

Digitale Forensik

Moritz Rupp
Dean Basic

Untersuchungsauftrag: Verdacht auf Ausspähen von Daten innerhalb des Firmennetzwerks gem.
§202a StGB und Steuerbetrugs gem. § 370 AO

Inhaltsverzeichnis

Seite 2
Seite 3
Seite 4
Seite 5 -6
Seite 6-7
Seite 8-10
Seite 11-12
Seite 12
Seite 13
Seite 14
Seite 15
Seite 15

Inhaltsverzeichnis
Beteiligte Personen
Untersuchungsgegenstand
Feststellung der Asservate
Bergung der Daten
Beweisliste
Beweiskette
Beweisführung Spionage
Beweisführung Steuerbetrug
Zusammenfassung
Fazit
Quellenverzeichnis

1 Beteiligte Personen

1.1 Auftraggeber

Staatsanwaltschaft HS-Albsig	Kontakt
Prof. Dr. Morgenstern	morgenstern@hs-albsig.de
Simon Malik	maliks@hs-albsig.de

1.2 Auftragnehmer

Gutachter	Kontakt
Moritz Rupp	ruppmori@hs-albsig.de
Dean Basic	basicdea@hs-albsig.de

1.3 Beschuldigter

Beschuldigter	Tatverdacht
Andreas Wurstmann	Ausspähung von Daten innerhalb eines Firmennetzwerkes gem § 202a StGB und Steuerbetrug gem § 370 AO

1.4 Zeugen

Zeuge	Aussage
Alfred Riess-Pohlmann	Herr Wurstmann nannte eine korrekte Kombinationen von Benutzernamen und Passwort eines Mitarbeiters.

1.5 Geschädigte

Geschädigter	Schadensereignis
Y-Ways Technologies	Veruntreuung und Änderung von Steuerunterlagen, Spionage innerhalb des Firmennetzwerks

2 Untersuchungsgegenstand

2.1 Anklageschrift

Die Staatsanwaltschaft lässt auf Grundlage des Untersuchungsauftrages, der am 12.05.2022 ausgehändigt wurde, folgenden Tatverdacht prüfen.

Gegen Herr Andreas Wurstmann besteht der Verdacht des Ausspähens von Daten innerhalb eines Firmennetzwerks gem § 202a StGB und Steuerbetrugs gem. § 370 AO.

Im konkreten Fall soll der Angeklakte Steuerunterlagen der Firma Y-Ways gefälscht haben, sowie verschiedene Zugangsdaten von Mitarbeiter Accounts veruntreut haben.

Bezüglich beiden Verdachtsfällen existieren Zeugenaussagen welche die Anklage stützen.

Den vollständigen Untersuchungsauftrag kann dem beigelegten Ordner entnommen werden.

2.2 Beweismittel

Bei der Durchsuchung des Arbeitsplatzes von Herr Wurstmann hat die Staatsanwaltschaft bereits Datenträger sicherstellen können. Diese sind mitsamt der MD5-Summe des Image für die Beweisführung auswertbar.

Der Datenträger(Asservat 01) des Arbeitsplatzrechners von Herr Wurstmann, stellt den Einstieg der Forensischen Untersuchungen dar.

Desweiteren hat der potentiell geschädigte Hr. Alfred Riess-Pohlmann zugestimmt seinen Datenträger der Untersuchung bereitzustellen(Asservat 02).

Eine formelle Auflistung der Beweismittel mit zugehörigem Hashwert und Aushändigungsdatum, können Beweismittelauflistung 01 entnommen werden.

2.3 Beschlagnahmung

Die gesicherten Beweismittel wurden uns von der Staatsanwaltschaft in Form eines Downloads zugestellt.

Die Auswertung des Datenträgers findet auf einem speziell gesicherten bzw. überwachten System statt. Dieser Computer ist mit einem langen sicheren Passwort geschützt, welches nur den Gutachtern bekannt ist. Zu keiner Zeit wurde der Computer von einer unbefugten Person verwendet.

Vor Beginn des Gutachtens wurde das System ausgiebig getestet mit dem Ergebniss das keine Komprimierung vorliegt. Die Auswertung der Beweismittel erfolgt auf einer Virtuellen Maschine auf der ein Windows 10 Betriebssystem läuft. Die Virtuelle Maschine wurde auf Forensische Untersuchungen ausgelegt und anhand von einer MD5 Prüfsumme auf Integrität überprüft.

3 Feststellung der Asservate

Die Asservate client.E01 und sysop.E01 wurden uns am 12.05.2022 übergeben und stellen den Untersuchungsanfang dar. Die Asservate können durch die mitgelieferte Prüfsumme identifiziert werden. In beiden Fällen handelt es sich um ein Windows 7 Betriebssystem. Folgend sind die Eckdaten des Asservates formal aufgelistet.

Beweismittelauflistung 01

Das Image Client.E01 stellt den Arbeitsplatzrechner von dem potentiell geschädigten Alfred Riess-Pohlmann dar.

Referenz	Details
Asservat-Nr.	1
Dateiname	Client.E01
Erstelldatum	29.11.2019
Ausstellungsdatum	12.05.2022
MD5 Hashsumme	3c2167183c21e741bda57966861e6e1c
SHA1 Hashsumme	9e46515995f0a9e7cc081dd30d193b155d44d43f
Größe	42,949,672,960
Partitionen	vol1, vol2, vol3, vol4
Sektorenanzahl	83886080

Das Image sysop.E01 stellt den Arbeitsplatzrechner des beschuldigten Herr Wurstmann dar.

Referenz	Details
Asservat-Nr.	2
Dateiname	sysop.E01
Erstelldatum	29.11.2019
Ausstellungsdatum	12.05.2022
MD5 Hashsumme	f98f910fb971f2718527e3e8ffcd6fa7
SHA1 Hashsumme	89a4548dd877bab86414cd00529c35107938cbd8
Größe	42,949,672,960
Partitionen	vol1, vol2, vol3, vol4
Sektoren	83886080

Das Image gateway.E01 stellt ein Gateway bzw. Den DHCP Server des Netzwerkes dar.

Referenz	Details
Asservat-Nr.	3
Dateiname	gateway.E01
Erstelldatum	29.11.2019
Ausstellungsdatum	30.06.2022
MD5 Hashsumme(gepackt)	fc971632664d72dae7450e253fdebd06
SHA1 Hashsumme(gepackt)	f68217486228b7653e55f77c00a99e4c8d27a813
Größe(entpackt)	40,960,672,960
Partitionen	vol1, vol2, vol3, vol4
Sektorenanzahl	83886080

4 Bergung aller Daten

4.1 Reduzierung der Daten

Von der Staatsanwaltschaft wurden uns zwei Images zur Verfügung gestellt.

Zum einen handelt es sich um ein Image der Festplatte des mutmaßlich Geschädigten Herrn Alfred Riess-Pohlmann(vgl. Asservat 01). Zum anderen handelte es sich um ein Image der Festplatte des Beschuldigten Herrn Wurstmann(vgl. Asservat 02).

Für eine weitere Analyse der Daten mussten wir die zur Verfügung gestellten Daten hinsichtlich Ihrer Relevanz für den Untersuchungsauftrag klassifizieren. Bei diesem Schritt wird bestimmt welche Daten für den Fall wichtig sein könnten.

Dabei sind folgende Daten vermutlich relevant für den Verdacht auf Ausspähen von Daten innerhalb eines Firmennetzwerks.

Da der Verdacht besteht dass der Beschuldigte Daten über das Firmennetzwerk ausgespäht hat, lag ein Hauptaugenmerk darauf Aufzeichnungen über die Netzwerkaktivität zu erlangen.

Hierüber hätte versucht werden können, sensible Daten mitzuschneiden und damit auch abzugreifen.

Dabei sind die Logs über den Netzwerkverkehr sowohl vom Geschädigten als auch vom Beschuldigten relevant. Da sie Rückschlüsse darüber geben mit wem, wann kommuniziert wurde. Als nächstes wurde auf dem Image des Beschuldigten nach installierten Programmen gesucht und ob beziehungsweise wann diese ausgeführt wurden. Dies erlaubt Einblicke darauf was wirklich auf dem Rechner installiert ist und damit möglicherweise auch ob die Tat überhaupt durchgeführt hätte, werden können mit den zur Verfügung stehenden Mitteln.

Zudem wurden die Browsercookies sowohl vom Geschädigten Riess-Pohlmann als auch vom Beschuldigten ausgelesen. Dies erlaubt Rückschlüsse darüber was im Browser geschehen ist, welche Angaben wann und wo gemacht wurden, sowie welche Websites wann besucht wurden.

Folgende Daten sind vermutlich relevant für den Verdacht auf Steuerbetrug.

Beim Verdacht auf Steuerbetrug werden nur Daten vom Image des Beschuldigten benötigt.

Auch hier sind die installierten Programme relevant da ein Programm installiert sein könnte, welches für die Steuer verwendet wird. Falls ein solches Programm gefunden wird, werden auch die Dateien im Speicherformat dieses Steuerprogrammes relevant.

Als nächstes werden die Dokumente ausgelesen da sich auch dort Steuerunterlagen befinden könnten.

Anschließend wurde mit einer Keyword Search nach den Begriffen Rechnung, Steuer und Steuererklärung gesucht. Wenn diese Begriffe in einer Datei auf dem Rechner verwendet wurden, dann werden die betreffenden Dateien damit gefunden.

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context
			● EnableDHCP			Metadata	
			● NameServer			Name: DhcpServer	
			● Domain			Type: REG_SZ	
			● RegistrationEnabled			Value	
			● RegisterAdapterName			192.168.178.254	
			● DhcpIPAddress				
			● DhcpSubnetMask				
			● DhcpServer				
			● Lease				

Nachdem in Image sysop.E01 Hinweise auf ein weiteres Gerät, in Form eines Netzwerkgateways gefunden wurden, konnte die Staatsanwaltschaft

dieses für weitere Untersuchungen bereitstellen.

Die Hinweise fanden sich bei Untersuchungen der Netzwerkkonfiguration.

Unter /vol_vol03/Windows/system32/config/System konnte eine DHCP Adresse gefunden werden.









4.2 Beweisliste

Auflistung relevanter installierter Programme in sysop.E01:

Befund Nr. 1	
Programmname	Beschreibung
Wireshark	Netzwerkanalyse tool. Packer sniffer
Tor-Browser	Browser Software für anonyme Internet Nutzung
Cain und Abel	Multifunktionale Spionagesoftware
Virtual-box	Virtualisierungssoftware
Puppet	Administrationsprogramm
Winrtgen	Rainbow table generator

Auflistung relevanter ausgeführter Programme in sysop.E01 mit Timestamp:





Befund Nr. 2

 CAIN.EXE-578E80AC.pf			CAIN.EXE	/PROGRAM FILES/CAIN	2019-11-29 10:15:11 CET	2	Prefetch File	sysop.E01
 CAIN.EXE-82B85A37.pf			CAIN.EXE	/PROGRAM FILES/CAIN	2019-11-28 16:42:17 CET	1	Prefetch File	sysop.E01
 CA_SETUP_4.9.56.EXE-B96A29FE.pf			CA_SETUP_4.9.56.EXE	/USERS/VAGRANT/DOWNLOADS	2019-11-28 16:36:05 CET	1	Prefetch File	sysop.E01
 VBOXDRVINST.EXE-7DCD6070.pf			VBOXDRVINST.EXE	/PROGRAM FILES/ORACLE/VIRTUALBOX GUEST ADDITIONS	2015-08-19 12:37:42 CEST	9	Prefetch File	sysop.E01
 VBOXTRAY.EXE-1D286C83.pf			VBOXTRAY.EXE	/WINDOWS/SYSTEM32	2019-11-28 16:35:26 CET	2	Prefetch File	sysop.E01
 VBOXWINDOWSADDITIONS-X86.EXE-C4ADF8B8.pf			VBOXWINDOWSADDITIONS-X86.EXE		2015-08-19 12:37:12 CEST	1	Prefetch File	sysop.E01
 VBOXWINDOWSADDITIONS.EXE-EE01DD11.pf			VBOXWINDOWSADDITIONS.EXE		2015-08-19 12:37:10 CEST	1	Prefetch File	sysop.E01
 WIRESHARK-WIN64-3.0.6.EXE-8AEFAAD6.pf			WIRESHARK-WIN64-3.0.6.EXE		2019-11-28 16:41:18 CET	1	Prefetch File	sysop.E01

Die Webhistory von sysop.E01 liefert zudem weitere Befunde.

Folgend ein Ausschnitt relevanter Besuche. Die gesamte Web-History ist aufgrund der Größe als mitgelieferten Ordner einsehbar.

Befund Nr. 3

 index.dat	1	https://www.torproject.org/static/fonts/fontawesome/png...	2019-11-29 09:07:36 CET		Internet Explorer	torproject.org	sysop.E01
 index.dat	1	https://www.torproject.org/static/fonts/fontawesome/png...	2019-11-29 09:06:17 CET		Internet Explorer	torproject.org	sysop.E01
 index.dat	1	https://www.torproject.org/static/css/bootstrap.css?h=31...	2019-11-29 09:07:35 CET		Internet Explorer	torproject.org	sysop.E01
 index.dat	1	https://www.torproject.org/static/fonts/fontawesome/png...	2019-11-29 09:06:17 CET		Internet Explorer	torproject.org	sysop.E01

Nr.	4
Dateiname	HTTPS-2019112992419579-49529.txt
Bezeichnung	Cain und Abel sniffing files
Erstellung	29/11/2019 09:24:19 CET
Letzter Zugriff	29/11/2019 09:24:19 CET
Modification	29/11/2019 09:24:24 CET
Fundort	<i>img_sysop.E01/vol_vol3/programm Files/Cain/HTTPS</i>
Hashes	MD5: 7bc47d5ad2a2682eb0e3ecf1665300a4 SHA-256: a4cd9d3c499b236ad0c8ad159722cb0726e9267bd64b820c0f4eddf9366fb8a0

Nr.	5
Dateiname	HTTPS-2019112817254771-49170.txt
Bezeichnung	Cain und Abel sniffing file
Erstellung	28/11/2019 18.02.54 CET
Letzter Zugriff	28/11/2019 18:02:54 CET
Modification	28/11/2019 18:02:54
Fundort	<i>img_sysop.E01/vol_vol3/programm Files/Cain/HTTPS/</i>
Hashes	MD5 Hash ec3cbe4c8ab98d27f4a62ef905978b4b SHA-256Hash:e70464020109658ab5dcfc6d90a1c7e165df74c64f9ae0d9b526ce18d6850563

Nr.	6
Dateiname	HTTPS-2019112991911586-49373.txt
Bezeichnung	Cain und Abel sniffing file
Erstellung	2019-11-29 10:19:11 CET
Zugriff	2019-11-29 10:19:11 CET
Modification	2019-11-29 10:19:12 CET
Fundort	<i>img_sysop.E01/vol_vol3/programm Files/Cain/HTTPS/</i>
Hash	MD5 Hash 8ceef4966f5bba86499ed9d2ba9e9a5d SHA-256 Hash afe5d4dbd7ef0b9123b21db04ad4e946dcd4ab87754dbb398d41a0ceb69d68a4

Nr.	7
Dateiname	Chained_172.217.14.99.crt
Bezeichnung	SSL Zertifikat

Hierbei wurde IP Adressen in den Netzwerkkonfigurationen gefunden(vgl. Befund 8). Über diese konnten den Asservaten(vgl. Beweismittelaufstellung 01) eine IP-Adresse zugeordnet werden. Anschließend wurde nach installierte Programmen gesucht. Hierbei sind Executables von Wireshark, Cain und Abel, Virtualbox , Puppet sowie Winrtgen in dem Dowload Ordner gefunden worden(vgl. Befund 1). Anschließend wurden die Order der jeweiligen Programme untersucht. Im Systemordner von Cain und Abel wurden Beweise festgestellt(vgl. Befund 4-7). Hierbei fanden sich Netzwerkaufzeichnungen eines anderen Netzteilnehmers. Nach folgender Recherche wurde festgestellt, das diese Aufzeichnungen höchstwahrscheinlich anhand ARP Spoofing entstanden sind.

Hierzu eine Ausführung in fern dies Ermittlungstechnisch relevant sein könnte..

Adress Resolution Protocoll:

Alle Computer systeme haben eine individuelle statische Adresse. Diese Rechneradresse wird auch als Media Access Control oder MAC-Adresse bezeichnet. Mit dieser kann auf ein Computer zurückgeführt werden. Um über Netzwerkdienste zu Kommunizieren wird jedoch eine Internet-Protokoll-Adresse (IP Adresse) benötigt, die ein Netzwerkteilnehmer zugewiesen bekommt. Mit Hilfe des Address Resolution Protocols (ARP) ist es nun möglich, zu einer bekannten Netzwerk Adresse die physikalische MAC-Adresse zu ermitteln.

Dazu sendet ARP ein Anforderungspaket an alle Rechner im LAN und fragt, ob einer der Rechner weiß, dass er diese bestimmte IP-Adresse verwendet. Wenn eine Maschine die IP-Adresse als ihre eigene erkennt, sendet sie eine Antwort, sodass ARP den Cache für zukünftige Referenzen aktualisieren und mit der Kommunikation fortfahren kann.

Dies können sich Angreifer mithilfe von ARP Spoofing zunutze machen.

ARP Spoofing:

Hierbei wird versucht den Netzwerkverkehr eines Opfers mitzuschneiden und gegebenenfalls zu Manipulieren und auszuwerten. Dies wird bewerkstelligt indem sich der Angreifer als Router ausgibt bzw. zwischen Opfer und Router stellt und somit jeglichen Datenverkehr des Opfers mitlesen kann. Dies wird auch Man-in-the-middle Angriff genannt.

Hierfür benötigt der Angreifer einen Netzwerkscanner wie Wireshark um die Ip-adressen von mindestens 2 Geräten zu finden. Darunter können auch Virtuelle Maschine sein. Des weiteren wird ein Angriffstool wie Cain und Abel benötigt das falsche ARP Requests etc. stellt. Der Datenträger von Herr Wurstmann weißt alle benötigten Programme auf um solch einen Angriff durchzuführen. Hierbei sind insbesondere die Programme Wireshark, Cain und Abel, Virtual-box sowie Winrtgen relevant(vgl. Befund 1).

Im konkreten Fall wurden im Ordner des Programmes Cain und Abel mitschnitte von Herr Pohlmanns Netzwerkverkehr gefunden(vgl. Befund 4-7). Die Anfragen nach Webseiten decken sich mit denen auf Herr Pohlmann Datenträger. Eine ausführliche Beschreibung dieser Annahme findet sich in der Beweisführung 05.

Im Programmordner von Cain und Abel wurden zudem Zertifikatsdateien gefunden(vgl. Befund 7).

Ein SSL-Zertifikat stellt die Identität einer Webseite sicher und ist einfach ausgedrückt ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Ein Zertifikat an sich ist dabei ein simpler Datensatz: In einer Datei sind zahlreiche Informationen enthalten wie zum Beispiel der Name des Ausstellers, die Seriennummer oder auch der sogenannte Fingerabdruck für die Verschlüsselung. Diese Zertifikate müssen von einer Zertifizierungsstelle ausgehändigt werden.

Im Rahmen des Untersuchungsauftrages in Verbindung mit ARP-spoofing kann Zertifikate spoofing ein weiterer Verdachtfall sein.

Cain und Abel:

Cain und Abel ist ein Multifunktionswerkzeug das größtenteils für Spionagezwecke verwendet wird. Es erlaubt das Cracking von verschlüsselten Passwörtern mit Hilfe einer Wörterbuch-, Brute-Force- und Rainbow-Table Attacke. Des Weiteren ist das Aufzeichnen von Netzwerkverkehr anhand ARP-Spoofing möglich.

5 Beweisführung Spionage im Firmenetzwerk

Da Herr Wurstmann gegenüber Herr Riess-Pohlmann korrekte Anmeldedaten genannt hat, stellt sich nun die Frage ob und wie er in Besitz dieser Informationen gelangt ist.

Auf dem Aservat Client.E01 war eine Anmeldung von Herrn Riess-Pohlmann zu finden. Diese Anmeldung war bei der Webmail der Universität Erlangen. Die Universität ist unter dem Link <https://faumail.uni-erlangen.de> erreichbar. Bei dieser Anmeldung von Herrn Riess-Pohlmann wurde sowohl eine Email als auch ein Passwort abgefragt. Der mutmaßlich Geschädigte Herr Riess-Pohlmann hat seine Daten eingegeben. Diese wurden dann per HTTP über das Firmennetzwerk übertragen. Über einen Token war es dann möglich den Usernamen und das Passwort abzufangen.

The screenshot displays the Cain & Abel software interface. At the top, there are various filter tabs like 'Evidence', 'Artifacts', 'Content types', etc. The main window shows 'MATCHING RESULTS (2 of 6)' with a table listing files. The selected file is 'HTTPS-2019112992419579-49529.txt' from 'sysop.E01 - Partition 2 (Microsoft NTFS, 39.9 GB)'. The right pane shows a 'PREVIEW' of the file's content, which includes a cookie and a token. Below the preview, there is a 'DETAILS' section with 'ARTIFACT INFORMATION' and 'EVIDENCE INFORMATION'.

Filename	Last Modified	Last Accessed	Created Date	Size	Source
HTTPS-2019112993038213-49533.txt	29/11/2019 09:30:42	29/11/2019 09:30:38	29/11/2019 09:30:38	4622	sysop.E01 - Partition 2 (Microsoft NTFS, 39.9 GB)(P...
HTTPS-2019112992419579-49529.txt	29/11/2019 09:24:24	29/11/2019 09:24:19	29/11/2019 09:24:19	4595	sysop.E01 - Partition 2 (Microsoft NTFS, 39.9 GB)(P...

PREVIEW

Cookie: roundcube_sessid=4ee66e8aac7b6f6e8e537ev6

token=skWpJrwZkklngJadUskBr4tVkdZCH4Tl&_task=login&_actor=pohlmann@fau.de&_pass=EmsSch%G39%BgnerTag17

[Server-side data (788 bytes)]
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2019 09:24:18 GMT
Server: Apache/2.4.18
Strict-Transport-Security: max-age=31536000
Expires: Fri, 29 Nov 2019 09:24:18 GMT
Cache-Control: private, must-revalidate
Pragma: private
Last-Modified: Fri, 29 Nov 2019 09:24:18 GMT

DETAILS

ARTIFACT INFORMATION

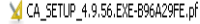
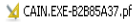
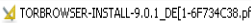

Filename: HTTPS-2019112992419579-49529.txt
Last Modified Date/Time: 29/11/2019 09:24:24
Last Accessed Date/Time: 29/11/2019 09:24:19
Created Date/Time: 29/11/2019 09:24:19
Size (Bytes): 4595

EVIDENCE INFORMATION

Source: sysop.E01 - Partition 2 (Microsoft NTFS, 39.9 GB)

Für das Abfangen der Daten werden spezielle Programme verwendet, eines dieser Programme ist Cain & Abel. Mithilfe dieses Programms lässt der Netzwerkverkehr mitschneiden. Cain & Abel legt dann eine Datei in der die Daten die abgefangen werden, gespeichert wird. Dabei fällt auf das sich auf dem Rechner von Herrn Wurstmann zahlreiche solche Mitschnitte aus dem Netzwerkverkehr befinden. Zwei dieser Mitschnitte enthalten dabei jeweils einen Token, in diesen Tokens befinden sich die Anmeldedaten von Herrn Riess-Pohlmann bei der Universität Erlangen. Dabei fällt auch auf das die Daten zur selben Zeit von Herrn Wurstmann empfangen wurden, als sie von Herrn Riess-Pohlmann abgeschickt werden. Im folgenden der Zeitliche Ablauf der die verschiedener Aktivitäten

die mit dem Tatvorwurf in Zusammenhang stehen, auf den Rechnern von Herrn Riess-Pohlmann als auch auf dem Rechner von Herrn Wurstmann in tabellarischer Form.

Systemzeit	Aktion
2019-11-28 16:36:05 CET	ca_setup.exe wurde auf dem PC von Herr Wurstmann gestartet. Dies ermöglicht die Installation des Programms Cain & Abel.  CA_SETUP_4.9.56.EXE /USERS/VAGRANT/DOWNLOADS 2019-11-28 16:36:05 CET
2019-11-28 16:42:17 CET	Cain.exe wurde von Herrn Wurstmann gestartet.  CAIN.EXE /PROGRAM FILES/CAIN 2019-11-28 16:42:17 CET
2019-11-29 10:09:02 CET	Der Installer des Tor Browsers wurde von Herr Wurstmann gestartet. Der Tor Browser erlaubt es die eigenen Aktivitäten im Internet zu verschleiern.  TORBROWSER-INSTALL-9.0.1_DE[1 2019-11-29 10:09:02 CET
2019-11-29 10:15:11 CET	Cain.exe wird erneut von Herr Wurstmann gestartet.  CAIN.EXE /PROGRAM FILES/CAIN 2019-11-29 10:15:11 CET
29.11.2019 10:22:58 - 10:23:08 CET	Aufenthalt von Herrn Riess-Pohlmann auf der Website der Uni Erlangen. Diese Verbindung wurde von Herr Wurstmann abgefangen. 5032-HTTPS-201911299238106-49523.txt- 5032-HTTPS-201911299238106-49528.txt
2019-11-29 09:24:22 CEST*	Erste Anmeldung von Herrn Riess-Pohlmann auf der Website seiner Universität. Er loggte sich auf seinem PC mit seinen Credentials ein. index.dat 1 https://faumail.uni-erlangen.de/?_task=login7ecfed9d 2019-11-29 09:24:22 CET Internet Explorer uni-erlangen.de
29.11.19 10:24:27 CET	Hier findet ein Login vom PC des Herrn Riess-Pohlmann auf der Website der Uni statt. Im Token befindet sich das Passwort von Herrn Riess-Pohlmann. Herr Wurstmann erlangt damit zum ersten mal Zugriff auf das Passwort. Der Zugriff auf das Passwort war vermutlich deshalb möglich da die Verbindung auf dem Rechner des Opfers auf HTTP gestellt wurde und damit nicht mehr eine Verschlüsselung verfügt. 5044-HTTPS-2019112992419579-49529.txt
2019-11-29 09:30:41 CEST*	Zweite Anmeldung von Herrn Riess-Pohlmann auf der Website seiner Universität. 1 https://faumail.uni-erlangen.de/?_task=login1d279dff 2019-11-29 09:30:41 CET Internet Explorer uni-erlangen.de
29.11.19 10:30:46 CET	Etwas später loggt sich Herr Riess-Pohlmann erneut bei der Website der Uni ein. Auch hier konnte das Passwort ausgelesen werden. 5046-HTTPS-2019112993038213-49533.txt

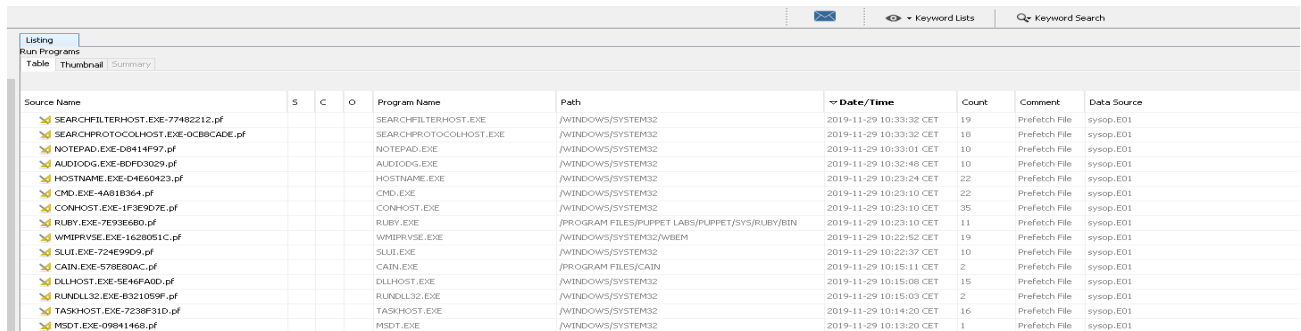
* Da Herr Riess-Pohlmann seine Uhr im Rechner nicht umgestellt hat, ist bei ihm noch die Mitteleuropäische Sommerzeit die Systemzeit. Diese liegt eine Stunde hinter der Winterzeit welche von Herrn Wurstmann verwendet wird.

Aufgrund des Tor-Browser auf dem Rechner von Herr Wurstmann, lässt sich damit nicht mehr nachvollziehen, was er in diesem gesucht oder aufgerufen hat.

6 Beweisführung Steuerbetrug

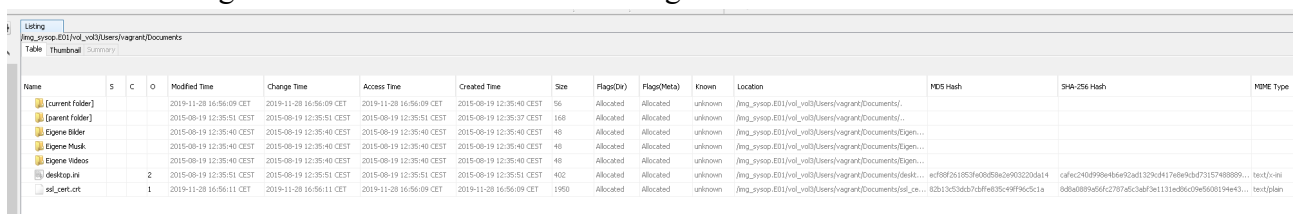
Aufgrund der Aussage von Herr Wurstmann sowie der damit verbundenen Zeugenaussage von Herr Riess-Pohlmann besteht der Verdacht das Herr Wurstmann Steuerbetrug begonnen hat.

Zunächst wurde auf dem Rechner überprüft welche Programme als letztes gestartet wurden. Anschließend wurde überprüft welche Programme auf dem Rechner installiert sind. Bei der Überprüfung dieser Programme ist aufgefallen das keine Programme vorhanden sind welche für die Veränderung oder Verwaltung von Steuern zuständig sind.



Source Name	S	C	O	Program Name	Path	Date/Time	Count	Comment	Data Source
SEARCHFILTERHOST.EXE-7748212.pf				SEARCHFILTERHOST.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:33:32 CET	19	Prefetch File	sysop.E01
SEARCHPROTOCOLHOST.EXE-0C89CADE.pf				SEARCHPROTOCOLHOST.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:33:32 CET	18	Prefetch File	sysop.E01
NOTEPAD.EXE-00414F97.pf				NOTEPAD.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:33:01 CET	10	Prefetch File	sysop.E01
AUDIODG.EXE-80FD3029.pf				AUDIODG.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:32:48 CET	10	Prefetch File	sysop.E01
HOSTNAME.EXE-04E60423.pf				HOSTNAME.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:23:24 CET	22	Prefetch File	sysop.E01
CMD.EXE-4AB1B364.pf				CMD.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:23:10 CET	22	Prefetch File	sysop.E01
CONHOST.EXE-1F3E907E.pf				CONHOST.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:23:10 CET	35	Prefetch File	sysop.E01
RUBY.EXE-7093660.pf				RUBY.EXE	\\PROGRAM FILES\\PUPPET LABS\\PUPPET\\SYS\\RUBY\\BIN	2019-11-29 10:23:10 CET	11	Prefetch File	sysop.E01
WMIPRVSE.EXE-1628051C.pf				WMIPRVSE.EXE	\\WINDOWS\\SYSTEM32\\WBEM	2019-11-29 10:22:52 CET	19	Prefetch File	sysop.E01
SLUI.EXE-724E9909.pf				SLUI.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:22:37 CET	10	Prefetch File	sysop.E01
CAIN.EXE-578E80AC.pf				CAIN.EXE	\\PROGRAM FILES\\CAIN	2019-11-29 10:15:11 CET	2	Prefetch File	sysop.E01
DLLHOST.EXE-5E46FA0D.pf				DLLHOST.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:15:08 CET	15	Prefetch File	sysop.E01
RUNDLL32.EXE-8321059F.pf				RUNDLL32.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:15:03 CET	2	Prefetch File	sysop.E01
TASKHOST.EXE-7238F31D.pf				TASKHOST.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:14:20 CET	16	Prefetch File	sysop.E01
MSDT.EXE-09841468.pf				MSDT.EXE	\\WINDOWS\\SYSTEM32	2019-11-29 10:13:20 CET	1	Prefetch File	sysop.E01

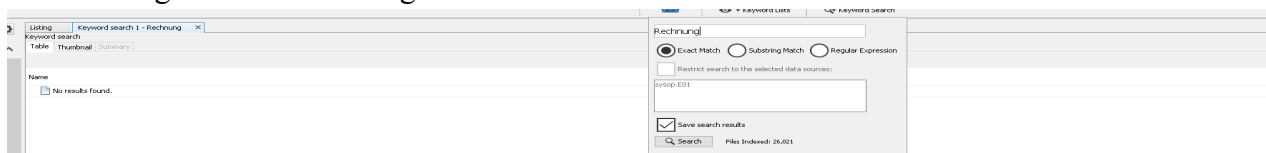
Anschließend wurden die Dokumente des Asservat01 überprüft. Es fanden sich dabei keine Dateien, die mit Rechnungen oder Steuern in Zusammenhang stehen.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(DI)	Flags(eta)	Known	Location	MD5 Hash	SHA-256 Hash	MD5 Type
[Current folder]				2019-11-29 16:56:09 CET	2019-11-29 16:56:09 CET	2019-11-29 16:56:09 CET	2019-09-19 12:35:40 CET	96	Allocated	Allocated	unknown	\\msysop.E01\\vol_v03\\users\\vagant\\Documents\\			
[Current folder]				2019-09-19 12:35:51 CET	2019-09-19 12:35:51 CET	2019-09-19 12:35:51 CET	2019-09-19 12:35:37 CET	168	Allocated	Allocated	unknown	\\msysop.E01\\vol_v03\\users\\vagant\\Documents\\			
Eigene Bilder				2019-09-19 12:35:40 CET	2019-09-19 12:35:40 CET	2019-09-19 12:35:40 CET	2019-09-19 12:35:40 CET	48	Allocated	Allocated	unknown	\\msysop.E01\\vol_v03\\users\\vagant\\Documents\\Eigen...			
Eigene Musik				2019-09-19 12:35:40 CET	2019-09-19 12:35:40 CET	2019-09-19 12:35:40 CET	2019-09-19 12:35:40 CET	48	Allocated	Allocated	unknown	\\msysop.E01\\vol_v03\\users\\vagant\\Documents\\Eigen...			
Eigene Videos				2019-09-19 12:35:40 CET	2019-09-19 12:35:40 CET	2019-09-19 12:35:40 CET	2019-09-19 12:35:40 CET	48	Allocated	Allocated	unknown	\\msysop.E01\\vol_v03\\users\\vagant\\Documents\\Eigen...			
desktop.ini		2		2019-09-19 12:35:51 CET	2019-09-19 12:35:51 CET	2019-09-19 12:35:51 CET	2019-09-19 12:35:51 CET	402	Allocated	Allocated	unknown	\\msysop.E01\\vol_v03\\users\\vagant\\Documents\\desktop...	edf88261953f0e0d58a2e03220da14	cafec240d998e6b692ad1329d417e6bdc73157488899...	text/plain
set_cant.txt		1		2019-11-29 16:56:11 CET	2019-11-29 16:56:11 CET	2019-11-29 16:56:09 CET	2019-11-29 16:56:09 CET	1950	Allocated	Allocated	unknown	\\msysop.E01\\vol_v03\\users\\vagant\\Documents\\set_c...	02b13c5366b7dbf6b35c49f965c1a	0d8a089a566f2787af5cab3e1131ed86c9e500194e43...	text/plain

Als nächstes wurden die gelöschten Daten ausgelesen, auch dort gab es keine relevanten Dateien, die im Zusammenhang mit Rechnungen oder Steuer stehen.

Anschließend wurde nach den Begriffen Rechnung, Steuer und Steuererklärung mit einer Keywordsearch gesucht. Wenn in einer Datei diese Begriffe auftauchen würde sie durch diese Methode gefunden werden. Der Keywordsearch konnte aber auch keine Dokumente finden die mit Steuerbetrug in Zusammenhang stehen.



Listing	Keyword search 1 - Rechnung
Keyword search	Rechnung
Table	Thumbnail Summary
Name	
No results found.	

Damit gibt es keine Forensischen Beweise, die den Verdacht gegen Herr Wurstmann in Bezug auf Steuerbetrug stützen.

7 Zusammenfassung

Auf dem Rechner von Herr Wurstmann befinden sich keine Dateien die den Verdacht des Steuerbetrugs stützen. Auch verfügt Herr Wurstmann nicht über die Software die für ein solches Verbrechen benötigt werden würde.

Für den Verdacht auf Ausspähen von Daten innerhalb des Firmennetzwerks gibt es aber Aktivitäten die einen Verdacht gegen Herr Wurstmann stützten würden. Er ist im Besitz der Software die für einen derartigen Angriff nötig wäre. Explizit handelt es sich dabei um Cain & Abel, sowie Wireshark. Herr Wurstmann hat außerdem einen Anmeldeversuch von Herr Riess-Pohlmann abgefangen. Dieser hat versucht sich auf der Webmail seiner Hochschule anzumelden. Herr

Wurstmann ist dabei in Besitz eines Tokens gekommen der den Username und das Passwort von Herr Riess-Pohlmann enthält. Um dies zu erreichen wurde vermutlich der Netzwerkverkehr von HTTPS auf HTTP umgestellt.

8 Fazit

Herr Wurstmann hat die Technischen Voraussetzungen für das Ausspähen von Daten im Firmennetzwerk getroffen. Er hat Programme heruntergeladen und installiert die eigentlich nur für einen Angriff dieser Art benötigt werden. Er hat außerdem den Tor-Browser heruntergeladen und installiert vermutlich um seine Aktivitäten zu verschleiern. Die Tatsache das er das Programme Cain & Abel gestartet hat und dieses Programm dann das Netzwerk ausgespäht hat. Es ist auch unwahrscheinlich das dies ohne das Wissen von Herr Wurstmann passiert ist. Cain & Abel wurden nicht zufällig gestartet. Er hat es zwei mal gestartet. Herr Wurstmann ist außerdem im Besitz eines Tokens, welcher die Anmeldedaten von Herr Riess-Pohlmann enthält. Dieses Token erlangte er durch den Einsatz von Cain & Abel. Damit stimmen vermutlich die Vorwürfe gegen Herr Wurstmann und damit ist die Firma Y-Ways Technologies wahrscheinlich geschädigt. In Bezug auf den Verdacht des Steuerbetrugs lässt sich sagen das Herr Wurstmann weder die Software noch irgendwelche Dokumente besitzt die im Zusammenhang mit der Steuer oder mit Rechnungen stehen. Damit ist ein Steuerbetrug unwahrscheinlich.

9 Quellenverzeichnis

<https://de.wikipedia.org/wiki/ARP-Spoofing> [28.06.2022]

https://www.wz.de/digital/ssl-zertifikate-so-erkennen-sie-eine-phishing-seite_aid-25596245
[29.06.2022]

<https://www.heise.de/> [29.06.2022]

Die Ermittler Dean Basic und Moritz Rupp versichern hiermit das sie unparteiisch und ehrlich Aussagen. Alle in diesem Dokument genannten Punkte entsprechen der Wahrheit nach bestem Wissen und Gewissen.

Dean Basic

Dean Basic

Moritz Rupp

Moritz Rupp