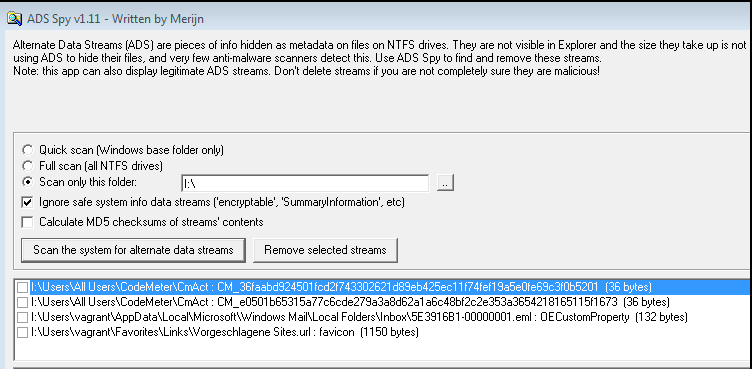


Abbildung 10: Client - Internet Explorer typed URL

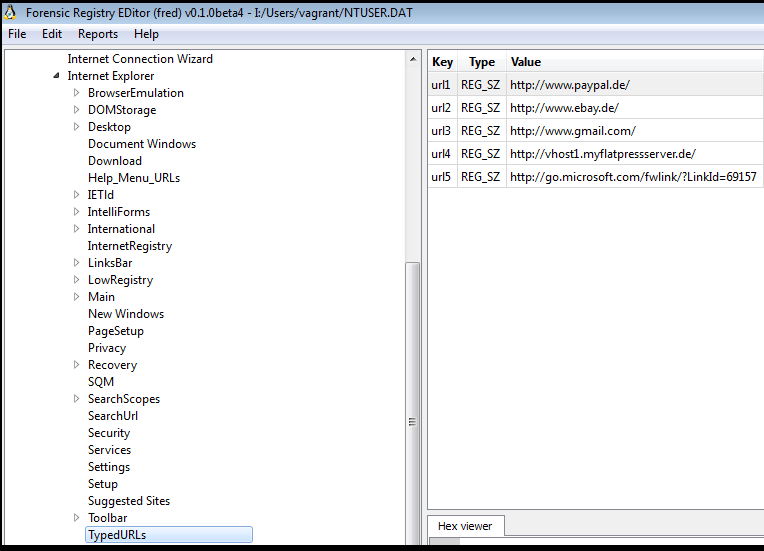


Abbildung 11: Client - installierte 64 Bit Anwendungen

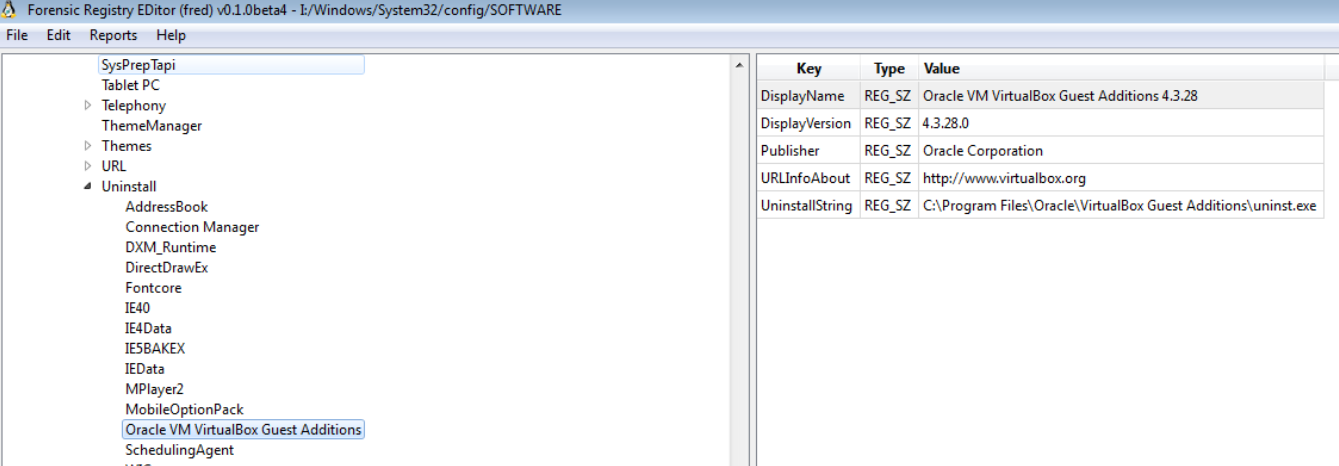


Abbildung 12: Client - installierte 32 Bit Anwendungen

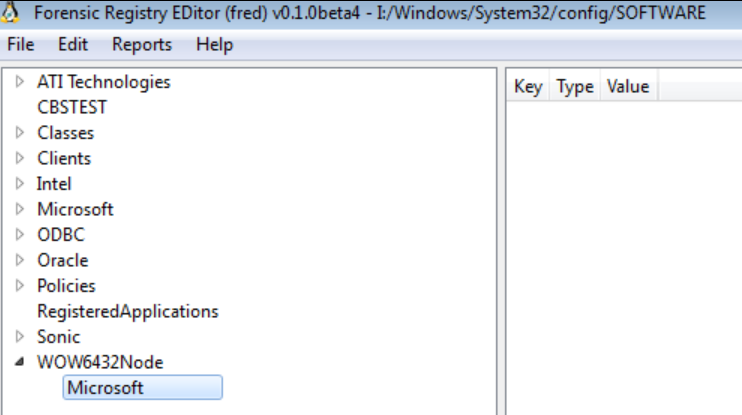


Abbildung 13: Client - angeschlossene USB Geräte

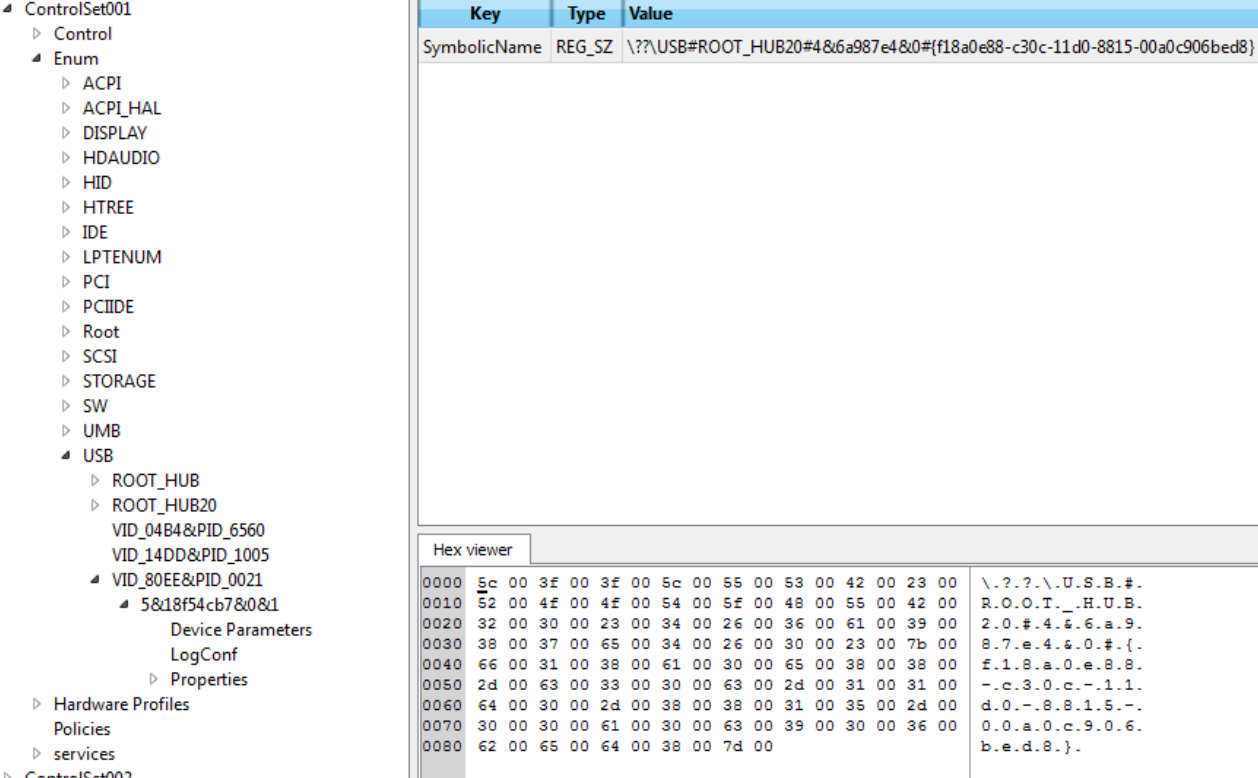


Abbildung 14: Client Programm Kompatibilität Cache

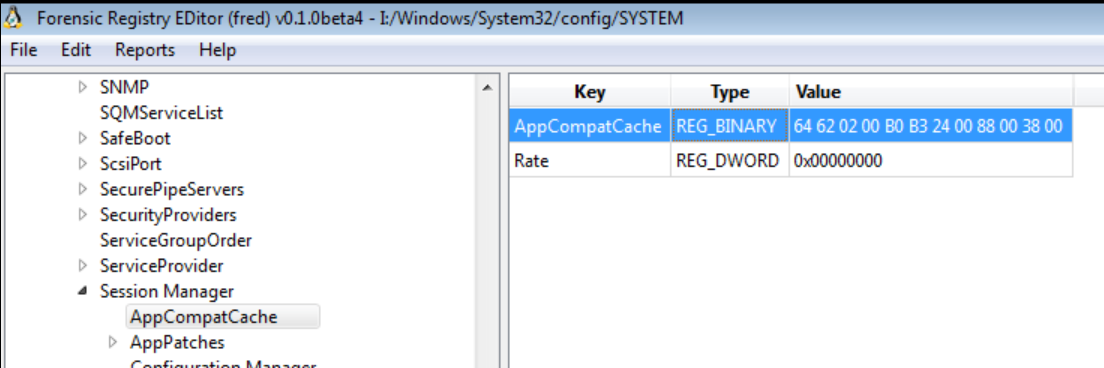


Abbildung 15: Client - Windows Version

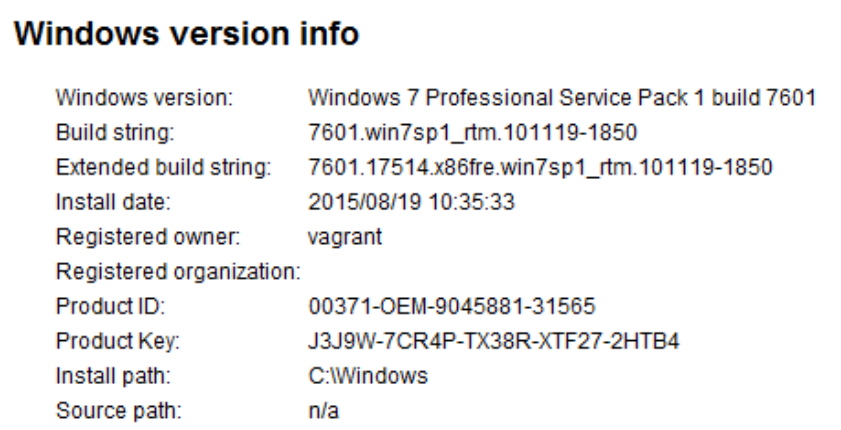


Abbildung 16: Client - mounted devices

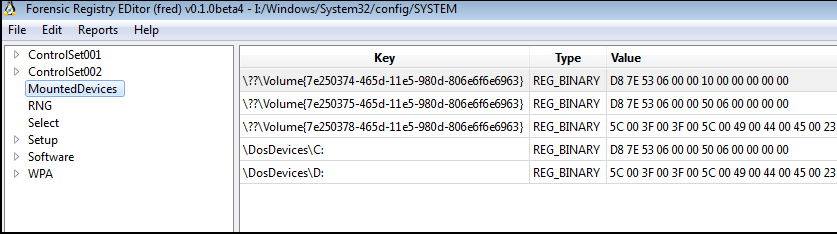


Abbildung 17: Client - Einträge in der Firewall für z.B. Filesharing Programme

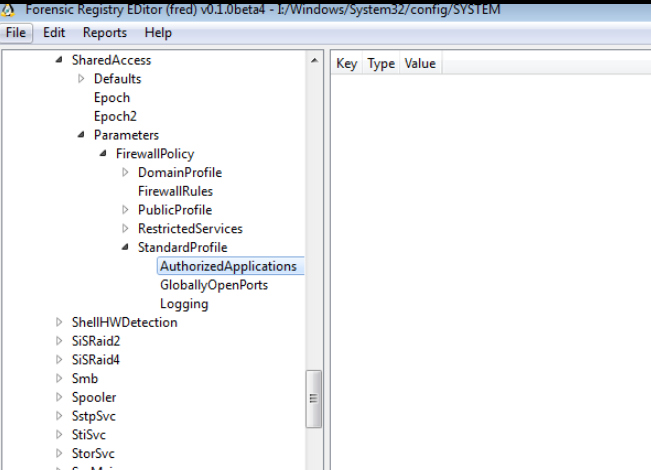


Abbildung 18: Client - system time info

