Klaut-Tracing - Welche Spuren Kriminelle bei Ihren Recherchen im Netz hinterlassen

Hausarbeit zum Thema 'Internetrecherchen vor Begehung von Delikten'
BCSM 505 WS2023/24

vorgelegt von
Stephan Reugels
Alexander Hanke

Prof. Dr. Marcus Niemietz
Dr. Gael Pentang
Cyber Security Management
Clavis - Institut für Informationssicherheit

Entstanden an der

Zusammenfassung

In einer zunehmend digitalisierten Welt gewinnt das Thema Cyberkriminalität stetig an Bedeutung. Insbesondere die Informationsgewinnung von Tätern im Vorfeld von Straftaten nimmt eine herausragende Rolle ein, da sich Kriminelle vermehrt im Internet bewegen, um Informationen für ihre Tatvorbereitungen zu sammeln. Ein prominentes Beispiel hierfür ist die Recherche von Tätern im Rahmen von geplanten Straftaten, wie beispielsweise Einbrüchen oder Überfällen, bei denen sie auf verschiedene Informationen, wie zum Beispiel Luftbilder und Kartenmaterial angewiesen sind.

Diese Hausarbeit widmet sich der Analyse von Datenspuren, die Täter bei ihren Recherchen im Internet hinterlassen. Ein spezieller Fokus liegt dabei auf den Methoden, Straftäter bereits kurz nach Begehen der Tat durch intelligente Kombination von digitalen Spuren zu identifizieren. Dabei werden verschiedene Aspekte beleuchtet, wie beispielsweise die Nutzung von Online-Diensten (Google, Google Maps etc.), sozialen Netzwerken (Meta, LinkedIn) aber auch Analysen auf Basis von gespeicherten Providerdaten und Logs.

Ein zentraler Ansatzpunkt dieser Arbeit ist die Aggregierung und Auswertung dieser Datenspuren mithilfe von Analysetools, darunter auch populäre Werkzeuge wie Google Analytics. Die Untersuchung dieser Werkzeuge ermöglicht nicht nur einen Einblick in die digitalen Aktivitäten der Täter, sondern eröffnet auch die Möglichkeit, präventive Maßnahmen zur Verhinderung von Straftaten zu entwickeln.

Der gewählte Rahmen dieses Moduls, ein Hackathon, bietet eine ideale Plattform für die praktische Umsetzung und Entwicklung von innovativen Lösungen. Studierende haben hier die Gelegenheit, ihre Fähigkeiten im Bereich der Cybersecurity und forensischen Datenanalyse zu vertiefen. Durch die Bearbeitung realer Anwendungsfälle können sie nicht nur theoretisches Wissen erwerben, sondern auch konkrete Lösungsansätze entwickeln, die in der Praxis Anwendung finden können. Dieses Hausarbeit stellt die Abschlussarbeit des Moduls dar.

Diese Hausarbeit zielt darauf ab, ein tieferes Verständnis für die Vorgehensweisen von Straftätern im digitalen Raum zu schaffen, die Bedeutung von Datenspuren zu betonen und innovative Ansätze zur Analyse und Prävention von kriminellen Handlungen zu entwickeln. Durch die Verbindung von theoretischem Wissen und praktischer Anwendung im Rahmen eines Hackathons hoffen wir dazu beitragen zu können, die digitale Sicherheit mittels aktueller Methoden zu stärken und einen Beitrag zur Kriminalprävention im digitalen Zeitalter zu leisten.

Inhaltsverzeichnis

1 Einführung

Diese Hausarbeit im Modul 'Hackathon' befasst sich mit Internetrecherchen von Straftätern vor der Begehung von Delikten.

1.1 Szenario

Folgendes Szenario ist gegeben:

Täter recherchieren im Rahmen der Tatvorbereitung verschiedene Dinge im Zusammenhang mit der von ihnen geplanten Tat im Internet (Luftbilder vom Tatort zur Planung der Fluchtwege, Offnungszeiten von Geschaften, Bilder der Opfer etc.). Die Datenspuren dieser Suchen sind im Netz zum Teil frei verfügbar und konnten mit Auswertetools ausgewertet werden (bspw. Google Analytics).[8]

1.2 Fragestellung

Im Rahmen der Arbeit sollen insbesondere drei Fragen konkret beantwortet werden. [8]

1. Besteht eine Moglichkeit, über frei verfugbare Tools eine Internet-Auswertung diesbezuglich zu machen, um Täterspuren zu erkennen?
2. Konnen neben Google noch andere Quellen / Erfassungssysteme möglicherweise in Kombination in die Recherche einbezogen werden?
3. Kann der Rechercheprozess so optimiert werden, dass zeitnah nach einem herausragenden Tatgeschehen Ermittlungsansatze eines noch unbekannten Taters erarbeitet werden konnen (etwa IP-Adressen)?

1.3 Vorgehensweise

Bei der Erstellung dieser Arbeit haben sich die Autoren auf ein dreistufiges Vorgehen zur bestmöglichen Betrachtung, sowohl der Täterperspektive, als auch der Perspektive der Strafverfolger geeinigt.

1. Ermittlung von Informationsquellen (Perspektive Straftäter):
    - Identifikation relevanter digitaler Plattformen (soziale Medien, Foren, Chaträume, etc.), auf denen Straftäter aktiv sein könnten.
    - Erkundung öffentlich zugänglicher Datenbanken und Berichte von Strafverfolgungsbehörden.
    - Analyse von Studien und Forschungsliteratur zum Thema Verhaltensmuster von Straftätern im digitalen Raum.
2. Methoden der Überwachung der Quellen
    - Überwachung von Datenverkehr an wichtigen Knotenpunkten
    - Auswahl eines Monitoring-Systems für ausgewählte digitale Plattformen zur kontinuierlichen Beobachtung.
    - Einsatz von Software zur Datenanalyse und zum Erkennen von Mustern, die auf potenzielle Straftaten hinweisen könnten.
    - Zusammenarbeit mit Behörden und Plattformbetreibern zur Gewährleistung rechtlicher Konformität.
3. Erfassung/Auswertung der Daten einer Simulation:
    - Sammlung und Organisation der gewonnenen Daten in einer strukturierten Form (z.B. Datenbanken).
    - Anwendung qualitativer und quantitativer Analysemethoden zur Mustererkennung und Verhaltensanalyse.

2 Informationsquellen

2.1 Suchmaschinen

Ein Straftäter könnte Suchmaschinen zur Informationsbeschaffung vor der Begehung seiner Tat nutzen. Beispielsweise könnte er online nach Informationen über Orte, Personen oder Unternehmen suchen, die er ins Visier nehmen möchte. Dabei könnten Details über Sicherheitssysteme, Öffnungs- und Schließzeiten von Einrichtungen oder persönliche Informationen über potenzielle Opfer gesammelt werden, um einen effektiveren Angriffs- oder Raubplan zu entwickeln. Darüber hinaus können Suchmaschinen genutzt werden, um Anleitungen oder Methoden zu finden, wie man bestimmte Straftaten begeht, wie das Erlernen des Knackens von Schlössern, das Umgehen von Sicherheitssystemen, das Hacken von Computern oder sogar das Herstellen illegaler Substanzen. Durch den Zugriff auf solche Informationen kann ein Straftäter seine Fähigkeiten verbessern oder neue Methoden für kriminelle Aktivitäten erlernen.

Ein weiterer Aspekt ist die Beschaffung von Werkzeugen und Materialien, die für die Begehung einer Straftat benötigt werden. Ein Straftäter könnte Informationen darüber suchen, wo und wie er bestimmte Werkzeuge, Waffen oder Materialien erwerben kann, was den Kauf von Einbruchswerkzeugen, Waffen, gefälschten Ausweisen oder anderen hilfreichen Gegenständen einschließen könnte. Zudem könnten Straftäter Suchmaschinen nutzen, um zu recherchieren, wie Strafverfolgungsbehörden arbeiten und welche Gesetze in ihrem Bereich gelten. Dieses Wissen könnte genutzt werden, um Risiken zu minimieren, die Wahrscheinlichkeit einer Festnahme zu verringern und Strategien zu entwickeln, um einer Verfolgung zu entgehen. Insgesamt nutzen Straftäter die weitreichenden Informationen, die durch Suchmaschinen zugänglich sind, um ihre kriminellen Absichten zu unterstützen und die Erfolgschancen ihrer geplanten Taten zu erhöhen.

In einem Bericht von Deutschlandfunk Nova werden konkrete Fälle erwähnt, in denen Straftäter digitale Spuren hinterlassen haben, die von Ermittlern genutzt wurden, um sie aufzuspüren. Beispielsweise hat ein Mann aus Regensburg nach dem perfekten Mord und der tödlichen Dosis eines Beruhigungsmittels gesucht, bevor seine Verlobte unvermittelt starb. Ein anderer Mann recherchierte im Netz zu tödlichen Stichverletzungen, kurz bevor eine Person, mit der er sich per SMS verabredet hatte, Opfer eines Angriffs wurde. In einem weiteren Fall suchte eine Frau im Netz nach "Tote Rentnerin Wohnung Hamburg"wenige Stunden nach der Tat. Diese digitalen

Spuren halfen den Ermittlern, Zusammenhänge herzustellen und Indizien gegen die Verdächtigen zu sammeln. [10]

Das Bundeskriminalamt (BKA) unterstreicht die Bedeutung von Suchmaschinen und stellt allgemein fest, dass das Internet und die Sozialen Medien neue Handlungsfelder und Tatbegehungsweisen für Kriminelle geschaffen haben. Um Straftaten im Internet wirksam bekämpfen zu können, sei es für die Sicherheitsbehörden wichtig, ein klares Bild der Lage, der Täterstrukturen und der Tatbegehungsweisen zu haben. [4]

2.2 Social Media

Straftäter nutzen Soziale Netzwerke auf verschiedene Weise, um Informationen vor der Begehung einer Straftat zu sammeln. Insbesondere können diese Plattformen als reiche Informationsquellen über potenzielle Opfer dienen. Durch das Durchsuchen von Profilen ist es möglich, persönliche Informationen wie Wohnort, Arbeitsplatz, tägliche Routinen und sogar Urlaubspläne zu erfahren. Solche Details können bei Einbrüchen, Stalking oder Identitätsdiebstahl ausgenutzt werden.

Darüber hinaus ermöglichen soziale Netzwerke die Beobachtung und Analyse des Verhaltens und der Gewohnheiten von Zielpersonen. Zum Beispiel können regelmäßige Posts über bestimmte Aktivitäten oder Orte Muster offenbaren, die ein Straftäter für einen Überfall oder eine andere Form von Verbrechen nutzen könnte.

Ein weiterer Aspekt ist die Bildung von Netzwerken und Kontakten zu anderen Kriminellen oder die Rekrutierung von Komplizen über soziale Medien. Plattformen wie Facebook, X (ehem. Twitter) oder spezialisierte Foren können zur Koordination von Aktivitäten oder zum Austausch von Tipps und Tricks unter Kriminellen dienen.

Bei besonders ausgeklügelt, mehrschichtigen Straftaten können Social Media Plattformen für die Durchführung von Cybercrimes genutzt werden, wie zum Beispiel Phishing-Angriffe, bei denen Täter sich als vertrauenswürdige Quellen ausgeben, um an sensible Informationen wie Passwörter oder Kreditkartendaten zu gelangen, welche dann für die eigentliche Tat genutzt werden. [7]

2.3 Webseiten

Insbesondere für Unternehmen oder öffentliche Einrichtungen als Ziele von Straftaten stellen Firmenwebseiten oder im Netz zu findende Services eine weitere Informationsquelle dar, da diese häufig detaillierte Informationen über Mitarbeiter, Standorte und verwendete Technologien bereitstellen. Über Schwachstellen-Scans könnten des

Weiteren Sicherheitslücken in Webapplikationen ausgenutzt werden, um sensible Informationen für die bessere Verschleierung von Straftaten oder für eine höhere Effektivität bei deren Durchführung zu erlangen.

2.4 Darknet

Das Darknet beinhaltet nicht nur eine Fülle an Daten aus Daten-Leaks, sondern auch 'Erfahrungsberichte' anderer Straftäter, die bei der Vorbereitung hilfreich sein können. Bei unserer Recherche fanden wir zudem Anbieter, die sich explizit auf die Informationsbeschaffung und Auskundschaftung von potentiellen Opfern gegen Zahlungen spezialisiert haben. [1]

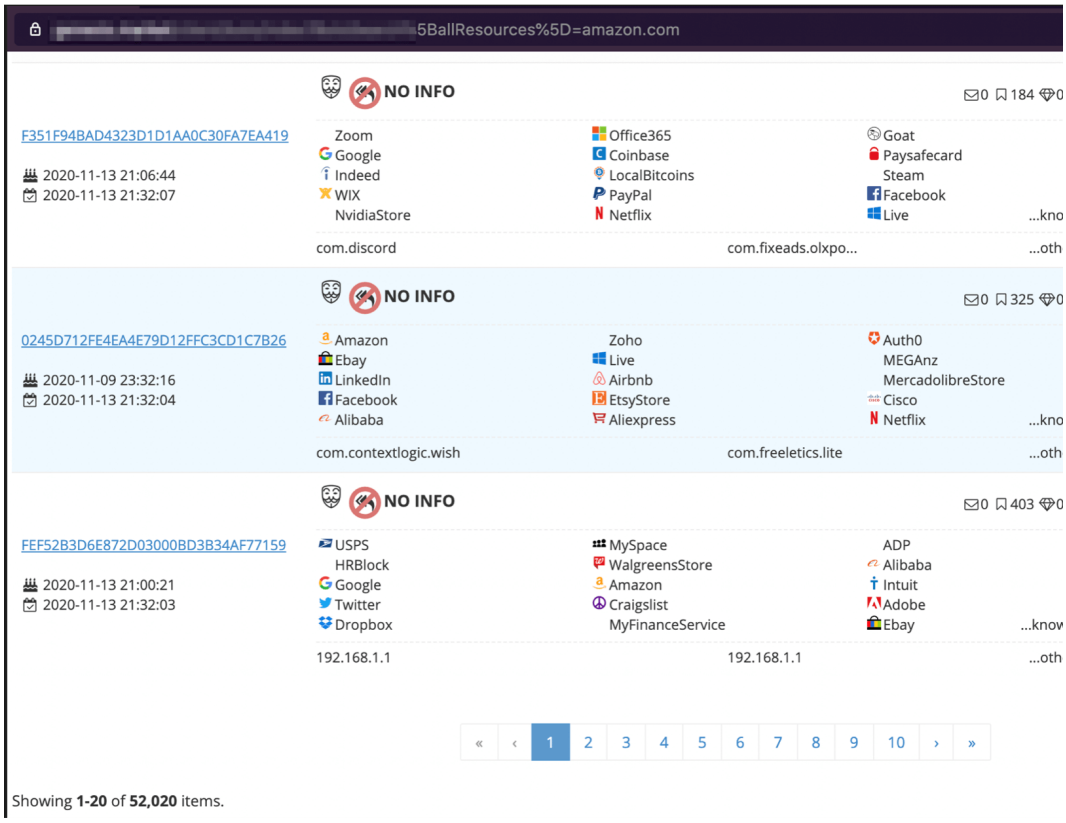

Abbildung 2.1: Datensätze auf einem Darknet-Marktplatz[1]

3 Methoden

Nun wechseln wir die Seiten und begeben uns auf die Seite der Strafverfolger. Im Folgenden beleuchten wir die technischen Methoden und bewerten jene auf einer dreistufigen Skala anhand der Umsetzbarkeit gemäß aktueller Gesetze.

- Grün Legal im Rahmen der Ermittlungsarbeiten
- Gelb Legal nur mit richterlichem Beschluss
- Rot Illegal und daher gerichtlich nicht verwertbar

3.1 Allgemeines Vorgehen

1. Ermittlungsanforderung: Die Strafverfolgungsbehörden stellen eine formelle Anfrage bei Suchmaschinenbetreibern oder Internetdienstanbietern, um Zugang zu spezifischen Benutzerdaten zu erhalten. Dies kann Suchhistorien, IP-Adressen und andere digitale Spuren umfassen.
2. Gerichtliche Anordnung: Für den Zugriff auf solche Daten ist in der Regel eine gerichtliche Anordnung notwendig, die die Rechtmäßigkeit der Datenerhebung sicherstellt.
3. Datenauswertung: Nach Erhalt der Daten führen forensische Analysten eine detaillierte Auswertung durch. Sie analysieren Suchbegriffe, Datum und Uhrzeit der Suchanfragen sowie die verwendeten Geräte.
4. Korrelation mit anderen Daten: Die Suchdaten können mit anderen verfügbaren Informationen (wie Überwachungskameras, Zeugenaussagen, Finanztransaktionen) abgeglichen werden, um ein umfassenderes Bild der Aktivitäten des Verdächtigen zu erhalten.

3.2 Internet Exchanges (IXPs)

Bedingt erlaubt

Der überwiegende Teil des weltweiten Internet-Datenverkehrs findet an Internet-Knotenpunkten (IXP) statt. [5]. IXPs sind daher ein lohnenswertes Ziel für die

zentrale Überwachung von Internet-Traffic und wurden hierfür gem. Berichten mancher Whistleblower (Snowden o.ä.) von führenden, internationalen Geheimdiensten auch genutzt. Mit fortschreitender Verbreitung von Verschlüsselung, Anonymisierung etc. und exponentiell wachsender Datenmenge verlieren Überwachungen an IXP jedoch mutmaßlich an Bedeutung. Konkrete Nachweise oder Studien konnten von uns hierzu nicht gefunden werden. Die Anlassbezogene Überwachung von Internetverkehr ist weiterhin denkbar, spielt für unsere Thematik der Informationsermittlung vor Begehung der Straftat jedoch nur eine untergeordnete Rolle, da in den meisten Fällen zu diesem Zeitpunkt der Täter noch nicht bekannt ist. Die technische Umsetzung solcher Maßnahmen erfolgt zum Beispiel über dedizierte Hardware (Network Packet Broker) welche Datenverkehr auf physikalischer Ebene kopieren und dann zu einem Aufzeichnungssystem (z.B. n2disk, ntop) leiten. Die hierfür führende Software n2disk erreicht Aufzeichnungsraten von über 10 Gbit/s auf Standardhardware. [2]

Nicht erlaubt

Die anlasslose und flächendeckende Vorratsdatenspeicherung wurde vom Bundesverwaltungsgericht in Deutschland als europarechtswidrig eingestuft. Diese Regelung darf nicht mehr angewendet werden. Das Gericht ist damit einer Entscheidung des Europäischen Gerichtshofs (EuGH) aus dem Jahr 2022 gefolgt, die besagt, dass die Kommunikationsdaten aller Bürgerinnen und Bürger nicht ohne Anlass gespeichert werden dürfen. Allerdings ist eine gezielte und zeitlich begrenzte Speicherung der Daten bei einer ernsten Bedrohung für die nationale Sicherheit oder zur Bekämpfung schwerer Kriminalität unter bestimmten Umständen möglich. [9]

3.3 Internet Service Provider (ISPs)

Erlaubt

Internet Service Providers (ISPs) spielen eine entscheidende Rolle bei der Bereitstellung von Internetzugang für Kunden. Ursprünglich in den 1980er Jahren entstanden, als Unternehmen wie CompuServe, Prodigy und America Online begannen, eingeschränkte Internetzugangsdienste wie E-Mail-Austausch anzubieten, haben sich ISPs zu den Hauptanbietern von Internetzugang entwickelt. ISPs nutzen eine Vielzahl von Technologien, um Benutzer mit ihrem Netzwerk zu verbinden. Dazu gehören traditionelle Optionen wie Kupferdrähte für Dial-up- und DSL-Anschlüsse, Kabelmodems, Wi-Fi und Glasfaser. Für anspruchsvollere Kundenanforderungen, wie mittlere bis große Unternehmen oder andere ISPs, können höhergeschwindigkeits-DSL, Ethernet, Gigabit Ethernet und andere fortgeschrittene Technologien eingesetzt werden. Die Hauptaufgabe eines ISPs besteht darin, eine Verbindung zum Internet bereitzustellen. Sie verwalten die technischen Aspekte wie das Routing von Daten und das Management von Servern, sodass die Kunden sich nicht um diese Details kümmern müssen.

ISPs sind für Strafverfolger enorm hilfreich, da sie als einziges Bindeglied Datenverkehr konkreten Anschlüssen und somit auch echten Personen zuordnen können (sofern kein VPN oder TOR verwendet wird). Des Weiteren bieten ISPs oft Hilfsdienste an, welche genaue Rückschlüsse auf das Verhalten einer Person im Netz zulassen (vgl. Simulation-> DNS Server) [3]

Die Nutzung von Daten, welche durch ISPs erhoben werden ist in vielen Fällen auch ohne richterlichen Beschluss im Rahmen eines Ermittlungsverfahrens möglich und stellt eine Standardmethode in der Strafermittlung dar. Auf Grund der hohen Datenmenge und fehlendem Personal greifen Behördern hierauf nur bei gewichtigen Straftaten oder zur Aufklärung von Straftaten, die keine anderen, erfolgsversprechenden Beweise/Spuren zulassen (Cyberkriminalität) zurück, wie bereits 2020 der Bund deutscher Kriminalbeamte in einem Interview mitteilte. [6]

3.4 Drittanbieter (CDN, Hoster, MSP)

Erlaubt

Während zu Beginn des Internets Inhalte noch von seinen Nutzern selbst bereitgestellt ('gehostet') wurden übernehmen spezialisierte Dienstleister diese Rolle zunehmend. Content Delivery Networks (CDN) wie Akamai und Cloudflare stellen Inhalte durch ein verteiltes Netz an Speicherknoten möglichst nah am Edge (Anschluss des Kunden) bereit und ermöglichen somit eine möglichst niedrige Latenz und hohe Bandbreite. Entsprechend liegen bei jenen Anbietern auch höchstwahrscheinlich Protokolle zum Datenabruf in Form von Analytics oder Logs vor. Ob diese Daten durch Strafverfolger angefragt werden können ist öffentlich nicht bekannt. Hoster von z.B. Webseiten halten in den Meisten Fällen Zugriffslogs des Webservers vor. Meist sitzen diese Anbieter im Gegensatz zu großen CDNs in Deutschland und unterliegen somit auch dem Zugriff von Strafverfolgungsbehörden. Nicht selten werden daher bei Hostern Auskunftersuche der Polizei oder Staatsanwaltschaft eingeholt. Ein Beispiel ist im Anhang beigefügt. Gemäß geltendem Recht sind Hoster in Deutschland zur Kooperation verpflichtet, sofern sie sich nicht selbst dadurch strafbar machen. Im Zweifel kann durch richterlichen Beschluss die Erlaubnis zur Freigabe von sensiblen Daten erzwungen werden. Gleiches gilt für Managed Service Provider, die im unternehmerischen Kontext als externe IT-Abteilung Daten verwalten und Administrationsarbeiten durchführen. Hier können ebenfalls Daten in Form von Logs entweder des Täters innerhalb des betreuten Unternehmens (MSP Kunde als Täter) oder durch Zugriff auf Dienste und Webseiten des Ziels (MSP Kunde als Opfer) erhoben werden.

3.5 Extern: Suchmaschinen

Bedingt erlaubt

Die Rekonstruktion von Suchanfragen von Kriminellen vor Straftaten erfolgt typischerweise in enger Zusammenarbeit mit dem Suchmaschinenanbieter (z.B. Google, Microsoft, Yahoo). Anhand von eingrenzenden Metadaten können von Strafverfolgungsbehörden Datenpakete angefragt werden, welche zum Beispiel einen bestimmten Firmennamen (des Opfers) oder eine Adresse enthalten. Auch Suchen nach bestimmten Waffentypen, Beschaffung etc. können ausgewertet werden.

Ohne konkrete Anfrage bieten Google Analytics und Google Search Console ein grobes Bild der Suchanfragen und können in der Recherche von Straftätern wertvolle Hinweise liefern, indem dort gesammelte Daten über Website-Besucher abgerufen werden können, welche jedoch stark anonymisiert sind. Dies umfasst Informationen wie geografische Standorte, verwendete Geräte, Betriebssysteme, Browser, Verweildauer auf der Website, besuchte Seiten und die Herkunft des Traffics. Diese Daten können Muster und Verhaltensweisen aufzeigen, die für Ermittlungen relevant sein könnten. Beispielsweise könnte die Analyse der Herkunft des Traffics helfen, die geografische Region zu identifizieren, aus der ein Verdächtiger möglicherweise operiert.

3.6 Extern: Social Media

Bedingt erlaubt

Für Social Media Plattformen gilt gleiches Vorgehen wie bei Suchmaschinen, sowie anderen Dienstleistern. Verwertbare und beweissicher zuzuordnende Informationen erhalten Strafverfolger nur über Auskunftsersuchen. Bei großen Plattformen geht dies jedoch in der Regel sehr schnell, da es auf Grund der Menge der Ersuchen standardisierte Prozesse gibt.

3.7 Tools

Es gibt verschiedene frei verfügbare Tools, die für die Nachverfolgung von Täterspuren im Internet genutzt werden können. Zu diesen Tools gehören:

1. Wireshark: Ein Netzwerkanalysetool, das Datenverkehr aufzeichnen und detailliert analysieren kann.
2. Maltego: Ein Tool für Open-Source-Intelligence (OSINT) und forensische Untersuchungen, das hilft, Beziehungen und Verbindungen zwischen Personen, Gruppen und verschiedenen Internetstrukturen aufzudecken.

3. TheHarvester: Ein Tool zur Sammlung von E-Mail-Adressen, Subdomains, Hosts, Mitarbeiter-Namen und offenen Ports von verschiedenen öffentlichen Quellen.
4. Shodan: Eine Suchmaschine, die speziell für das Auffinden von an das Internet angeschlossenen Geräten und Diensten entwickelt wurde.
5. Google Analytics: Details über Suchanfragen und Verhalten von Nutzern auf Webseiten.

4 Simulation / Praxis

4.1 Kurzüberblick gesammelte Daten

Zur praktischen Einordnung wurde von uns im Rahmen dieser Hausarbeit die Recherche eines Straftäters auf den OLMS-Verlag simuliert. Auf Grund des beschränkten Umfanges der Hausarbeit haben wir uns bei der Simulation auf Methode 3.3 und 3.4 konzentriert.

Hierzu wurde von uns ein Testszenario mit Netz des Straftäters (ISP-Gateway, DNS-Server) und Netz des Opfers (Firewall, Webserver) aufgesetzt. Der Webserver stand hierbei im öffentlichen Netz.

Über einen Zeitraum von 1 Tag wurde die Domain des Verlags 1144 Mal aufgerufen. Durch filtern der IP-Adressen in den Weblogs unter Ausschluss von bekannten Bots, ausländischen IPs und anderer Crawler konnten wir 12 IP Adressen isolieren. Ein Abgleich mit einer Geo-IP Datenbank ergab nur eine IP im vermuteten Täterumfeld.

Time	Src hostname	Src port	Dest hostname	Dest port	Query type	Query
[redacted] 5:04 PM	5.199.1[redacted]	62287	62.159.[redacted]	53	AAAA	www.olms-pferdebuch.de
4:49 PM	5.199.1[redacted]	60635	62.159.[redacted]	53	A	www.olms-pferdebuch.de
4:46 PM	5.199.1[redacted]	61218	62.159.[redacted]	53	AAAA	www.olms-pferdebuch.de
4:28 PM	5.199.1[redacted]	60943	62.159.[redacted]	53	AAAA	www.olms-pferdebuch.de
4:10 PM	5.199.1[redacted]	60584	62.159.[redacted]	53	AAAA	www.olms-pferdebuch.de
3:52 PM	5.199.1[redacted]	60473	62.159.[redacted]	53	AAAA	www.olms-pferdebuch.de
3:46 PM	5.199.1[redacted]	62519	62.159.[redacted]	53	A	www.olms-pferdebuch.de
3:34 PM	5.199.1[redacted]	60796	62.159.[redacted]	53	AAAA	www.olms-pferdebuch.de
3:16 PM	5.199.1[redacted]	61742	ns01.m[redacted]	53	AAAA	www.olms-pferdebuch.de
2:58 PM	5.199.1[redacted]	61014	ns01.m[redacted]	53	AAAA	www.olms-pferdebuch.de
2:43 PM	5.199.1[redacted]	61621	ns01.m[redacted]	53	A	www.olms-pferdebuch.de

Abbildung 4.1: DNS-Abfragen der Domain[1]

Im DNS-Server des simulierten ISP Netzes konnte der Aufruf der Webseite (DNS Query) mit Zeitstempel ebenfalls nachgewiesen werden (Abb. 4.1).

Zur besseren Übersicht haben wir alle erfassten IP-Adressen auf einer Karte dargestellt. Auffällig ist die Bündelung in die USA (links außerhalb des Bildes). Hier sitzen mit Microsoft (Bing) und Google (Search) die meisten Crawler.

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)
5.199.129.120	DE	Düsseldorf, North Rhine-Westphalia, Germany, Europe	5.199.128.0/23	40472	51.2705, 6.8144	20

Abbildung 4.2: Geo-IP Lookup des Täters[2]

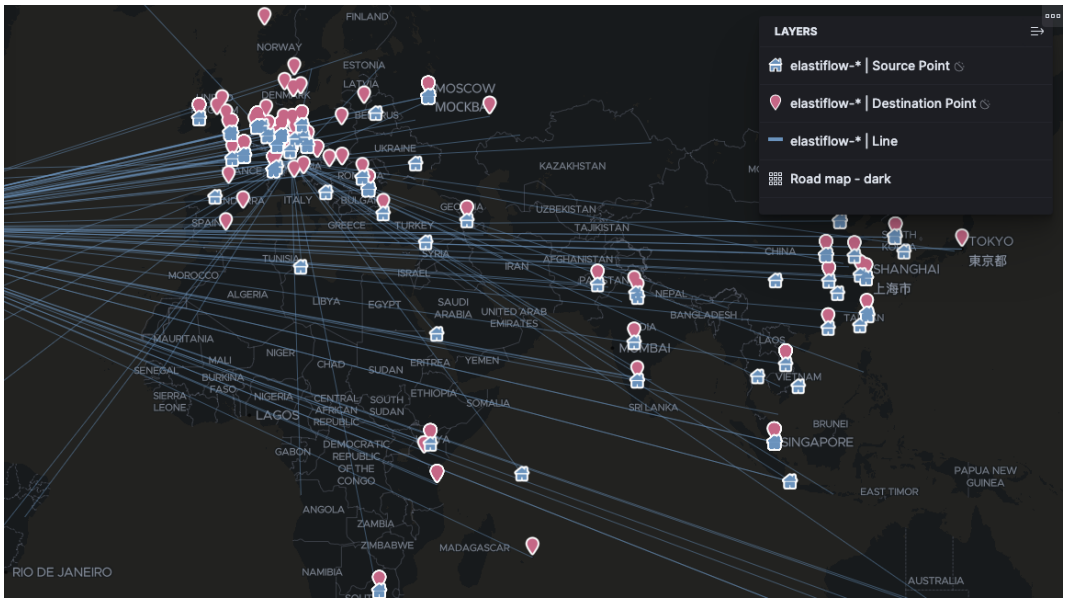

Abbildung 4.3: Zugriffe auf Karte[3]

4.2 Ableitungen / Weiterführung

Aus der Simulation folgern wir folgende 3 Kernaussagen

1. Je unbekannter das Opfer, desto eindeutiger die mögliche Zuordnung auf Grund geringerer Datenmenge.
2. Je bekannter das Opfer, desto signifikant größer die zu analysierende Datenmenge
3. Geo-IP Lookups und Logmanagement sind unverzichtbare Quellen

Mit den aus dieser Analyse gewonnenen Daten können nun weitere Datenquellen einfacher und genauer durchsucht werden. Im Verlauf der Simulation hatten wir die Idee jedem gewonnenen Datentyp einen Qualitäts-/Bedeutsamkeitsindex zuzuordnen. Eindeutige Merkmale erhalten den höchsten Index (1), nur schwer einzugrenzende Merkmale den niedrigsten (9). Möglichen Daten haben wir im Folgenden Indizes exemplarisch zugeordnet.

- IPv4-Adresse (3)
- IPv6-Adresse (2)
- Anschrift (1)
- Name (1)
- IMEI/MAC des Gerätes (1)
- Geo-IP Radius (5)
- Herkunftsland (9)
- Verwendeter ISP (7)

Anmerkung: Durch den zunehmenden Wechsel auf IPv6 wird die Verfolgung signifikant vereinfacht, da IPv6 Adressen mit einer Eindeutigkeit von

$$E = 2^{128} \tag{4.1}$$

in der Praxis Nutzern fest bis zum Endgerät zugewiesen werden, IPv4 Adressen mit einer Eindeutigkeit von

$$E = 2^{32} \tag{4.2}$$

jedoch durch NAT etc. eingespart werden müssen und somit nicht auf eine Person oder ein Gerät, sondern nur auf einen Anschluss und auch nur für 24h zugeordnet werden können.

5 Fazit

5.1 Herausforderungen / Lösungen

Die jährlich zunehmende Menge an Daten und deren Einfluss auf die Strafverfolgung, insbesondere bei der Ermittlung von Rechercheversuchen mutmaßlicher Täter vor Straftaten ist ein komplexes und kontroverses Thema. Einerseits ermöglicht der Zugriff auf große Datenmengen der ISPs, CDNs, Hoster etc., die durch moderne Technologien gesammelt wird, eine präzisere und effektivere Ermittlungsarbeit. Andererseits führt diese Datenflut auch zu Herausforderungen und Bedenken, insbesondere in Bezug auf Datenschutz und die Effizienz der Strafverfolgungsbehörden.

Zunächst ermöglicht die Analyse großer Datenmengen, sogenanntes "Big Data", den Strafverfolgungsbehörden, Muster und Verbindungen zu erkennen, die bei traditionellen Ermittlungsmethoden möglicherweise übersehen werden. Dies kann zu einer präziseren Identifizierung von Verdächtigen, zur Aufdeckung komplexer Zusammenhänge und Mittäterschaften und sogar zur Vorhersage krimineller Aktivitäten führen. Beispielsweise können durch die Analyse von Standortdaten, Kommunikationsmustern und Online-Verhalten wertvolle Hinweise gewonnen werden, die zur Aufklärung von Verbrechen beitragen. Die konkrete Suche nach gewissen Waffen könnte bei präventiver Datenanalyse bei ISPs schon Ermittlungen vor der tatsächlichen Tat ermöglichen

Auf der anderen Seite stellt die Menge an verfügbaren Daten die Strafverfolgungsbehörden vor erhebliche Herausforderungen. Die Notwendigkeit, riesige Datenmengen effizient zu verarbeiten und relevante Informationen zu extrahieren, erfordert erhebliche Ressourcen und fortschrittliche technologische Werkzeuge. Zudem kann die Masse an Daten zu einer Informationsüberflutung führen, die die Ermittlungen verlangsamt und die Gefahr von Fehlinterpretationen erhöht.

Ein weiterer wichtiger Aspekt ist der Datenschutz. Die Sammlung und Analyse von Daten durch Strafverfolgungsbehörden wirft Fragen hinsichtlich der Privatsphäre der Bürger auf. Die Sorge besteht, dass der Einsatz von Big Data-Technologien zu einer übermäßigen Überwachung und zum Eindringen in die Privatsphäre unschuldiger Personen führen kann. Es entsteht ein Spannungsfeld zwischen der Notwendigkeit, Verbrechen effektiv zu bekämpfen, und dem Recht der Bürger auf Datenschutz. Nicht zuletzt in den letzten Jahren haben höchste Gerichte die Legalität von sog. Vorratsdatenspeicherung ernsthaft in Frage gestellt.

Zusammenfassend lässt sich sagen, dass die Nutzung großer Datenmengen in der Strafverfolgung sowohl Chancen als auch Herausforderungen bietet. Während sie die Möglichkeit bietet, Ermittlungen präziser und effektiver zu gestalten, müssen gleichzeitig Datenschutzbedenken und die Effizienz der Datenverarbeitung sorgfältig abgewogen werden. Es ist notwendig, einen Gleichgewichtspunkt zu finden, der sowohl die Sicherheit der Gesellschaft als auch die Rechte des Einzelnen schützt.

5.2 Ideen / Ausblick

Im Rahmen unserer Arbeit kam immer wieder die Zusammenarbeit von Ermittlungsbehörden mit ISPs und anderen Diensteanbietern auf. Auf Nachfrage im direkten Umfeld bei einem Mitarbeiter eines regionalen ISPs teilte dieser uns mit, dass bis heute keine standardisierten Verfahren zur Abfrage und Übergabe von Datenpaketen an die Behörden bestehen.

Unserer Meinung nach Bedarf es hier dringend an Vereinheitlichung, um die Ermittlungsarbeit zu vereinfachen und Strafverfolgern das Durchsuchen von Datenpaketen, welche durch Diensteanbieter erstellt werden, zu ermöglichen. Mit CASE (Cyber-Investigation Analysis Standard Expression) gibt es insbesondere im Ausland zwar Versuche der Vereinheitlichung, diese passen aber nur grob auf die europäischen Anforderungen hinsichtlich Datenschutz und Verarbeitung.

Literaturverzeichnis

[1] Genesis marketplace: A digital fingerprint darknet store. URL https://www.f5.com/labs/articles/threat-intelligence/genesis-marketplace--a-digital-fingerprint-darknet-store. Accessed on 2. Januar 2024.

[2] n2disk - High-Speed Traffic Recording and Replay. https://www.ntop.org/products/traffic-recording-replay/n2disk/, 2024. Zugriff: 2. Januar 2024.

[3] Luca Belli. Internet Service Providers and Data Protection. Springer, Cham, 2018. ISBN 978-3-319-78184-7.

[4] Bundeskriminalamt. Straftaten im internet. https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/internet_node.html, 2024. Zugriff am 2024-01-02.

[5] Ignacio Castro. Shaping the internet: History and impact of ixp growth. https://labs.ripe.net/author/ignacio_castro/shaping-the-internet-history-and-impact-of-ixp-growth/, 2019. Zugriff: 2. Januar 2024.

[6] dpa. Kriminalbeamte fordern mehr kollegen für cybercrime. Heise Online, 2020. URL https://www.heise.de/news/Kriminalbeamte-fordern-mehr-Kollegen-fuer-Cybercrime-4624803.html. Zugriff: 2. Januar 2024.

[7] Christopher Hadnagy. Social engineering: The art of human hacking. In Wiley, 2011.

[8] Niemitz, M. & Pentang, G. Themenübersicht Hackathon.

[9] Tagesschau. Bundesverwaltungsgericht: Anlasslose vorratsdatenspeicherung ist rechtswidrig. https://www.tagesschau.de/inland/gesellschaft/bundesverwaltungsgericht-vorratsdatenspeicherung-rechtswidrig-100.html, 2023. Zugriff: 2. Januar 2024.

[10] Thomas Goger und Wolfgang Prehl. Auswertung von smartphones: Kriminelle aufspüren anhand ihrer google-suche. https://www.deutschlandfunknova.de/, 2021. Zugriff am 2024-01-02.

POLIZEI
Nordrhein-Westfalen
Düsseldorf

Polizeipräsidium Düsseldorf
Dir.K, KI 2, KK 23
Heesenstraße 26, 40549 Düsseldorf

Persönlich
[redacted]

27.11.2023

[redacted]
Bearbeitung: [redacted], KK
Telefon: 0211 / 870 [redacted]
Telefax: 0211 / 870 [redacted]
[redacted]@polizei.nrw.de

Auskunftsersuchen

Sehr geehrter Herr [redacted]

die Kriminalpolizei Düsseldorf ermittelt derzeit in einem Strafverfahren der Staatsanwaltschaft Düsseldorf mit dem Aktenzeichen [redacted] u.a. wegen des Tatverdachts der

Verletzung von Geschäftsgeheimnissen und der

Unerlaubten Verwertung urheberrechtlich geschützter Werke

gegen die Verantwortlichen der

[redacted]

Gegenstand der Ermittlungen ist u.a. die Entwendung und weitere widerrechtliche Verwendung von Daten durch [redacted] Nach unserem Kenntnisstand hat [redacted] in Ihren Hause Server angemietet und Daten auf diese übertragen lassen.

Daher ersuche ich Sie höflichst uns eine Auskunft darüber zu geben,

- **ob [redacted] aktuell Rechenserver bei [redacted] angemietet hat und falls ja**
  - **seit wann bzw. in welchen Zeitraum,**
  - **unter welcher Vertragsnummer,**

- **und in welchem Umfang (eingelagerte Datenmenge, Anzahl Server, etc.),**

- **wer die zuständigen Kontaktpersonen [redacted] waren/sind, welche zum einen für den damals ersten Datentransfer/Datenübergabe und zum anderen für die derzeitigen Datentransfers verantwortlich sind/waren,**

- **wie der erste Datentransfer bzw. die erste Datenübergabe konkret stattgefunden hat (z.B. Daten [redacted] auf Hardware erhalten?),**

- ***ob Ihnen damals eventuell* NAS-Server des Farbikats Synology Typ RS814RP+ zur *Datenübergabe ausgehändigt worden sind* (Seriennummern: [redacted] und [redacted]**

- **und falls ja, ob diese eventuell bei Ihnen mit in die *Serverstruktur eingebunden* worden und ggf. auch noch in Betrieb sind.**

Bitte übersenden Sie mir zu den entsprechenden Vertragsunterlagen *jeweils eine Kopie zu. Sie* können mir auf dieses Schreiben auch per gerne E-Mail antworten und ggf. *Kopien von Belegen* auf elektronischen Wege übersenden.

Bitte geben Sie uns eine Rückinfo bis zum **20.12.2023**.
Das Ersuchen erfolgt im Auftrag der Staatsanwaltschaft Düsseldorf.

Es wird dringend darum gebeten, [redacted] und deren Verantwortliche *über* dieses Ersuchen nicht in Kenntnis zu setzen, da ansonsten die weiteren *Ermittlungen* gefährdet werden könnten und Sie sich darüber hinaus wegen *Strafvereitelung / Begünstigung* strafbar machen könnten.

Für Ihre Bemühungen bedanke ich mich im Voraus. Für Rückfragen stehe ich Ihnen gerne zur *Verfügung.*

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Kriminalkommissar