Helion

<packt>

OSINT w praktyce

Jak gromadzić i analizować dane dostępne w sieci

DALE MEREDITH

Tytuł oryginału: The OSINT Handbook: A practical guide to gathering and analyzing online information

Tłumaczenie: Karolina Stangel

ISBN: 978-83-289-2042-2

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/osintw
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

Rozdział 2 Niewidoczni i nietykalni — znaczenie anonimowości w pracy analityka OSINT

W szybko ewoluującej dziedzinie **OSINT** zabezpieczenie własnej anonimowości jest nie tylko najlepszą praktyką, lecz nieodzownym elementem skutecznego dochodzenia. W tym rozdziale rzucimy nieco światła na priorytetową rolę anonimowości w analizie OSINT. W kolejnych podrozdziałach będziemy zajmować się różnymi aspektami ochrony prywatności w procesie kompleksowego gromadzenia informacji wywiadowczych. Wraz z końcem tego rozdziału będziemy uzbrojeni w wiedzę i umiejętności niezbędne do utrzymania anonimowości, zarządzania swoim cyfrowym śladem i prowadzenia bezpiecznej komunikacji w ramach białego wywiadu.

W tym rozdziale zajmiemy się przede wszystkim następującymi tematami:

- wprowadzenie do anonimowości i prywatności w OSINT;
- ochrona własnego śladu cyfrowego;
- aktualizowanie wiedzy na temat cyberzagrożeń.

Wprowadzenie do anonimowości i prywatności w OSINT

OSINT wymaga głębokiej analizy dużych ilości danych z publicznie dostępnych źródeł. Z wielu ważnych powodów analitycy OSINT muszą jednak zadbać również o swoją prywatność i anonimowość. Powody te możemy podsumować w następujących punktach:

- **Alarm dla podejrzanych**. Jeżeli osoba lub firma zorientuje się, że jest przedmiotem dochodzenia OSINT, jest w stanie podjąć działania utrudniające gromadzenie danych. Może skasować posty w portalach społecznościowych, ograniczyć widoczność profilu, przestać udostępniać witrynę internetową lub zniszczyć dowody. Anonimowość działań odgrywa zatem kluczową rolę w tym, aby nie zaalarmować celu.
- **Niepowodzenie akcji**. Jeżeli cel zorientuje się, że jest obserwowany, może zmodyfikować swoje działania lub zmienić sposób komunikacji, unikając tym samym wykrycia. Może to poważnie zaszkodzić otwartemu dochodzeniu OSINT, jeżeli prowadzący je nie zgromadzili jeszcze danych wywiadowczych wystarczających do podjęcia decyzji. Anonimowość pomaga chronić dochodzenie przed wykryciem.
- **Przerwanie podejrzanych działań**. Jeżeli dochodzenie zostanie wykryte na wczesnym etapie, organy ścigania i inne instytucje mogą nie być w stanie wykryć działalności przestępczej ani zgromadzić dowodów niezbędnych do postawienia winnych przed sądem. Podejrzani mogą unikać wzbudzania podejrzeń. Anonimowość to klucz do rzetelnego monitorowania celów bez ryzyka wykrycia.
- **Konsekwencje prawne i kwestie etyczne**. W niektórych krajach nawet niezamierzone poinformowanie podejrzanych o prowadzonym dochodzeniu może owocować postawieniem nam zarzutów. Anonimowość pozwala uniknąć nieumyślnych naruszeń etyki i prawa.
- **Bezpieczeństwo osób**. Sprawcy, tacy jak hakerzy, terroryści czy inne grupy przestępcze, mogą mścić się na analitykach i źródłach, jeżeli dowiedzą się o prowadzonym dochodzeniu. Anonimowość i prywatność gwarantują, że my analitycy i nasze źródła będziemy bezpieczni.
- **Wycieki danych**. Informacje poufne powinny być chronione przed dostaniem się w niepowołane ręce. Jest to możliwe jedynie dzięki ścisłej kontroli sposobu wykorzystania tych danych i dostępu do nich. W celu uniknięcia katastrofalnych w skutkach naruszeń danych konieczne jest przestrzeganie zasad zachowania prywatności.

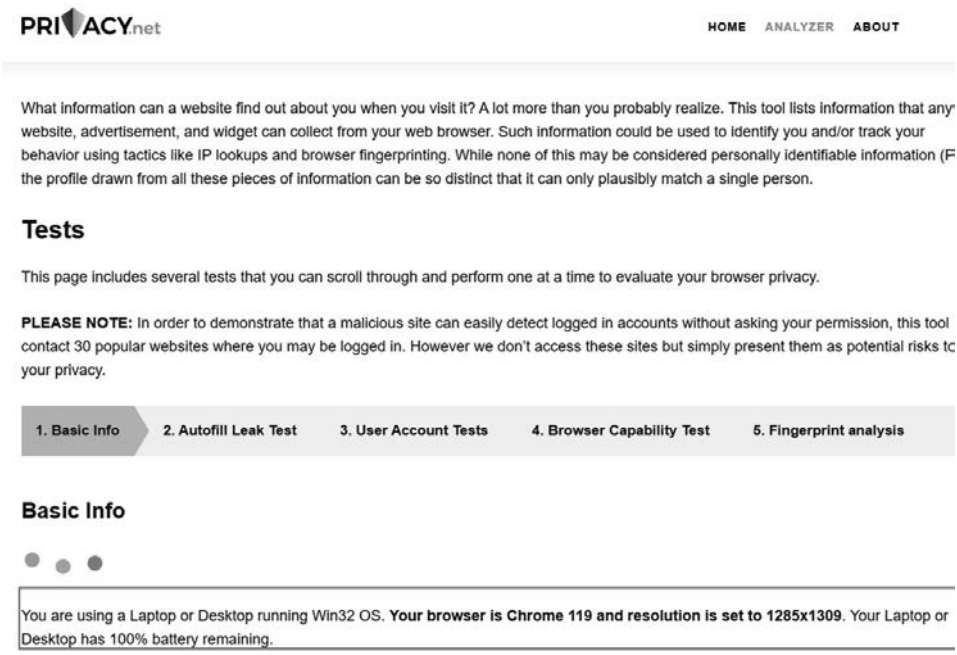
Czynniki prowadzące do utraty anonimowości w OSINT

W jaki sposób możemy zostać wykryci w trakcie dochodzenia? Spójrzmy na kilka przykładów:

- **Ujawnienie adresu IP**. Jednym z najprostszych sposobów na ukrycie się jest nieujawnianie swojego adresu IP. Jeżeli nie korzystamy z **wirtualnej sieci prywatnej** (ang. *Virtual Private Network*, VPN) lub przeglądarki Tor, odwiedzane strony mogą zarejestrować nasz prawdziwy adres IP.

Jako specjalista ds. cyberbezpieczeństwa stanąłem kiedyś w obliczu dużego wyzwania. Potrzebowałem znaleźć informacje na temat cyberataków, które wydawały się pochodzić z konkretnego miejsca. Aby dokonać tego bez wzbudzania podejrzeń atakujących, użyłem **sieci VPN**. Połączyłem się z serwerem z innego kraju, który ukrył mój prawdziwy adres IP i lokalizację. Wyglądało to tak, jakbym przeglądał sieć z lokalizacji powiązanej z tym serwerem, a nie ze swojej własnej. To pozwoliło mi bezpiecznie przeglądać różne strony i fora oraz zbierać informacje bez ujawniania mojej tożsamości. Doświadczenie to uświadomiło mi potęgę sieci VPN, jeżeli chodzi o ochronę cyfrowej tożsamości podczas badania wrażliwych tematów.

- **Pobieranie cyfrowego odcisku palca przeglądarki (ang. *browser fingerprinting*)**. Przeglądarki internetowe zbierają zaskakujące ilości danych, od rozdzielczości ekranu po zainstalowane wtyczki. Wszystkie te informacje mogą stanowić swoisty **odcisk palca** (ang. *fingerprint*). Nie wierzysz? Zrób sobie przerwę i odwiedź stronę *https://privacy.net/analyzer* (rysunek 2.1). A nie mówiłem?



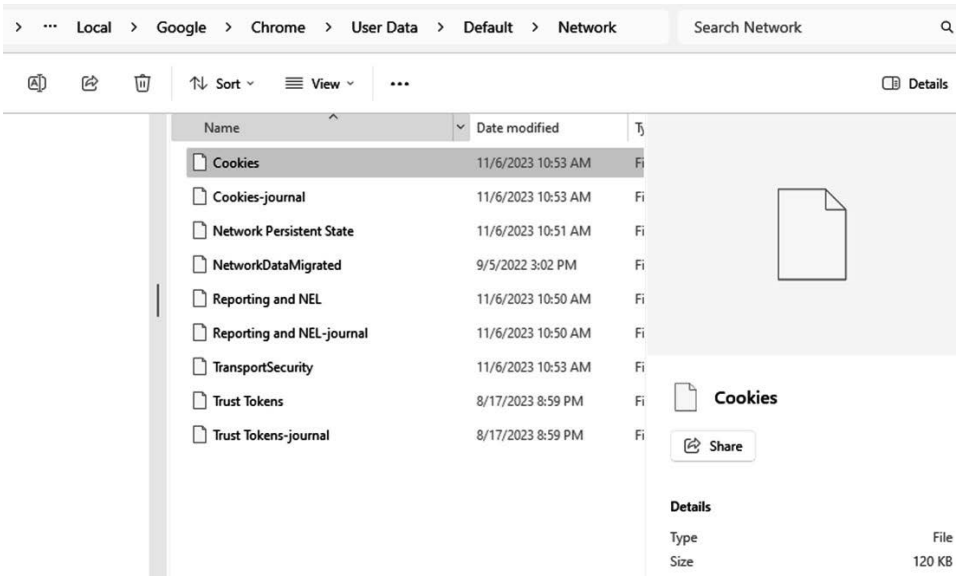
Rysunek 2.1. Moje wyniki z analizatora Privacy.net

Jeżeli myślisz, że tryb incognito Cię ochroni, to niestety się mylisz. Dzięki cyfrowemu odciskowi palca przeglądarki możliwe jest śledzenie działań użytkownika z różnych sesji.

- **Nadmierne zaufanie do technologii**. Poleganie na narzędziach takich jak sieci VPN czy przeglądarka Tor bez pełnego zrozumienia ich ograniczeń

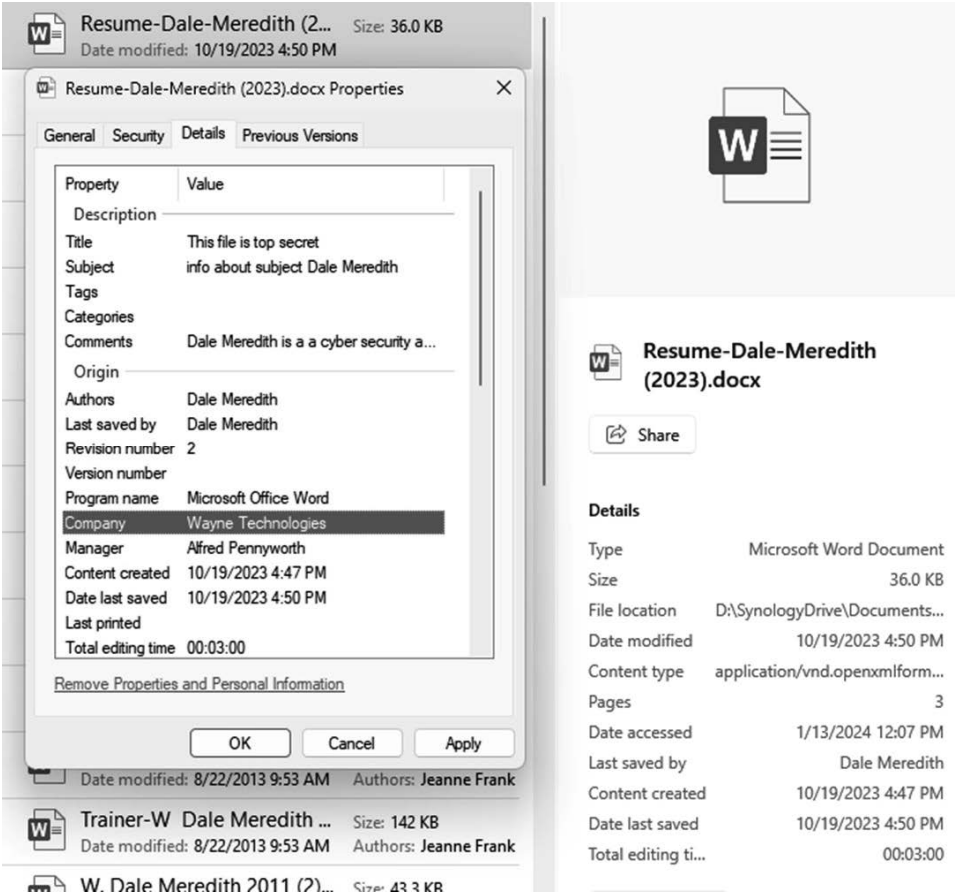
może stworzyć fałszywe poczucie bezpieczeństwa. Na przykład niektóre sieci VPN logują działania użytkownika, adresy IP, znaczniki czasowe i inne informacje pomimo haseł marketingowych, że tego nie robią. Potężni przeciwnicy, tacy jak organy państwowe, w niektórych przypadkach są w stanie zdeanonimizować działania użytkownika korzystającego z przeglądarki Tor. Żadna technologia nie stanowi uniwersalnego rozwiązania w kwestii ochrony anonimowości. Trzeba stosować wiele warstw zabezpieczeń i mieć świadomość słabości każdego z narzędzi lub podejść.

- **Śledzenie za pomocą plików cookie (ang. *cookie tracking*)**. Pliki cookie to niewielkie pliki tekstowe, które strony internetowe zapisują na urządzeniach, aby śledzić i zapamiętywać działania użytkowników (rysunek 2.2). Chociaż są wygodne, gdy pamiętają nasze dane do logowania lub zawartość koszyka, pozwalają firmom tworzyć skomplikowane profile dotyczące zwyczajów, zainteresowań, zachowań i innych aspektów na podstawie danych zgromadzonych z wielu stron i sesji. Regularne usuwanie plików cookie może ograniczyć śledzenie, ale firmy opracowały bardziej zaawansowane technologie, takie jak pobieranie cyfrowego odcisku palca przeglądarki czy identyfikacja na podstawie unikalnych cech elementu *canvas* na danej przeglądarce (ang. *canvas fingerprinting*), dzięki którym pliki cookie nie są niezbędne do śledzenia. Korzystanie z przeglądarek dbających o prywatność użytkownika, takich jak Tor, oraz zacieranie za sobą cyfrowych śladów poprzez niepowtarzanie tych samych wzorców zachowań jest ważne, jeżeli chcemy uniknąć śledzenia.



Rysunek 2.2. Pliki cookie są przechowywane w różnych miejscach i mogą zawierać wiele cennych informacji

- **Wycieki metadanych**. Dokumenty, zdjęcia, pliki audio oraz wideo, mogą zawierać metadane, czyli generowane przez urządzenie informacje na temat samego pliku. Mogą one obejmować znaczniki geograficzne i czasowe, numery seryjne urządzeń czy historię edycji (rysunek 2.3). Podobnie wiadomości takie jak e-maile mają nagłówki, które zawierają adres IP, informacje na temat klienta itp. Wyciek metadanych może dostarczyć informacji na temat tożsamości użytkownika i narazić na szwank jego anonimowość. Dlatego przed udostępnieniem starannie usuwajmy metadane z plików za pomocą odpowiednich narzędzi. Unikajmy też metod komunikacji, które powodują ujawnianie takich metadanych.



Rysunek 2.3. Przykład metadanych dołączonych do pliku

- **Niezabezpieczone publiczne sieci wi-fi**. Publiczne sieci wi-fi w kawiarniach, na lotniskach czy w hotelach często nie są zabezpieczone hasłem ani innymi metodami. Z tego względu każdy w pobliżu może łatwo przechwycić niezaszyfrowaną komunikację przechodzącą przez sieć i obserwować nasze

działania online. Nigdy nie loguj się do ważnych kont, w tym do poczty elektronicznej czy aplikacji bankowej, i nie podawaj poufnych informacji, gdy używasz niezabezpieczonej, publicznej sieci wi-fi. W takich przypadkach korzystaj z zaufanej sieci VPN, aby zaszyfrować komunikację. Najlepszym rozwiązaniem byłoby w ogóle poczekać z przesyłaniem wrażliwych danych do momentu połączenia się ze znaną i zaufaną siecią.

- **Socjotechnika**. Choć dysponujemy coraz lepszymi zabezpieczeniami technicznymi, ludzka natura nadal jest podatna na stare dobre triki socjotechniczne, takie jak phishing. W ochronie przed nimi kluczowe znaczenie ma nieużywanie tych samych haseł do różnych kont, korzystanie z uwierzytelniania wieloskładnikowego, gdy tylko to możliwe, zabezpieczanie komunikacji szyfrowaniem PGP oraz nauczenie się wykrywania oszustwa przed kliknięciem łącza lub załącznika. Żaden zestaw narzędzi do ochrony anonimowości nie pomoże nam, gdy ktoś podstępem wydobędzie od nas dane osobowe.
- **Korzystanie z kont osobistych do celów OSINT**. Jednym z najpoważniejszych błędów w dziedzinie bezpieczeństwa operacyjnego (ang. *operations security*, OPSEC) jest prowadzenie działań OSINT i badań w obszarze cyberbezpieczeństwa z kont, które można powiązać z naszą prawdziwą tożsamością. Gdy gromadzimy informacje wywiadowcze za pomocą wyszukiwarek internetowych, sieci społecznościowych, forów i innych cyfrowych lokalizacji, zawsze używajmy jednorazowych, anonimowych kont i maskujmy adresy IP. Zadbajmy o rygorystyczne rozdzielenie swoich prywatnych działań w internecie od związanych z dochodzeniem.
- **Przypadkowe potknięcia**. Pojedynczy wyciek danych osobowych na czacie, w poście na forum lub podczas rozmowy za pomocą komunikatora może wystarczyć, aby nasza anonimowość legła w gruzach. Musimy zachowywać niezwykłą ostrożność, gdy dzielimy się jakimikolwiek informacjami na swój temat w internecie, gdyż takie szczegóły mogą nas zdemaskować. Musimy również konsekwentnie rozdzielać alternatywne tożsamości. Wielokrotne wykorzystywanie tych samych nazw użytkownika, elementów adresów e-mailowych czy haseł przy tworzeniu kolejnych kont może ułatwiać ich powiązanie. A wystarczy chwila nieuwagi.
- **Nieaktualna wiedza**. Co chwila mamy do czynienia z nowymi technikami hakerskimi i sposobami wykorzystania luk w zabezpieczeniach. Jeżeli nie aktualizujemy swojej wiedzy na temat najnowszych zagrożeń dla prywatności i bezpieczeństwa, nasze dane mogą paść ofiarą tych nowych metod, o których nic nie wiemy i przeciw którym się nie zabezpieczyliśmy. Nigdy nie możemy zakładać, że mamy wystarczającą wiedzę. Aby dotrzymać kroku zmieniającym się zagrożeniom, uczenie się powinno być nieustającym procesem.

W poszukiwaniu złotego środka — prywatność w dochodzeniach OSINT

Technologia zawsze wywraca zasady gry do góry nogami. Chociaż łapanie przestępców, złoczyńców i arcyłotrów brzmi jak świetna przygoda, to jeżeli nie będziemy uważni, może zaszkodzić naszemu życiu prywatnemu.

Potrzebujemy systemu, który zapewnia nadzór, kontrolę, obiektywność i, co najważniejsze, osobistą odpowiedzialność. Nie możemy pozwolić na beztroskie korzystanie z tych potężnych narzędzi, jak się komu żywnie podoba, bez określenia kilku fundamentalnych zasad. Te zasady muszą być przejrzyste, tak aby każdy mógł zgłosić obiekcje, gdy coś jest nie w porządku.

Technologia sama w sobie nie jest wyposażona w moralny kompas. To tylko narzędzie. Musimy działać mądrze, etycznie i przede wszystkim czujnie. W końcu to bardziej maraton niż sprint. Jeżeli będziemy naginać zasady dla krótkoterminowych zwycięstw, sami sobie zgotujemy porażkę w długoterminowej perspektywie. Zawsze musimy mieć z tyłu głowy prawdziwy cel, a mianowicie społeczeństwo, które jest jednocześnie bezpieczne i wolne. Ochrona tej kruchej równowagi, moi drodzy, jest czymś, na co nie należy szczędzić wysiłków. W porządku, myślę, że się rozumiemy. Kazanie zakończone.

Ochrona własnego śladu cyfrowego

Cyfrowy ślad jest jak cień w słoneczny dzień: zawsze nam towarzyszy i zmienia się nieco, w miarę jak idziemy przez życie. Ten cień może jednak czasem powiedzieć na nasz temat więcej, niż byśmy chcieli. Tylko jedno kliknięcie chroni nasze dane osobowe, takie jak miejsce zamieszkania czy numer PESEL, przed ciekawskim wzrokiem. Nie wyrażaliśmy zgody na tak szczegółową obserwację, ale prawda jest taka, że jesteśmy na nią narażeni i wszyscy powinniśmy być tym zaniepokojeni.

Ograniczanie TWOJEGO cyfrowego śladu

Zanim przejdziemy do prowadzenia dochodzenia OSINT, jako specjaliści z zakresu cyberbezpieczeństwa powinniśmy wiedzieć, jak chronić samych siebie. Czy wiesz, że około 91% przestępstw cybernetycznych rozpoczyna się od prostego e-maila (*https://www.yeoandyeo.com/resource/91-of-cyberattacks-begin-with-a-phishing-email*)?

Na początku atakujący może nawet nie wiedzieć, jak się nazywasz. W miarę zbierania informacji tworzy jednak pełen obraz Twojej cyfrowej tożsamości. W dzisiejszym świecie dane są równie cenne co ropa naftowa. Zdanie sobie sprawy z tego, z jaką łatwością ktoś może zdobyć informacje na nasz temat, jest nie tylko niepokojące, lecz także powinno skłonić nas do działania.

Nasze dane osobowe są wykorzystywane przez cyberprzestępców, stalkerów i szukające korzyści przedsiębiorstwa. Nawet jeżeli sami nie sprzedajemy bezpośrednio tych

informacji, nasze codzienne czynności robią to za nas. Każde zapytanie w wyszukiwarce Google, każdy post w mediach społecznościowych, a nawet każdy produkt, który przeglądamy w sklepie internetowym, uzupełnia nasz profil — profil, którego sami nie stworzyliśmy (rysunek 2.4).

Rysunek 2.4. Firma Google śledzi nas za pomocą naszego telefonu (*https://timeline.google.com*)

Dlaczego ochrona danych osobowych jest obecnie ważniejsza niż kiedyś?

Naruszenia danych stwarzają zagrożenie nie tylko tu i teraz. Mają dalekosiężne konsekwencje, łącznie z ryzykiem kradzieży tożsamości czy nawet naruszenia bezpieczeństwa fizycznego osób. Ich wpływ jest wielowymiarowy. Na przykład podszywający się pod nas oszuści mogą zaciągnąć pożyczkę, realizować nielegalne transakcje, a nawet dokonywać poważniejszych przestępstw. Oczyszczenie się z zarzutów jest nie tylko trudne, lecz również wyniszczające finansowo i emocjonalnie.

Naruszenia danych mogą mieć istotny wpływ na nasze życie prywatne. Na przykład potencjalny pracodawca może znaleźć nierzetelne lub niekorzystne informacje na nasz temat, co może zaszkodzić naszej reputacji, zanim w ogóle będziemy mieć szansę zaprezentować swoje umiejętności.

Stawka jest wysoka, a prawdopodobieństwo nie działa na naszą korzyść. Nie poddawajmy się jednak cyfrowemu przeznaczeniu. Oto kilka wskazówek, które nie tylko

zwiększą naszą cyfrową świadomość, lecz również możliwości. Nasze dane osobowe są cenne. Czas zacząć je traktować w ten sposób.

Przeglądarki internetowe — pierwszy front walki o dane

Przeglądarka to przyjacielsko usposobiony pośrednik, który umożliwia nam swobodne poruszanie się po cyfrowej autostradzie informacyjnej. Tutaj czytamy wiadomości, oglądamy filmy, prowadzimy potyczki w mediach społecznościowych czy co tam nam w duszy gra. Pod tą sympatyczną fasadą czai się jednak aparat gromadzenia danych, który zawstydziłby amerykańską agencję wywiadowczą NSA. Nie, nie chodzi mi o to, żeby napchać Ci głowę teoriami spiskowymi. Niemniej jednak lepiej zapamiętaj moje słowa: „To, że nie widzisz czarnych helikopterów, nie znaczy, że ich tam nie ma!".

Własne i zewnętrzne pliki cookie

Układ pokarmowy przeglądarki wypełniają różne rodzaje ciasteczek:

- **Własne pliki cookie**. Zapisywane przez witrynę internetową, którą odwiedzamy. Pamiętają nasze ustawienia, zawartość koszyka z zakupami i inne tajemnice.
- **Zewnętrzne pliki cookie**. Zdeponowane przez kogoś innego niż witryna internetowa, na której przebywamy, np. przez reklamodawców. Te pliki cookie nie odstępują nas na krok podczas naszej podróży po sieci, podsuwając nam pod nos tę parę butów, którą kiedyś zostawiliśmy w koszyku.

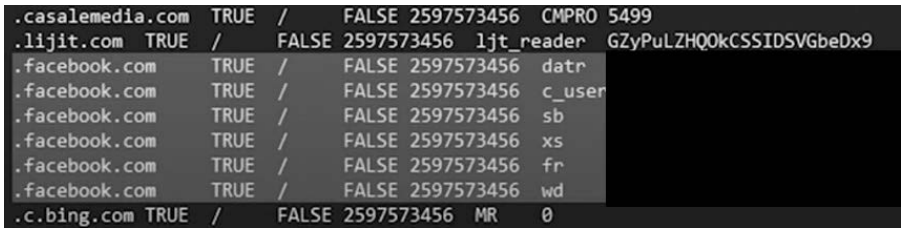
W jaskini ciasteczkowego potwora

Narzędzie nazywane **złodziejem ciasteczek** (ang. *cookie grabber*) zostało stworzone z myślą o przechwytywaniu plików cookie. Czy to groźne? Tak, złodziej ciasteczek może wykradać oba rodzaje ciasteczek, w tym te, które zawierają dane do logowania.

Dajmy na to, że wchodzimy na stronę, na której czyha na nas złodziej ciasteczek. Nieświadomi zagrożenia logujemy się na tej stronie, a nasze sesyjne pliki cookie wędrują do kieszeni złoczyńcy. W ten sposób atakujący zdobył klucz do naszego cyfrowego królestwa i uzyskał dostęp do wszystkich kont na innych platformach, a wszystko dzięki prostemu trikowi, którego nikt nawet nie zauważył.

To jednak nie wszystko. Niektóre witryny internetowe przechowują dane do logowania (tzn. nazwę użytkownika i hasło) w formie niezaszyfrowanego tekstu bezpośrednio w przeglądarce. W takim przypadku, gdy logujesz się w witrynie, przechowuje ona wpis z danymi uwierzytelniającymi w formacie czytelnym dla każdego. Jeżeli Twój komputer dostał się w niepowołane ręce lub pracujesz na współdzielonym urządzeniu, ktoś może użyć prostych narzędzi, takich jak edytor heksadecymalny, aby wykraść te dane. To tak, jakbyśmy zostawili klucze od domu na ławce w parku i poszli sobie dalej.

Wyobraź sobie logowanie na stronie internetowej, która nie podchodzi poważnie do kwestii prywatności. Dane do logowania są przechowywane w pliku cookie w formie niezaszyfrowanej. Nam się do niczego nie przydadzą, ale haker — a nawet wścibski współlokator — może z łatwością wydobyć te informacje i zalogować się na nasze konto jak na swoje własne (rysunek 2.5).



Rysunek 2.5. Dzięki złodziejowi ciasteczek można ukraść cudze konto lub tożsamość

Jak się chronić?

Zarówno sieci VPN, jak i konfigurowanie **łańcuchów serwerów pośredniczących** (ang. *proxy chaining*) to skuteczne sposoby ochrony prywatności w internecie. Dzięki nim można ukryć własny adres IP, utrudniając zewnętrznym plikom cookie śledzenie naszych działań. To szczególnie ważne w dzisiejszym cyfrowym świecie, gdzie śledzenie użytkowników i ochrona danych stanowią istotne zagadnienia. Ważne jest jednak, aby wybrane przez nas sieci VPN i serwery proxy były godne zaufania, ponieważ one również mają dostęp do naszych danych. Zawsze preferuj usługi, które są znane z rygorystycznych zasad ochrony prywatności i zaangażowania na rzecz bezpieczeństwa użytkownika.

DuckDuckGo — cichy bohater ochrony prywatności

Jeżeli przyrównać mainstreamowe przeglądarki do szukających poklasku celebrytów, DuckDuckGo (rysunek 2.6) jest introwertycznym geniuszem, którego nikt nie słucha, choć wszyscy powinni. Misją DuckDuckGo jest uproszczenie ochrony prywatności online. Ta odważna firma zabezpiecza użytkownika przed śledzeniem podczas jego podróży po internecie, a jej zapora sieciowa blokuje próby dostępu do historii przeglądania i danych osobowych.

Produkty DuckDuckGo są stworzone z myślą o tym, aby oddać nam kontrolę nad naszymi danymi. Ta wyszukiwarka nie zbiera historii zapytań ani danych użytkownika. Wszystkie wyszukiwania są domyślnie poufne. Rozszerzenie do przeglądarki i aplikacja mobilna również blokują agresywne skrypty śledzące, które czyhają na nas w sieci.

Szyfrowanie stanowi kolejną warstwę ochrony, która zabezpiecza połączenia między użytkownikiem a stronami internetowymi. Wspólnie te narzędzia tworzą skuteczną tarczę chroniącą prywatność przed profilowaniem ze strony reklamodawców i innych zewnętrznych firm.

Rysunek 2.6. DuckDuckGo to wspaniała przeglądarka pozwalająca użytkownikom zachować prywatność

Działalność biznesowa DuckDuckGo pokrywa się z misją stawiania prywatności na pierwszym miejscu. Firma zarabia dzięki reklamom dobranym na podstawie słów kluczowych — zamiast reklam bazujących na profilach osobowych, które ciągną się za nami jak koszmary z przeszłości.

Gotowi na dobrą zmianę? Doskonale. Nie da się jednak z dnia na dzień zapomnieć o jednym sposobie życia i skoczyć na główkę w inny. Na taką zmianę trzeba się przygotować:

1. **Pobierz i zainstaluj**. Wybierz swoją bezpieczną przeglądarkę.
2. **Zaimportuj ustawienia**. Większość przeglądarek pozwala importować zakładki i ustawienia z innych przeglądarek.
3. **Ustaw jako domyślną**. Ustaw nową przeglądarkę jako domyślną do wszystkich celów.

Alternatywne przeglądarki — wady i zalety

DuckDuckGo nie jest jedynym rycerzem na białym koniu, który może pospieszyć nam na ratunek. Są też inne przeglądarki, a każda z nich ma swoje słabe i mocne strony.

Przeglądarka Brave

To tę przeglądarkę polecam wszystkim. Jest to relatywnie nowy produkt na rynku.

Brave (*https://brave.com*) to wspaniały punkt wyjścia do ukrycia naszych działań w internecie przed ciekawskim wzrokiem (rysunek 2.7). Domyślnie blokuje narzędzia śledzące, ograniczając firmom zewnętrznym możliwość śledzenia nas.

Rysunek 2.7. Przeglądarka Brave — mój osobisty faworyt w dziedzinie ochrony tożsamości

Jeżeli niechętnie podchodzisz do zmiany przeglądarki, dodam, że rozszerzenia takie jak Startpage zapewniają podobne zabezpieczenia.

Startpage wyświetla ocenę prywatności strony na skali od jednego do pięciu, pozwalając użytkownikowi zobaczyć, jak wiele skryptów śledzących i plików cookie uniknięto na każdej stronie (rysunek 2.8). Szczegółowe informacje mogą zaskoczyć, ale są bardzo pomocne. Startpage ukrywa tożsamość użytkownika przed wszelkimi skryptami śledzącymi poprzez maskowanie jego cyfrowego śladu.

Chcemy zablokować skrypty śledzące, ale możemy potrzebować niektórych nieszkodliwych plików cookie, aby umożliwić stronom poprawne funkcjonowanie. Startpage umożliwia zatwierdzanie konkretnych plików cookie bez zezwalania na nieograniczony dostęp. W przypadku wyszukiwania Startpage przesyła zapytanie do wyszukiwarki Google, ale robi to anonimowo, aby nie przyczyniać się do budowy naszego upiornego profilu.

Rysunek 2.8. Rozszerzenie Startpage w Chrome Web Store

Z potężnymi sojusznikami u swego boku, takimi jak zabezpieczenia przeglądarki Brave oraz ułatwiające podejmowanie decyzji informacje z rozszerzenia Startpage, możesz teraz stanąć do walki ze swoim cyfrowym cieniem. Nigdy więcej nie będziesz bezbronną ofiarą dla cybernetycznych mechanizmów śledzących. Podsumujmy wady i zalety tego rozwiązania:

- **Zalety**: domyślnie blokuje reklamy i skrypty śledzące.
- **Wady**: wbudowany system wyświetlania reklam może nie trafić w nasze gusta.

Przeglądarka Tor

Tor to połączona ze sobą społeczność skupiona wokół wspólnego celu, jakim jest zapewnienie prywatności online. Projekt Tor (rysunek 2.9) zrodził się w duchu buntu. Rządy szpiegują, korporacje śledzą, a Tor przybywa nam na odsiecz! To swoisty ruch oporu online, wyposażony w serwery, serwery-przekaźniki (ang. *relays*) i węzły. Tę infrastrukturę utrzymują ochotnicy z całego świata, a żaden pojedynczy punkt nie ma obrazu pełnej ścieżki.

Tor usuwa metadane i maskuje adresy IP. Komunikacja jest wielokrotnie zaszyfrowana, a w miarę kolejnych skoków przez węzły prywatnej sieci stopniowo odszyfrowywana. To jak zdejmowanie kolejnych warstw cebuli. Każdy serwer pośredniczący potrafi określić jedynie następny przystanek, ale nie zna punktu docelowego.

Jest to możliwe jedynie dzięki dużej liczbie węzłów. Tysiące bezinteresownych ochotników użyczają swoich komputerów jako węzłów sieci Tor. Te zróżnicowane punkty wejścia, przejścia i wyjścia stanowią zdecentralizowany trzon tej sieci. Nie poddające się cenzurze połączenia są szyfrowane w sposób chroniący prywatność.

Rysunek 2.9. Strona projektu Tor

Tor to darmowe oprogramowanie (*https://torproject.org*) stworzone przez społeczność wyznawców prywatności. Kod jest dostępny dla wszystkich do kontroli i modyfikowania. Otwartość źródeł pozwala projektowi Tor realizować swoją misję. Te narzędzia nie mają ukrytych luk czy celów. Podsumujmy wady i zalety tego rozwiązania:

- **Zalety**: zapewnia najwyższy poziom anonimowości.
- **Wady**: korzystanie z przeglądarki jest wolniejsze ze względu na przechodzenie przez wiele serwerów pośredniczących.

„Dale, a od których przeglądarek trzymałbyś się z daleka?" — zapytasz. No cóż, lista wygląda mniej więcej tak, przy czym kolejność nie jest zbyt istotna:

- Google Chrome,
- Microsoft Edge,
- Firefox,
- Opera,
- Safari.

Przeglądarka to nasza pierwsza linia obrony przed cyberzagrożeniami. To nie tylko wrota do internetu. To forteca, która chroni nasze dane. Dokonaj zmiany już dziś i ufortyfikuj swoją przeglądarkę. Twoje cyfrowe „ja" będzie Ci wdzięczne za dodatkową ochronę.

Skarpetkowe pacynki — tworzenie person internetowych i zarządzanie nimi

Zanim nasza wyobraźnia pogalopuje zbyt daleko — nie, nie będziemy zajmować się tworzeniem urokliwych pacynek z ulubionej pary skarpetek. Skarpetkowe pacynki (ang. *sock puppets*) to inaczej fikcyjne tożsamości internetowe utworzone do maskowania,

manipulacji i zbierania informacji. Te postaci, niczym pacynki na dłoni lalkarza, pozwalają nam chować się pod różnymi tożsamościami i prowadzić anonimowe interakcje.

Chociaż nie jest w zasadzie nielegalne, używanie pacynek często nie jest mile widziane ze względu na potencjalne nadużycia. Można je wykorzystywać do szerzenia dezinformacji, sztucznie zwiększać wskaźniki popularności, anonimowo napastować innych i infiltrować społeczności incognito. Uzasadnione zastosowania obejmują z kolei dziennikarstwo śledcze i testy penetracyjne.

Istnieje kilka względów, dla których osoby i organizacje mogą korzystać z kont typu *sock puppet*:

- **Anonimowość**. Najważniejszym powodem jest rozdzielenie działań online od prawdziwej tożsamości, co umożliwia gromadzenie informacji bez utraty anonimowości.
- **Podstęp**. Fikcyjne konta pozwalają wpływać na przebieg rozmów, podawać nieprawdziwe informacje i manipulować percepcją. Można je wykorzystać do infiltracji lub socjotechniki.
- **Rozpoznanie**. Dobry kamuflaż jest potrzebny do zbierania informacji na temat osób, organizacji i innych zagadnień bez wzbudzania podejrzeń.
- **Prywatność**. Niektórzy po prostu chronią swoją prywatność poprzez rozdzielenie swojej działalności online na kilka niepowiązanych tożsamości.

Przygotowanie sceny — tworzymy własną pacynkę

Internetowa persona stworzona do ochrony anonimowości i gromadzenia informacji może być potężnym narzędziem w przypadku etycznego użycia. Konta pacynkowe są niczym cyfrowe kameleony: mogą zlać się z otoczeniem i zbierać dane OSINT bez ujawniania prawdziwej tożsamości analityka. Ta praktyka jest szczególnie cenna w przypadkach, gdy ujawnienie tożsamości mogłoby wypaczyć zdobyte informacje lub stanowić ryzyko dla bezpieczeństwa badacza.

Wyobraźmy sobie na przykład, że ekspert ds. cyberbezpieczeństwa ma za zadanie ocenić bezpieczeństwo instytucji finansowej. W etyczny sposób tworzy fikcyjne konto i dzięki temu może wejść w interakcję ze stronami phishingowymi lub potencjalnymi sprawcami, aby lepiej zrozumieć ich taktykę, bez narażania siebie i instytucji na niepotrzebne ryzyko. Przypomina to pracę policjanta pod przykrywką w cyfrowej dzielnicy. Obserwujemy i zdobywamy informacje, ale nie ingerujemy.

Dodatkowo konta pacynkowe mogą odgrywać istotną rolę w śledzeniu zagrożeń dla cyberbezpieczeństwa. Można je wykorzystać do monitorowania forów w dark webie, infiltrowania sieci cyberprzestępców oraz gromadzenia informacji na temat nadciągających zagrożeń, naruszeń czy sprzedaży ukradzionych danych. Pozwala to specjalistom z zakresu cyberbezpieczeństwa ostrzec potencjalne ofiary i wzmocnić zabezpieczenia, zanim dojdzie do szkody.

Etyczne wykorzystanie fikcyjnych kont w OSINT reguluje ścisły kodeks postępowania. Nie należy ich używać do oszustwa ani manipulacji, lecz raczej jako tarczę do ochrony

tożsamości specjalistów ds. bezpieczeństwa podczas zbierania danych potrzebnych do wzmocnienia cyfrowych zabezpieczeń. To peleryna niewidka dla pozytywnych bohaterów, dzięki której mogą obserwować i zgłaszać problemy bez znajdowania się na celowniku.

Oto kilka kwestii do rozważenia przy tworzeniu konta pacynkowego:

- Jasno określ cel fikcyjnego konta. Może to być badanie naukowe, zbieranie danych czy trening z zakresu cyberbezpieczeństwa. Zawsze miej sformułowany jasny i etyczny cel.
- Tworzenie pacynki zaczynamy od przygotowania wiarygodnej persony. Przypomina to tworzenie postaci do sztuki teatralnej. Potrzebujemy jakiejś przeszłości, zainteresowań, a także osobliwości. Narzędzia takie jak Fake Name Generator (*https://www.fakenamegenerator.com*) czy NameFake (*https://namefake.com*) to nasi najlepsi pomocnicy, jeżeli chcemy stworzyć wiarygodnie wyglądającą tożsamość.

  Oprócz imienia i nazwiska nasza pacynka potrzebuje również:

  - daty i miejsca urodzenia,
  - miejsca zamieszkania,
  - wykształcenia i zatrudnienia,
  - zainteresowań i hobby,
  - ulubionych książek, filmów i muzyki,
  - poglądów politycznych,
  - wyznania,
  - zdjęć i obrazów.

  Niektórzy nazwą te kroki **pretextingiem**.

Uwaga

Pretexting polega nie tylko na udawaniu, że jest się kimś innym. Wymyśla się również przeszłość, tło wydarzeń i wypowiedzi, aby uczynić wszystko bardziej wiarygodnym.

- Musimy dysponować zdjęciem lub awatarem persony, aby nasze fikcyjne konto wyglądało możliwie najbardziej wiarygodnie. Strona internetowa pod adresem *https://thispersondoesnotexist.com* to fantastyczne narzędzie do generowania zdjęć osób za pomocą sztucznej inteligencji (rysunek 2.10). W ten sposób nikt nie może wyszukać źródła obrazu w internecie, żeby dowiedzieć się, że go sobie od kogoś pożyczyliśmy.
- Potrzebujemy również specjalnego konta e-mailowego dla naszej persony. Możemy skorzystać z takich usług jak 10 Minute Mail (*https://10minutemail.net*), dzięki którym można stworzyć jednorazowe adresy e-mailowe wygasające po upływie określonego czasu.

Rysunek 2.10. Obraz wygenerowany przez sztuczną inteligencję (*https://thispersondoesnotexist.com*)

- Utwórzmy dla naszej pacynki również jakieś konta i profile w mediach społecznościowych.

Uwaga

Pamiętaj, że kluczem do sukcesu w tym przypadku jest konsekwencja. Ta sama persona powinna istnieć na różnych platformach.

- Korzystaj z sieci VPN (takich jak *https://www.expressvpn.com*) do zamaskowania swojego adresu IP i rozważ użycie przeglądarek, które chronią prywatność, takich jak Tor (*https://www.torproject.org*), aby utrzymać swoją prawdziwą tożsamość ukrytą za kulisami.

  Kiedyś przeprowadzał ze mną wywiad pewien reporter. Wolałem zachować anonimowość, więc zdecydowałem się użyć przeglądarki Tor, która szyfruje komunikację poprzez przekierowanie jej przez kilka serwerów z różnych części świata. Dodatkowo skorzystałem z szyfrowanego komunikatora dostępnego w dark webie. Dzięki temu mogłem bezpiecznie się z nim komunikować. Nasze rozmowy były w pełni prywatne. Nie było ryzyka namierzenia nas.

- Nie zapomnij o numerze telefonu dla swojej pacynki! Używając usługi takiej jak TextFree (*https://textfree.us*), możesz wysyłać i odbierać wiadomości tekstowe bez ujawniania swojego prawdziwego numeru telefonu. To niezłe rozwiązanie.

Nawiązywanie anonimowej komunikacji

Aby uniemożliwić powiązanie fikcyjnego konta pacynkowego z jego twórcą, niezbędne są anonimowe kanały komunikacji. Obejmuje to tworzenie niemożliwych do śledzenia adresów e-mailowych oraz przygotowanie telefonów na kartę z tymczasowymi numerami (ang. *burner phone*).

Tworząc adres e-mailowy dla pacynki, weź pod uwagę następujące kwestie:

- Unikaj nietypowych dostawców, którzy mogą wzbudzić podejrzenia.
- Używaj popularnych serwisów, takich jak Gmail czy Outlook.
- Twórz adresy z publicznych sieci wi-fi lub przez sieć VPN, aby zachować anonimowość.
- Adres e-mailowy musi wyglądać wiarygodnie i nie może składać się z przypadkowych znaków.
- Adresu e-mailowego użyjemy do rejestrowania kont, więc anonimowość jest ważna.

Telefony na kartę to ostatni element utrzymania śledztwa w tajemnicy (rysunek 2.11). Trzeba z nich jednak korzystać rozważnie. Używaj takiego telefonu jedynie do spraw bezpośrednio związanych z dochodzeniem: rozmów, wiadomości tekstowych, kodów uwierzytelniających itp.

Rysunek 2.11. Niektóre z moich telefonów na kartę, których używałem w trakcie dochodzeń

Należy też pamiętać, że w Polsce od 2017 r. nie jest możliwe korzystanie z karty SIM w usługach przedpłaconych bez rejestracji z użyciem imienia i nazwiska oraz numeru PESEL. Ogranicza to istotnie poziom anonimowości oferowany przez takie usługi.

Nigdy nie zapisuj poufnych dokumentów, nazw, dat, lokalizacji czy innych danych dotyczących sprawy na tym urządzeniu. Pamiętaj, że takie telefony nadal można podsłuchiwać, zhakować czy przejąć, pomimo że są jednorazowego użytku. W związku z tym podejmij dodatkowe środki ostrożności, a mianowicie korzystaj z komunikatorów szyfrujących wiadomości, takich jak Signal czy WhatsApp, unikaj wiązania telefonów na kartę z prywatnymi kontami, wyłącz GPS, usuń metadane z obrazów i regularnie

czyść pamięć podręczną. Używaj nazw kodowych zamiast prawdziwych do kontaktu ze źródłami.

Podczas dochodzenia OSINT odpowiedzialne zarządzanie telefonami na kartę to istotny etap w cyklu życia sprawy. Gdy dochodzenie zostaje zamknięte lub istnieją wątpliwości co do bezpieczeństwa korzystania z takiego telefonu, należy wycofać urządzenie z użytku w sposób bezpieczny i profesjonalny. Istnieją dwa dopuszczalne podejścia:

- **Odpowiedzialna archiwizacja**. Przypomina to postępowanie z innymi poufnymi materiałami po zakończeniu dochodzenia, gdzie konieczne jest utrzymywanie jasnego łańcucha dowodowego. Należy zdeponować telefon w bezpiecznym miejscu wraz z oprogramowaniem i wszelkimi innymi użytymi narzędziami. Dzięki temu mamy pewność, że zasoby, dane i potencjalne dowody znajdują się w nienaruszonym stanie i pod odpowiednim nadzorem. Nie chodzi tutaj o gromadzenie sprzętu, lecz o staranne rozdzielenie obowiązków i nienaganne utrzymywanie standardów zawodowych.
- **Staranny demontaż**. Zacznij od zresetowania urządzenia do ustawień fabrycznych, aby usunąć wszelkie dane, co jest standardową procedurą w branży. Następnie rozmontuj urządzenie. Usuń kartę SIM i zadbaj o to, aby nie nadawała się do dalszego użytku. Może to obejmować pocięcie jej na kawałki, aby zapobiec odzyskaniu danych. Jest to metoda sugerowana przez protokoły bezpieczeństwa. Dalsze rozmontowanie urządzenia, w tym oddzielenie baterii od innych podzespołów, ma zagwarantować, że żadne komponenty umożliwiające odzyskanie danych nie wpadną w niepowołane ręce. Utylizację należy przeprowadzić dyskretnie i w kilku miejscach, aby ograniczyć ryzyko odtworzenia danych.

To nie jest fragment kryminału, lecz chleb powszedni etycznego hakowania i profesjonalnego prowadzenia cyfrowych dochodzeń. Telefon na kartę to tarcza, która zarówno chroni anonimowość analityka, jak i zapewnia rzetelność jego pracy. Korzystanie z tych urządzeń, a następnie ich utylizacja, to świadectwo zawodowego zaangażowania na rzecz bezpieczeństwa i ochrony danych w dziedzinie, gdzie stawka jest zawsze wysoka.

Pamiętajmy o tym, że wszystkie kroki, jakie podejmujemy, mają na celu zwiększenie bezpieczeństwa i odkrycie podatności, zanim ktoś wykorzysta je do złych celów. Nasze praktyki są przejrzyste dla klientów i nie wykraczają poza granice prawa, dzięki czemu nasza praca jest zawsze spójna z celem ochrony zasobów i informacji w świecie, który jest w coraz większym stopniu zależny od cyfrowej infrastruktury.

Dzięki anonimowym, niepodatnym na śledzenie kanałom komunikacji nie będzie możliwe powiązanie kont pacynkowych z ich twórcami. Konta te będą żyć własnym życiem, gwarantując prywatność i kamuflaż, które mają kluczowe znaczenie w pracy analityka OSINT.

Pociągając za sznurki — agent Pacyna w akcji

Teraz, gdy nasza pacynka jest gotowa pojawić się na cyberscenie, musimy pamiętać o kilku zasadach etyki:

- **Transparentność wobec interesariuszy**. Jeżeli używamy fikcyjnych kont w działalności badawczej lub kontroli w ramach przedsiębiorstwa, musimy zachować transparentność wobec interesariuszy na temat metod i intencji.
- **Ochrona danych**. Bądźmy czempionami ochrony danych. Zbierajmy tylko te dane, które są niezbędne do prowadzenia dochodzenia, i podchodźmy do nich z najwyższą odpowiedzialnością.
- **Dokumentowanie i sprawozdania**. Należy prowadzić szczegółowy rejestr czynności wykonywanych z fikcyjnych kont. To nie tylko ułatwia prezentację wyników, lecz również zapewnia rozliczalność z przeprowadzonych działań.

Wykorzystanie dynamiki płci w działaniach z fikcyjnych kont

Na cybernetycznej scenie wywiadowczej zbudowanie swojego cyfrowego alter ego jest w połowie sztuką, a w połowie nauką i wymaga umiejętnego balansowania na etycznej linie rozciągniętej nad cyfrowym światem, zwłaszcza jeżeli chodzi o dynamikę płci. Tak, internet pełen jest stereotypów na temat płci, ale kiedy tworzymy personę, musimy podchodzić do tych uogólnień z ostrożnością.

Wyobraźmy sobie, że wybraliśmy żeńską postać jako swój kamuflaż. To prawda, że bycie kobietą może okazać się pomocne w niektórych sytuacjach ze względu na sposób, w jaki ludzie prowadzą interakcje społeczne. Pamiętajmy jednak, że nie jesteśmy tutaj po to, aby kogoś oszukiwać dla przyjemności. Musimy działać inteligentnie, a nie podstępnie. Możemy na przykład posłużyć się metodą „na wabia", zachowywać się odrobinę zalotnie i bezradnie, aby zdobyć uwagę celu. W takich przypadkach należy jednak zdecydowanie pamiętać o tym, aby działać etycznie. Chodzi o gromadzenie informacji w sprytny sposób, a nie o zwodzenie lub wykorzystywanie innych.

Gdy chcemy stworzyć wiarygodne konto typu *sock puppet*, diabeł tkwi w szczegółach. Dajmy sobie spokój z powielaniem stereotypów i wyposażmy naszą pułapkę w prawdziwą osobowość. Kilka niepowtarzalnych cech sprawi, że pacynka stanie się czymś więcej niż zbiorem pikseli — zyska głębię i wiarygodność, które mogą wzbudzić zaufanie tam, gdzie to najbardziej potrzebne.

Uwaga

Oto kilka profesjonalnych porad. Całkowicie odseparuj życie swojego fikcyjnego „ja" od życia prywatnego. Używaj maszyn wirtualnych, przeglądarek w trybie piaskownicy i tym podobnych rozwiązań. Mieszanie tych dwóch bytów to jak założenie skarpet do sandałów. Tak się po prostu nie robi. Dzięki temu mamy solidną przykrywkę oddzieloną grubym murem od naszej prawdziwej tożsamości.

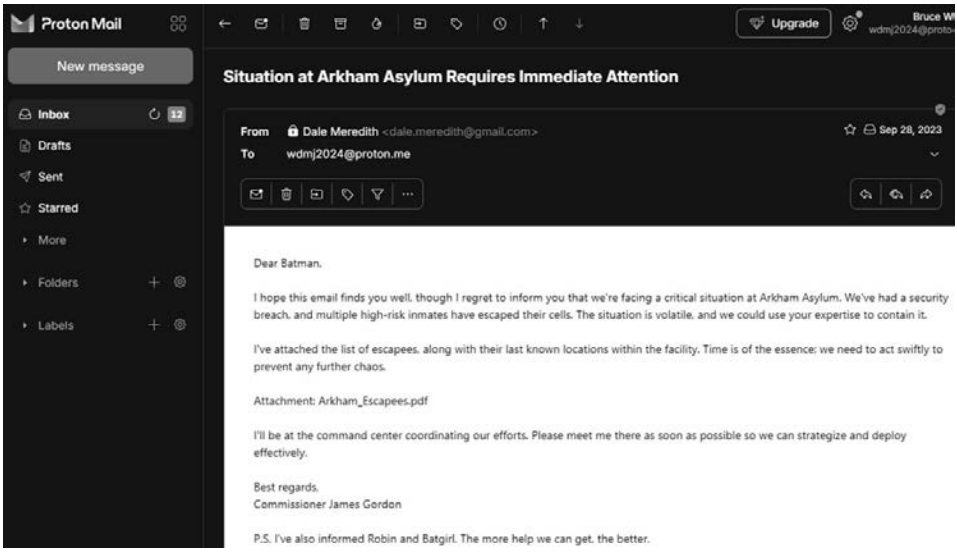
Gdy działamy w słusznej sprawie, te wszystkie pacynkowe akrobacje są jak najbardziej uzasadnione. To sprawdzony sposób na infiltrację podejrzanych cyfrowych klik, wykrywanie cyberzagrożeń, udawanie żółtodzioba we własnej firmie czy sprawdzenie, kto złapie się na phishingową przynętę. Przywdziewamy cybernetyczną pelerynę niewidkę i używamy swoich supermocy w służbie dobra.

Podsumowując: działajmy mądrze i etycznie. Pamiętajmy, że mamy zwalczać przestępców, a nie dołączyć do ich szeregów.

Anonimowe e-maile i wiadomości tekstowe

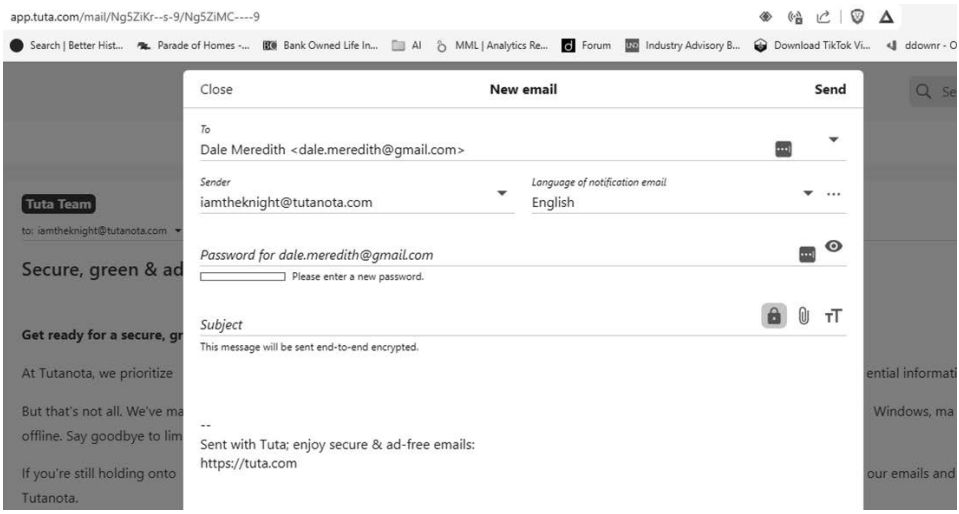
Korzystanie z anonimowych adresów e-mailowych to sprawa najwyższej wagi dla analityków OSINT, którzy pragną ukryć swoją tożsamość i zachować anonimowość w interakcjach online. Adresy e-mailowe często stanowią wrota do prawdziwej tożsamości danej osoby, gdyż dostarczają różnych wskazówek i ujawniają powiązania. Bez dbałości o anonimowość badacze OSINT ryzykują wyciekiem swoich danych osobowych, np. jeżeli ich adres e-mailowy zostanie powiązany z forami, usługami czy mediami społecznościowymi użytymi w ramach dochodzenia. Może to narazić badaczy na ataki hakerskie, nękanie poprzez publikowanie informacji na ich temat (ang. *doxing*), zemstę czy niepożądane powiązania z różnymi grupami i ruchami.

Tworzenie adresów e-mailowych w żaden sposób nie powiązanych z danymi identyfikującymi analityka OSINT ma kluczowe znaczenie dla bezpieczeństwa i prywatności. Z anonimowych adresów e-mailowych nigdy nie należy korzystać do realizowania działań, które mogłyby prowadzić do ujawnienia danych osobowych. Nie może to być adres zarejestrowany w mediach społecznościowych, portalach zawodowych takich jak LinkedIn, sklepach internetowych itd. Użycie odpowiedniej usługi, takiej jak Proton Mail (*https://protonmail.com*), byłoby najlepszym rozwiązaniem (rysunek 2.12).



Rysunek 2.12. Usługa Proton Mail pomaga w ukryciu prawdziwej tożsamości

Inną usługą, z której można skorzystać, jest Tuta (*https://tuta.com*). Do utworzenia konta nie są wymagane żadne prawdziwe dane osobowe (rysunek 2.13).



Rysunek 2.13. Anonimowe konto e-mailowe Tuta

Korzystanie ze specjalnie założonych anonimowych adresów e-mailowych pozwala analitykom OSINT rejestrować się na forach, zadawać pytania i prowadzić rozmowy bez obaw o bezpieczeństwo ich prawdziwej tożsamości. To istotna linia obrony przed utratą anonimowości.

Aktualizowanie wiedzy na temat cyberzagrożeń

Prowadzenie dochodzeń OSINT jest nierozłącznie powiązane z ryzykiem dla cyberbezpieczeństwa. Zachowanie prywatności i anonimowości w internecie to fundamentalne zasady etycznego białego wywiadu. Dlatego zajmujące się nim osoby nie mogą sobie pozwolić na to, aby zostać w tyle za nowymi zagrożeniami technologicznymi. Muszą na bieżąco śledzić nowinki w dziedzinie bezpieczeństwa, uczyć się na cudzych błędach i doskonalić warsztat.

Uzyskiwanie bieżących informacji na temat prywatności i bezpieczeństwa

Monitorowanie wiadomości z zakresu cyberbezpieczeństwa i prywatności pomaga zrozumieć stale zmieniający się profil ryzyka. Zasubskrybuj serwis monitorujący zagrożenia, taki jak jeden z tutaj wymienionych, aby otrzymywać powiadomienia na temat nowych podatności i ataków:

- newsletter ze strony Cybersecurity Threats organizacji Center for Internet Security (CIS) (*https://www.cisecurity.org/cybersecurity-threats*),

- biuletyny Agencji ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury Stanów Zjednoczonych (ang. *Cybersecurity and Infrastructure Security Agency*, CISA) (*https://www.cisa.gov/news-events/bulletins*).

Osobiście polecam biuletyny CISA. Nie tylko nie faworyzują żadnego z dostawców, lecz również są niezwykle drobiazgowe (rysunek 2.14).

Rysunek 2.14. Biuletyny CISA

Jeżeli chcesz być asem cyberbezpieczeństwa, polecam też lekturę branżowych blogów i serwisów informacyjnych, takich jak te:

- *Krebs on Security* (*https://krebsonsecurity.com*),
- *Privacy News* (*https://www.privateinternetaccess.com/blog*),
- *SCHMOOZE OSINT* (*https://www.sangoma.com*).

Dzięki tym zasobom będziesz mieć aktualne informacje o tym, co się dzieje w tej branży.

Należałoby również przysłuchiwać się, co mówią najważniejsze osobistości w dziedzinie bezpieczeństwa informacji w mediach społecznościowych, i w miarę możliwości brać udział w konferencjach, takich jak DEF CON, Black Hat czy BSides.

Uczenie się na podstawie wcześniejszych naruszeń i incydentów

Analizowanie już zakończonych dochodzeń w sprawie dużych naruszeń może owocować ważnymi spostrzeżeniami. Atak na LinkedIn z 2016 r. (*https://www.forbes.com/sites/daveywinder/2024/01/23/massive-26-billion-record-leak-dropbox-linkedin-twitterx-all-named/?sh=2ab1fc93ab58*) pokazuje, w jaki sposób dane ukradzione stronie trzeciej uruchomiły lawinę powiązanych ataków. Kampanie doxingu i innych form prześladowania przeciwko znanym osobom, takie jak Gamergate (*https://www.nytimes*

.com/interactive/2019/08/15/opinion/what-is-gamergate.html), rzucają nieco światła na rzeczywiste szkody, jakie może wyrządzić OSINT, jeżeli użyjemy go jako broni. Badanie praktyk samozwańczych detektywów uwidacznia również ryzyka, związane między innymi ze stosowaniem zabiegów socjotechnicznych, których etyczna praktyka OSINT powinna unikać.

Podsumowanie

Solidne zabezpieczenia własnej anonimowości stanowią pierwszą linię obrony analityka OSINT. Regularnie wyszukuj swoje imię i nazwisko online, aby ocenić swój cyfrowy ślad i usunąć wszelkie wycieki danych osobowych. Korzystaj z narzędzi takich jak przeglądarka Tor, wirtualne numery telefonów i anonimowe konta e-mailowe, aby zabezpieczyć swoją prawdziwą tożsamość. Postaw grubą kreskę między różnymi tożsamościami. Używaj oddzielnych urządzeń i kont do działań OSINT. Uczyń z nieustannego podnoszenia swoich kompetencji w dziedzinie prywatności priorytet — co chwilę bowiem mamy do czynienia z nowymi zagrożeniami.

Etyczni analitycy OSINT potrafią zagwarantować sobie osobiste bezpieczeństwo i prowadzić badania bez zbędnego ryzyka dzięki ostrożności w tym zakresie. Zagrożenia stale ewoluują, więc nie możemy spocząć na laurach, jeżeli nie chcemy pozostać w tyle. Na tym zakończymy na razie temat anonimowości, a za chwilę przedstawię metody i techniki, które mamy do dyspozycji podczas dochodzeń OSINT.

Dołącz potężne narzędzia OSINT do swojego arsenału!

Pojęcie OSINT pochodzi od angielskiego wyrażenia *open source intelligence* i oznacza biały wywiad. Polega na pozyskiwaniu danych z publicznie dostępnych źródeł. Okazuje się, że niezwykle cenne informacje są dostępne na wyciągnięcie ręki, ale trzeba wiedzieć, w jaki sposób do nich dotrzeć. A potrafi to być niezwykle wciągające zajęcie, przy okazji którego można poznać podstawy cyberbezpieczeństwa, zrozumieć czyhające w internecie zagrożenia i nauczyć się zabezpieczać swoją cyfrową obecność.

Z tą książką krok po kroku zagłębisz się w metody OSINT, a także powiązane z nim zagadnienia natury prawnej i etycznej. Poznasz sposoby gromadzenia i analizowania informacji z wykorzystaniem wyszukiwarek, portali społecznościowych i innych zasobów internetowych. Zrozumiesz wagę anonimowości i technik gwarantujących bezpieczne poruszanie się po sieci, ułatwiających zarządzanie cyfrowym śladem czy tworzenie fikcyjnych tożsamości internetowych. Zdobędziesz również doświadczenie w korzystaniu z popularnych narzędzi OSINT, takich jak Recon-ng, Maltego, Shodan czy Aircrack-ng. Dowiesz się też, jak ograniczać ryzyko, przewidywać cyberataki, zapobiegać im i na nie reagować — wszystko dzięki technikom opartym na OSINT.

W książce:

- działanie OSINT i najlepsze praktyki
- automatyzacja zbierania i analizy danych
- dane z mediów społecznościowych a OSINT
- zarządzanie swoim cyfrowym śladem, ograniczanie ryzyka i ochrona prywatności
- skuteczny program analizy ryzyka na bazie OSINT
- zwiększanie bezpieczeństwa firmy technikami OSINT

Dale Meredith jest hakerem i certyfikowanym trenerem Microsoftu, jego znak rozpoznawczy to angażujący, zapadający w pamięć styl uczenia. Był instruktorem firm z rankingu Fortune 500, wykładowcą na wielu uczelniach na świecie, a także pracownikiem Departamentu Bezpieczeństwa Krajowego i innych departamentów wojskowych Stanów Zjednoczonych.

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-2042-2
9 788328 920422
Cena: 67,00 zł
packt