https://doi.org/10.34836/pk.2022.316.2

Unikanie rejestrowania czynności użytkownika: TOR, Linux Tails

podkom. Sylwester Panasewicz[1]

[1] Laboratorium Kryminalistyczne Komendy Wojewódzkiej Policji w Białymstoku, sylwester.panasewicz@bk.policja.gov.pl

Streszczenie

Sieć TOR (The Onion Router) jest wirtualną siecią komputerową zapewniającą anonimizację oraz dostęp do często nielegalnych danych lub dla unikających cenzury. Linux Tails (The Amnesic Incognito Live System) stanowi natomiast system operacyjny bootowany wyłącznie z nośnika przenośnego (np.: pendrive, karty pamięci czy też płyty DVD) lub uruchamiany w sposób zwirtualizowany. Tails jako jedno z narzędzi oferuje dostęp do sieci TOR, zapewniając ponadto dalece wyszukane mechanizmy służące do unikania pozostawienia śladów cyfrowych na maszynie, z której korzysta użytkownik. Mimo innych intencji twórców obu omawianych powyżej narzędzi stały się one ulubionym pakietem olbrzymiej grupy przestępców na całym świecie. Autor w niniejszej publikacji skupia się na omówieniu zarówno obszarów powstawania śladów cyfrowych użytkowania TOR oraz Tails, jak i na możliwościach badawczych oraz możliwościach wnioskowania na ich podstawie. W pierwszej części artykułu opisany został mechanizm działania anonimizującej sieci TOR. Następnie autor zapoznaje czytelnika ze środowiskiem Linux Tails oraz odnosi się do faktycznych przypadków użycia.

Słowa kluczowe: anonimizacja, TOR, Tails, Linux, trasowanie, wirtualny

Jeszcze niedawno sen z oczu włamywacza spędzał problem, w jaki sposób pozostawić możliwie niewiele śladów na miejscu przestępstwa. Dziś, w dobie cyfrowej, sprawcy korzystają z różnorodnych narzędzi, by uzyskać nieuprawniony dostęp, fałszywą tożsamość lub dokonać innych działań, praktycznie nie pozostawiając śladów innych niż cyfrowe. Próbują ukryć się w cieniu zwykłego ruchu sieciowego, maskują swoją działalność, szyfrują dane stanowiące dowody cyfrowe. Niekiedy mogą wręcz powrócić na miejsce przestępstwa i kontynuować zacieranie śladów lub weryfikować ich istnienie bez wiedzy organów ścigania. Choć idea sieci anonimizujących czy elastycznych systemów operacyjnych typu live nie powstała z myślą o świecie przestępczym, jej owoce coraz częściej stają się takimi narzędziami. Skłoniło to autora do opisania w niniejszym artykule systemu operacyjnego Linux Tails, w charakterze narzędzia i zawartych w nim programów anonimizujących m.in. korzystających z sieci TOR, w kontekście kryminalistycznych badań informatycznych. Trzeba pamiętać jednak, że tego typu narzędzia są używane również m.in. przez ludzi żyjących w systemach autorytarnych lub osoby chcące zachować swoją prywatność. Czytelnicy, którzy mieli okazję zapoznać się z książką *Pamięć nieulotna* autorstwa Edwarda Snowdena, wiedzą, że podczas jego pracy dla NSA w kontakcie z prasą korzystał z systemu operacyjnego Tails. I co najważniejsze – nie został na tym przyłapany, co stanowi szczególną rekomendację.

Sieć TOR (The Onion Router) jest wirtualną siecią komputerową, w której zaimplementowano trasowanie cebulowe drugiej generacji, co zapobiega analizie ruchu sieciowego i zapewnia jej użytkownikom prawie anonimowy dostęp do zasobów Internetu.

Projekt TOR był początkowo sponsorowany przez laboratoria badawcze Marynarki Wojennej Stanów Zjednoczonych (U.S. Naval Research Laboratory) i rozwijany jako projekt militarny w celu ochrony komunikacji wywiadowczej USA w Internecie. Miał maskować działalność agentów wywiadu w sieci.

Inicjatorami sieci TOR byli programiści Roger Dingledine, Nick Mathewson oraz Paul Syverson, którzy przy wsparciu Centrum Badawczego Marynarki Wojennej USA rozpoczęli w 2002 r. pracę nad projektem. W 2004 roku na 13. Sympozjum Bezpieczeństwa Stowarzyszenia USENIX przedstawili pracę *Tor: The Second-Generation Onion Router*. W czasie od końca 2004 r. do listopada 2005 r. stał się on projektem

firmowanym przez Electronic Frontier Foundation (EFF). Obecnie rozwojem oprogramowania TOR zajmuje się Tor Project – niedochodowa organizacja non-profit o charakterze badawczo-edukacyjnym z siedzibą w Stanach Zjednoczonych, wspomagana przez wolontariuszy i użytkowników sieci na całym świecie. Projekt aktualnie funkcjonuje na licencji BSD, ale cały czas jest pośrednio sponsorowany przez Marynarkę Wojenną Stanów Zjednoczonych (Mider, 2019).

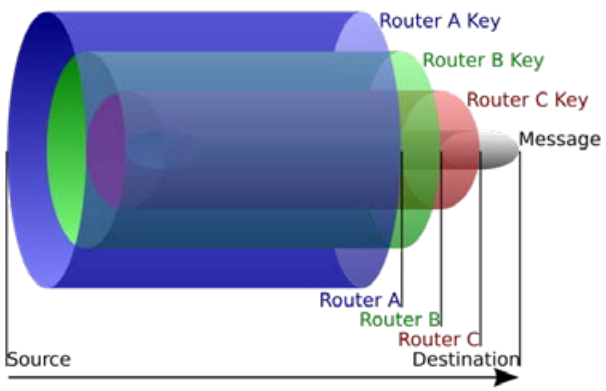
The Onion Router został udostępniony do użytku cywilnego w 2003 r. Serwery tworzące sieć TOR w początkowym okresie jej działania były umiejscowione jedynie w Stanach Zjednoczonych oraz Niemczech.

Nazwa sieci TOR jest skrótem od The Onion Router (router cebulowy). Pochodzi od techniki polegającej na wysyłaniu niezależnych i wielowarstwowo szyfrowanych pakietów, stąd określenie „trasowanie cebulowe". Tworzące tę sieć urządzenia realizują proces zwany trasowaniem cebulowym, odmiennym od klasycznego trasowania przez routery wykorzystujące model TCP/IP (Mider, 2019; Casad, 2017).

W sieci TOR dane są wysyłane zaszyfrowanymi warstwami, analogicznie do warstw cebuli. Zaszyfrowane w ten sposób dane są przesyłane przez serię węzłów sieciowych (routery cebulowe, ang. *onion routers*), z których każdy usuwa („odrywa") pojedynczą warstwę, odsłaniając kolejny cel przesyłanych danych. Gdy ostatnia warstwa zostanie odszyfrowana, dane docierają do miejsca docelowego. Nadawca pozostaje anonimowy, ponieważ każdy węzeł zna tylko lokalizację bezpośrednio poprzedzających i następujących węzłów. Router w każdej warstwie „wie" tylko to, co jest mu niezbędne do działania. Adresy IP wszystkich zapytań i odpowiedzi zmieniają się w każdym węźle (Ortega, 2022).

Trasowanie cebulowe jest strukturą danych utworzoną przez enkapsulowanie („zawijanie") danych w kolejne warstwy szyfrowania, które mogą być odszyfrowane przez tyle komputerów pośredniczących, ile jest warstw, zanim dotrą do miejsca docelowego. Połączenia pomiędzy każdym węzłem (serwerem proxy) jest szyfrowane. Pierwotne dane (i ich nadawca) pozostają ukryci, ponieważ dane są przesyłane pomiędzy węzłami pośrednimi, a żaden pośredni węzeł nie „zna" zarówno miejsca pochodzenia, jak i miejsca docelowego danych, dzięki czemu nadawca pozostaje anonimowy. Obserwacja takiego ruchu sieciowego nie pozwala stwierdzić, co jest w nim przesyłane.

Sieć TOR zapewnia anonimowość z wykorzystaniem protokołu TCP przy stosunkowo małym opóźnieniu i wysokiej przepustowości. Mechanizmy zaimplementowane w protokole sieci TOR nakładają warstwę anonimowości na warstwę TCP i tworzą ścieżkę (domyślnie minimum) trzypunktową, przez którą routery sieci TOR szyfrują warstwowo. Informacja o trasach jest przesyłana przez grupę autorytatywnych serwerów. W uproszczeniu: cała komunikacja TCP użytkownika jest tunelowana w jednym węźle, rotującym w czasie, a w celu zapewnienia niskich opóźnień sieć TOR nie wymusza retransmisji zgubionych pakietów.



Ryc. 1. Mechanizm trasowania cebulowego: źródło wysyła dane do routera A, który usuwa warstwę szyfrowania, aby dowiedzieć się tylko, gdzie wysłać je dalej i skąd pochodzą (chociaż nie „wie", czy nadawca jest źródłem, czy tylko innym węzłem). Router A wysyła je do routera B, który odszyfrowuje kolejną warstwę, aby poznać następne miejsce docelowe danych. Router B wysyła dane do routera C, który usuwa ostatnią warstwę szyfrowania i przesyła oryginalną wiadomość do miejsca przeznaczenia

Z perspektywy prywatności sieć TOR ma dwa cele:

1. Ukrywanie lokalizacji użytkowników korzystających z Internetu – wyśledzenie używanych przez nich adresów IP i lokalizacji ma być niemożliwe.
2. Szyfrowanie przesyłanych danych – sieć TOR szyfrując dane i przesyłając je routingiem cebulowym, ukrywa adresy IP użytkowników i przesyłane dane oraz ukrywa adresy IP operatorów ISP, poprzez których użytkownicy łączą się z siecią TOR (Ortega, 2022).

Węzły tworzące sieć TOR mają różne zadania i w zależności od charakterystyki i konfiguracji, rozróżniamy:

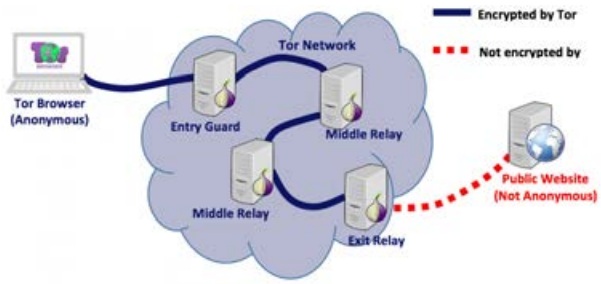
1. Węzły strażnicze (ang. *guard relays*) – komunikujące się z użytkownikami, połączone z resztą sieci TOR. Wykorzystywane od długiego czasu. Mają duże przepustowości.
2. Węzły przekaźnikowe (ang. *middle relays*) – komunikujące się wyłącznie z innymi węzłami. Dane, które z nich wychodzą, nie opuszczają sieci TOR.
3. Węzły wyjściowe (ang. *exit relays*) – punkty końcowe (brzegowe) sieci TOR. Odbierają żądania,

przesyłają je do odbiorców, odbierają odpowiedzi i wysyłają je w sieć w kierunku nadawcy.

4. Węzły pomostowe (ang. *bridge relays*) – będące węzłami, o których nie ma informacji w jawnym katalogu węzłów sieci TOR, które znacznie trudniej jest zablokować. Korzysta się z nich, gdy operator ISP blokuje sieć TOR. Lista ta jest dostępna na stronie https://bridges.torproject.org (Ortega, 2022).

Korzystanie z sieci TOR wygląda następująco:

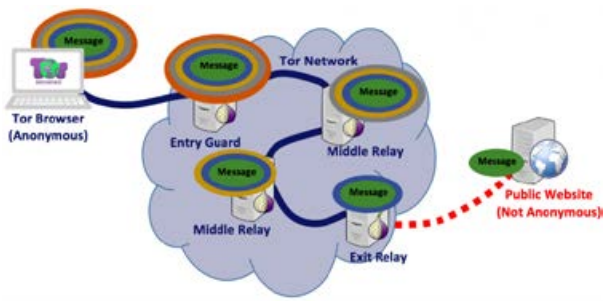
1. Host łączący się z siecią TOR pobiera listę dostępnych węzłów i wybiera trzy z nich: strażniczy, przekaźnikowy i wyjściowy.
2. Dane przeznaczone do wysłania przez sieć TOR są najpierw szyfrowane. Tylko węzeł wyjściowy zna adres żądanej usługi sieciowej i ma wgląd w przesyłane pakiety danych, ale ich pochodzenie nie jest mu znane, co zapewnia prywatność użytkownikowi.
3. Zaszyfrowane dane są ponownie szyfrowane i tylko węzeł przekaźnikowy wie, do którego węzła wyjściowego ma je przesłać. Dzięki podwójnemu szyfrowaniu tylko węzeł strażniczy wie, gdzie znajduje się węzeł przekaźnikowy (Ortega, 2022).



Ryc. 2. Diagram pokazujący typowy scenariusz działania klienta sieci TOR uzyskującego dostęp do publicznej strony w sieci Internet

Dane są szyfrowane, zanim opuszczą komputer użytkownika:

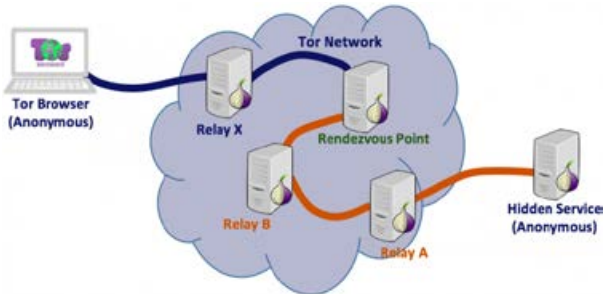
1. Jeśli istnieje system monitorujący połączenie internetowe (może to zrobić ISP), widzi on tylko zaszyfrowane dane wymieniane z węzłem strażniczym.
2. Tylko węzeł strażniczy widzi IP użytkownika i wie, gdzie znajduje się węzeł przekaźnikowy.
3. Tylko węzeł przekaźnikowy wie, gdzie są węzły strażniczy i wyjściowy. Nie wie jednak, gdzie jest użytkownik ani żądana strona internetowa (lub inna usługa sieciowa). Węzły przekaźnikowe nie znają swoich miejsc w sieci.
4. Węzeł wyjściowy wie, gdzie jest żądana strona internetowa (lub inna usługa sieciowa) i węzeł przekaźnikowy. Ale nie wie, gdzie jest użytkownik i węzeł strażniczy (Ortega, 2022).



Ryc. 3. Diagram pokazujący jak wiadomość będzie podróżować poprzez sieć TOR dopóki nie dotrze do publicznej witryny internetowej. Klient sieci TOR (przeglądarka Tor Browser) dodaje tyle warstw, ile jest przekaźników w łańcuchu

Niektóre sieci blokują ruch wychodzący na porcie TCP 9050 używanym przez sieć TOR, a nawet dynamicznie wciągają na czarną listę wszystkie węzły sieci TOR, uniemożliwiając korzystanie z tej sieci. Ograniczenie to można ominąć, używając tzw. mostków sieciowych, czyli węzłów sieci TOR niewidocznych w publicznym katalogu sieci (Allsopp, 2017).

Oprócz łączenia się z usługami w Internecie sieć TOR umożliwia korzystanie z tzw. ukrytych usług (*hidden services*), świadczonych na całkowicie anonimowych serwerach sieciowych zamkniętych w ekosystemie sieci TOR i widocznych tylko w niej, które korzystają z własnego rozproszonego systemu adresowania (Allsopp, 2017).



Ryc. 4. Diagram przedstawiający mechanizm uzyskiwania dostępu do serwera WWW ukrytego w sieci TOR (ukrytej usługi): (1) jeden serwer Tor Relay (przekaźnik) zostanie wybrany jako (przekaźnik) Rendezvous Point; (2) tworzone są dwa połączenia: jeden od klienta sieci Tor do węzła Rendezvous Point, a drugi od ukrytego serwera w sieci Tor do węzła Rendezvous Point. Autor uważnemu czytelnikowi pozostawia pod rozwagę, czy Hidden Service na powyższym diagramie nie powinien być objęty obszarem obrazowej chmury Tor Network

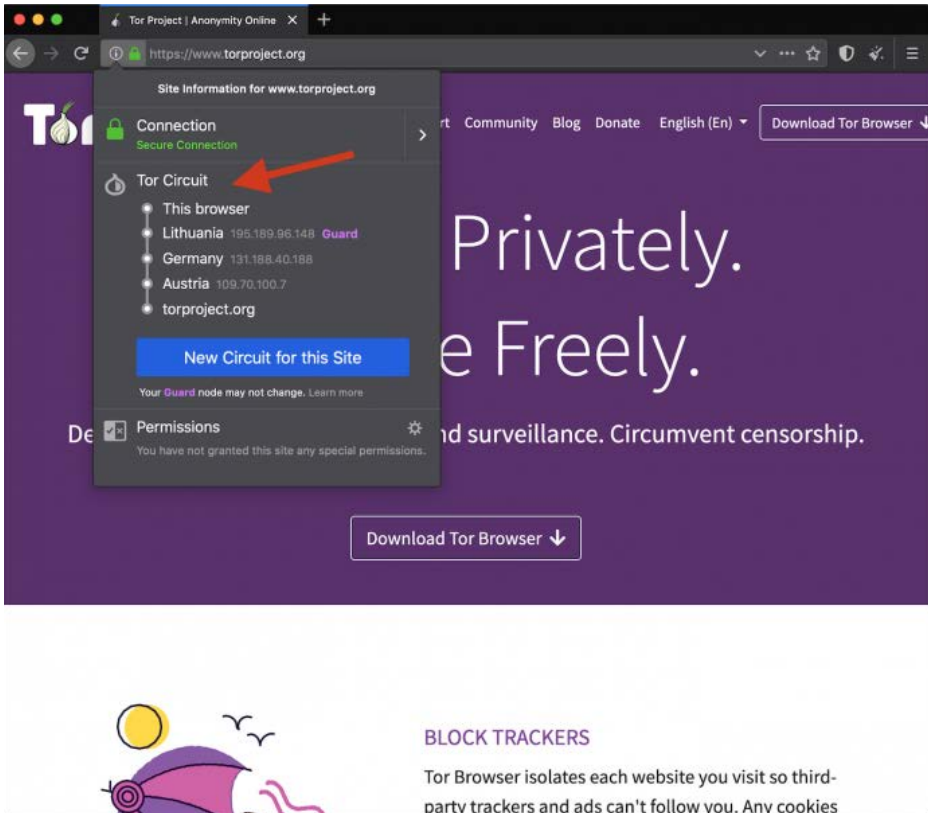
W przeciwieństwie do zwykłych stron internetowych, do których uzyskuje się dostęp za pomocą ich adresów URL, dostęp do ukrytych usług uzyskuje się za pomocą specjalnego typu adresów *onion*, zawierających losowy, niemnemoniczny ciąg znaków i niebędących

częścią typowego systemu DNS w Internecie. Losowe znaki w adresie witryny w sieci TOR (np.: https://zqktlwi-4fecvo6ri.onion/wiki/index.php/Main_Page) dodatkowo utrudniają znalezienie odpowiedniej witryny – dostęp mają osoby, które wiedzą, jak ich szukać.

Najpopularniejszym programem do przeglądania sieci TOR jest Tor Browser Bundle, który jest zintegrowany z przeglądarką internetową Mozilla Firefox. Program zapewnia ochronę użytkownikowi, jeśli korzysta on wyłącznie z wbudowanej przeglądarki Firefox. Po połączeniu z siecią TOR można swobodnie przeglądać strony internetowe, a także prowadzić rozmowy za pomocą komunikatorów. Program ma ogromną ilość różnych opcji konfiguracyjnych, za pomocą których możemy ustawić połączenie z siecią TOR i ustanowić nowe połączenie TCP, wpisując inny adres IP. Przeglądarka Tor Browser zapewnia bezpieczeństwo na trzech poziomach, a każdy z nich możemy w każdym momencie samodzielnie ustawić. Poziomy te to: *standardowy* (wszystkie funkcje przeglądarki TOR i stron są włączone); *bezpieczniejszy* (obsługa skryptów JavaScript na stronach bez HTTPS jest wyłączona, podobnie niektóre czcionki i symbole, media HTML5 (audio i video) uruchamiają się dopiero po naszym kliknięciu) oraz *najbezpieczniejszy* (ustawienie HTML5 jak wyżej, a także domyślnie wyłączony JavaScript na wszystkich stronach, tak samo niektóre czcionki, symbole i obrazki).

Jak można się dowiedzieć z powyższej analizy działania sieci wirtualnej Tor, do jej obsługi niezbędne jest specjalistyczne oprogramowanie. Bezpieczeństwo użytkownika wzrasta, gdy działa ono w środowisku minimalizującym powstawanie artefaktów cyfrowych. Najlepszym takim środowiskiem jest system operacyjny, który działa, opierając się wyłącznie na pamięci operacyjnej komputera lub systemie wirtualnym. Opisany w dalszej części artykułu system Tails nie jest jedyną dystrybucją Linux przeznaczoną do podobnych celów. Wśród popularnych można wymienić także: Qubes OS, minimalistyczny Alpine Linux, IprediaOS, Whonix oraz Kodachi Linux, jednakże autor skupił się na omawianej dystrybucji z uwagi na jej popularność w przekazywanym do badań materiale dowodowym.

The Amnesic Incognito Live System, czyli w skrócie TAILS, to oparta na Debianie i środowisku graficznym Gnome dystrybucja Linux przeznaczona wyłącznie do użytkowania w formie Live USB, Live DVD lub dla środowiska wirtualnego. Pierwsza wersja tego systemu operacyjnego została stworzona w 2009 przez deweloperów „The Tails project" z myślą o bezpieczeństwie, zachowaniu prywatności i anonimowości użytkownika. Do wersji 5.2 z 12 lipca 2022 roku, której funkcjonalności w tej części artykułu zostaną omówione (autor skupia się w swoim opracowaniu na funkcjonalnościach szczególnie istotnych dla cyfrowej analizy śledczej, w związku



Ryc. 5. Okno przeglądarki Tor Browser z widocznymi adresami węzłów sieci TOR oraz opcjami zmiany obwodu

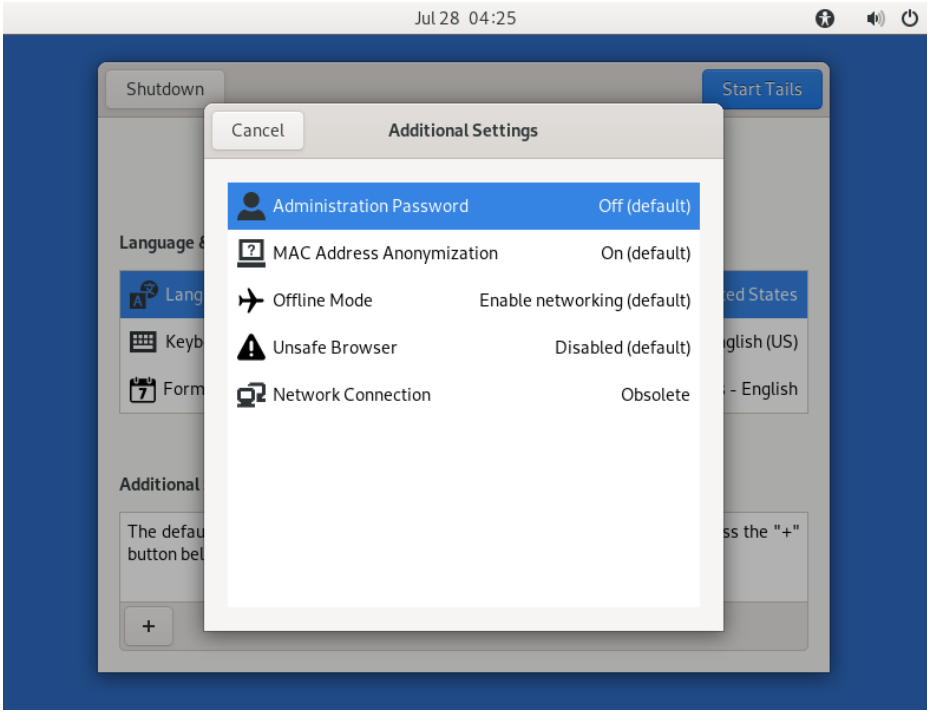
z tym nie zawiera ono pełnego opisu systemu Linux Tails 5.2), projekt przeszedł imponującą ewolucję, która znacząco wpływała również na *modus operandi* użytkujących go przestępców. Szczególnie istotna, z punktu widzenia informatyka śledczego, wydaje się ewolucja polityki twórców systemu dotyczącej metod dostępu do obszaru udostępnionego dla zapisu danych.

Aktualnie według dystrybutora TAILS jest systemem skierowanym do użytkowników takich jak: aktywiści, dziennikarze oraz ich źródła, osoby doświadczające nadmiernej kontroli w swoim środowisku oraz wszelkie osoby potrzebujące prywatności w świecie cyfrowym. Jest to oprogramowanie darmowe na licencji GNU/GPL, zatem źródłem finansowania wspomnianej grupy deweloperów są m.in. sponsorzy, wśród których szczególnie znamienna jest obecność organizacji takich jak: U.S. Department of State (powyżej 100 000 dolarów); ProtonMail, RIPE NCC (po 50 000–99 999 dolarów) czy też TOR.

Omawiany system operacyjny do działania potrzebuje 64-bitowego procesora oraz co najmniej 2 GB pamięci operacyjnej a producent deklaruje kompatybilność z większością komputerów osobistych produkowanych po 2006 roku. Jak wspomniano wcześniej, uruchamiany jest na komputerze przy użyciu nośnika USB lub płyty DVD z pominięciem użycia rodzimego systemu operacyjnego, gwarantując jednocześnie dostęp do zamontowanych nośników pamięci w trybie jedynie „do odczytu". Już na tym etapie działania użytkownika nie powstają na komputerze artefakty wskazujące na użycie TAILS, ponieważ jedynym niestandardowym poleceniem podczas rozruchu jest skorzystanie z interfejsu wyboru nośnika bootowania i, jak potwierdza praktyka autora artykułu, na większości testowanych oraz przedstawionych do badań w toku realizacji postanowień o powołaniu dowodu z opinii biegłego urządzeń operacja ta nie wymaga trwałej modyfikacji ustawień systemu BIOS.

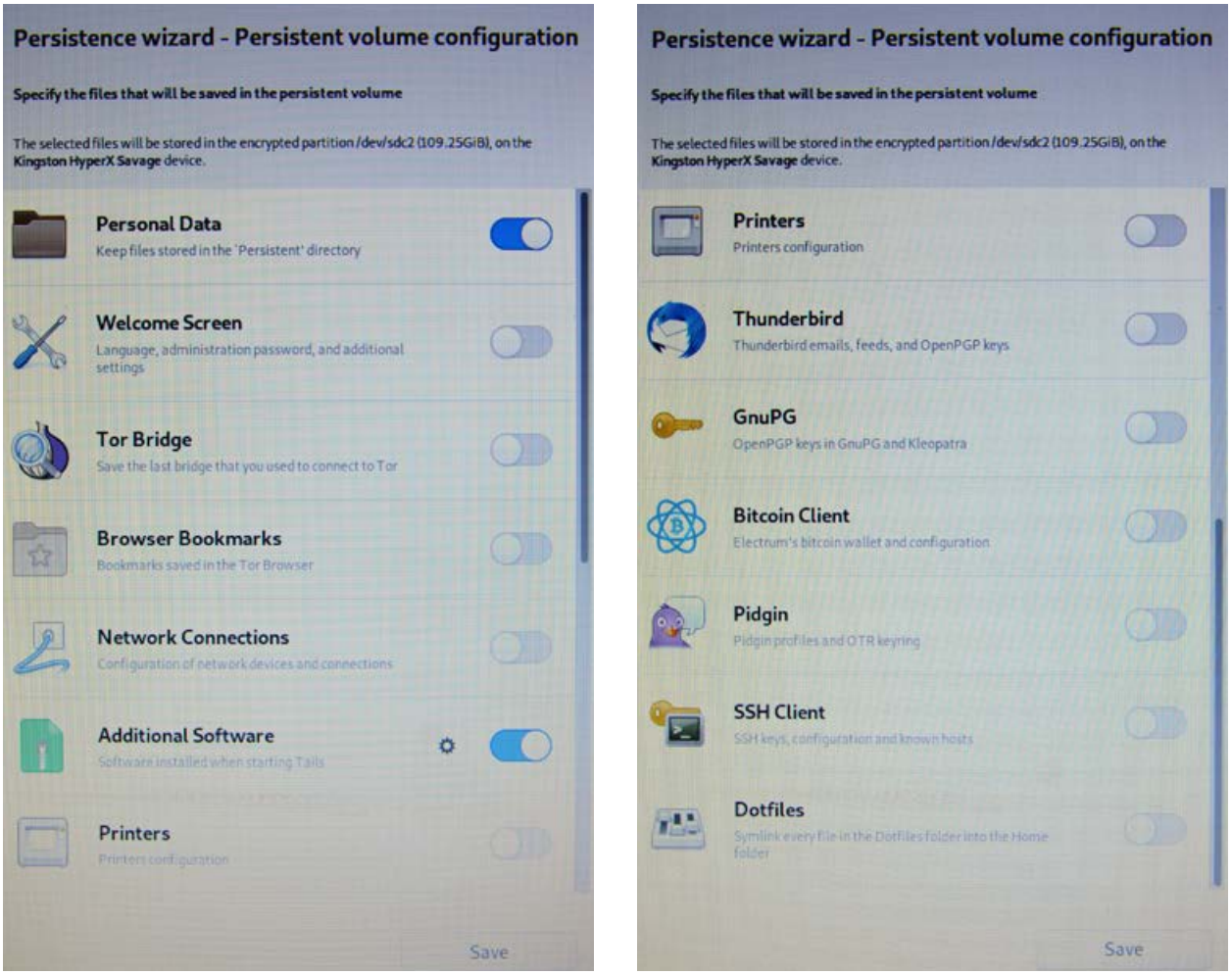
Po wybraniu standardowego trybu uruchomienia użytkownik ma możliwość prekonfiguracji parametrów, m.in. wpływających istotnie na bezpieczeństwo.

Do ustawień tych należy możliwość określenia hasła administracyjnego. Pominięcie tego kroku znacząco ogranicza pewne funkcjonalności, dając jednocześnie mniej zaawansowanemu użytkownikowi większą gwarancję uniknięcia powstania artefaktów o charakterze dowodu cyfrowego. Kolejnymi opcjami prekonfiguracyjnymi, o których warto wspomnieć, są: możliwość automatycznego anonimizowania adresu fizycznego MAC interfejsów sieciowych, wymuszony tryb offline, udostępnienie funkcji tzw. Unsafe Browser, czyli przeglądarki internetowej z możliwością użytkowania sieci Internet z pominięciem TOR, której działanie ze względów bezpieczeństwa domyślnie jest zablokowane. Poprzednie wersje rozwojowe Linux Tails na poziomie prekonfiguracji oferowały m.in. nawet kamuflaż w postaci graficznego interfejsu przypominającego pulpit MS Windows.



Ryc. 6. Widok okien wyboru panelu prekonfiguracyjnego sesji Linux Tails wykonany w formie zrzutu ekranu sesji na maszynie wirtualnej

System operacyjny Linux Tails uruchomiony z użyciem parametrów opisanych powyżej, jak wspomniano wcześniej, umożliwia dostęp do zamontowanych nośników pamięci w trybie „tylko do odczytu". Prawidłowe działanie softwarowej blokady zapisu systemu TAILS potwierdziły liczne testy autora polegające na montowaniu różnych nośników, zarówno pamięci przenośnej, jak i dysków zainstalowanych w badanych jednostkach, przeglądaniu ich zawartości, prób zapisu na tych nośnikach z wykorzystaniem oprogramowania z interfejsem graficznym dystrybuowanego z kompilacją live USB LinuX Tails 5.2 oraz pracy bieżącej tego systemu, a następnie weryfikowaniu ich wartości funkcji skrótu SHA-1 oraz MD5. Należy zauważyć, że dla systemów plików innych niż oparte na GNU/Linux wbudowana przeglądarka plików automatycznie ignoruje ograniczenia uprawnień dostępu do przeglądania zawartości nośników danych. W przypadku braku szyfrowania możliwe jest zatem uzyskanie dostępu do wszelkich plików użytkownika komputera osobistego, odczytanie ich zawartości lub wykonanie kopii, nawet jeśli natywny system operacyjny jest zabezpieczony przed nieuprawnionym dostępem (Prostym sposobem ochrony przed nieuprawnionym uruchomieniem systemu TAILS na komputerze jest zabezpieczenie panelu wyboru źródła bootowania hasłem z poziomu BIOS). Ponadto nie obserwuje się powstania artefaktów o charakterze dowodu cyfrowego związanych z tym faktem na użytkowanym komputerze. Operacje wykonywane są co prawda z użyciem pamięci RAM, jednakże architektura systemu TAILS ma wbudowany mechanizm, który po zakończeniu procesu natychmiast nadpisuje przydzielony mu obszar, system blokuje również standardowe metody wykonania zrzutu pamięci RAM. Wykonanie takiego zrzutu możliwe jest np. za pomocą oprogramowania AVML, jednakże z uwagi na ograniczenie możliwości zapisu wyniku wyłącznie w obszarze Persistent Storage (patrz dalsza część artykułu) lub za pomocą interfejsu sieciowego stanowi, obok samej analizy treści zrzutu, ciekawy i ważny do rozwiązania w toku dalszych analiz własnych autora problem badawczy. Ponadto w przypadku prawidłowego zakończenia pracy



Ryc. 7. Zdjęcia okna konfiguracyjnego Persistent Storage

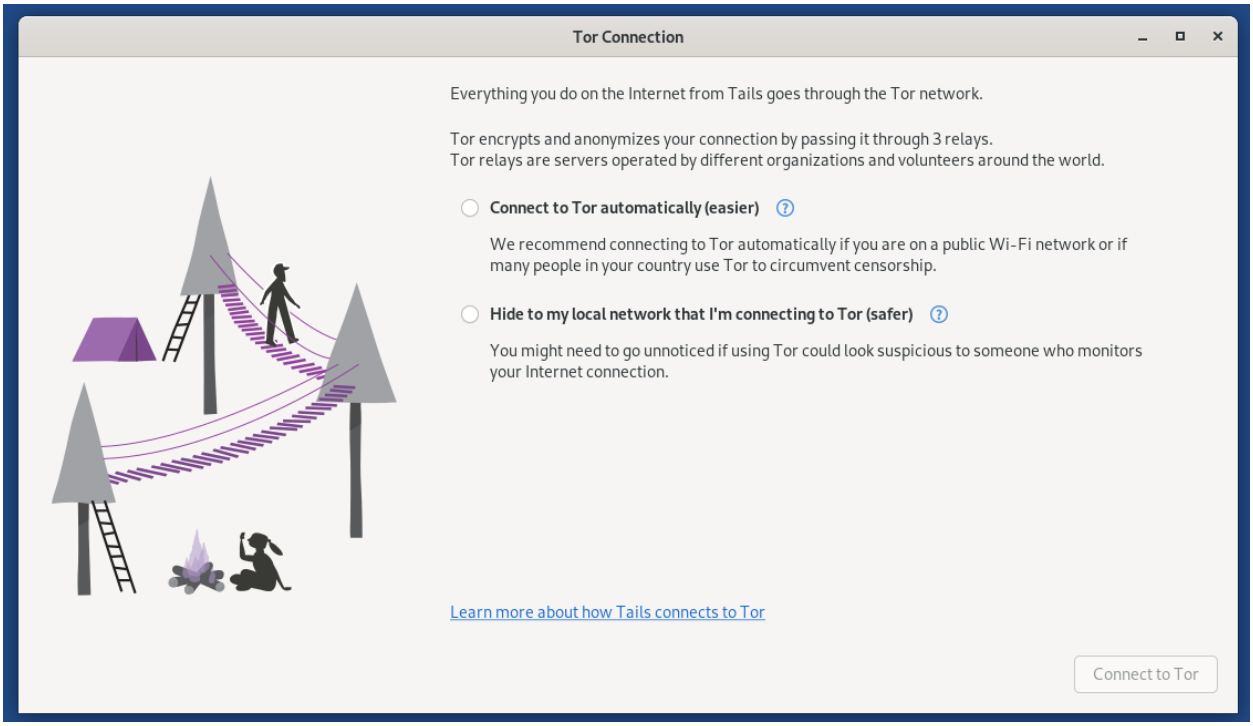
z systemem TAILS następuje nadpisanie całości pamięci ulotnej, co czyni go niewrażliwym na zastosowanie śledcze metod *cold boot attack*.

We wcześniejszych wersjach rozwojowych Linux Tails średnio zaawansowany użytkownik mógł zamontować nośniki pamięci w trybie *read-write*, a więc do opisanych powyżej możliwości dodać można było zdolność do ingerencji w dane. W opisywanej wersji 5.2 z poziomu standardowych ustawień systemu oraz załączonych aplikacji brak jest takiej funkcjonalności, co mimo podniesienia poziomu poufności użytkowania powoduje istotne utrudnienie tzn. brak magazynu na dane wytworzone w trakcie pracy. Deweloperzy m.in. w tym celu zaimplementowali funkcjonalność o nazwie: Persistent Storage – zaszyfrowaną pamięć trwałą. Funkcja ta dostępna jest do skonfigurowania z poziomu uruchomionego z nośnika USB Linux Tails. Za jej pomocą użytkownik w obszarze wolnej pamięci nośnika (Persistent Storage można jedynie zainstalować na nośniku z systemem Linux Tails) zakłada partycję szyfrowaną standardem Linux LUKS. Podczas kolejnego uruchomienia systemu Live partycja zostaje rozpoznana i po podaniu hasła w trybie *read-write* udostępniona zostaje szyfrowana przestrzeń, gdzie oprócz plików użytkownika mogą być m.in. zainstalowane aplikacje lub przechowywane ustawienia konfiguracyjne TAILS.

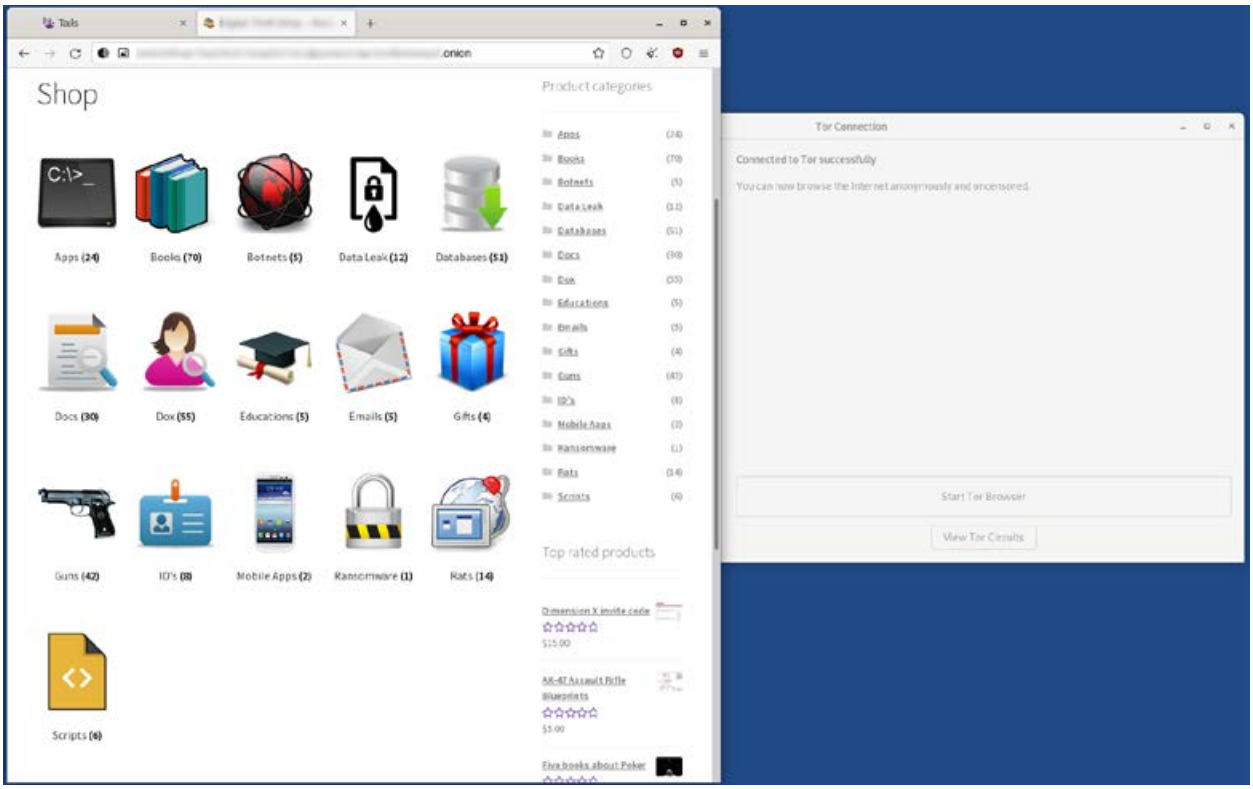
Znamiennym jest, że omawiany system operacyjny nie wymusza utworzenia hasła o wysokim stopniu skomplikowania (dopuszcza nawet jeden dowolny znak jako hasło dostępu), co czyni utworzoną partycję podatną na ataki słownikowe czy też *brute force* z wykorzystaniem m.in. oprogramowania takiego jak Passware Kit Forensics. Ponadto standard szyfrowania LUKS pozwala na odczyt zaszyfrowanej partycji z użyciem znanego hasła dostępu na dowolnym komputerze wyposażonym w stosowne oprogramowanie. Czynność ta może łatwo doprowadzić do powstania w systemie operacyjnym użytego komputera artefaktów zawierających np.: miniatury lub kopie zawartości multimedialnych, indeksy plików oraz ich metadane mające znaczenie śladów cyfrowych.

Kolejną warstwą użyteczności systemu Linux Tails jest interfejs sieciowy. Jak opisano wcześniej, przeglądarka Unsafe Browser dostępna jest jedynie na wyraźne żądanie użytkownika. W innym przypadku całość komunikacji z siecią Internet lub ukrytymi usługami w sieci TOR realizowana jest za pośrednictwem sieci TOR. Ponadto system oferuje zastosowanie tzw. Tor bridge, czyli specjalistycznych przekaźników ukrywających ruch, jak opisano we wcześniejszej części niniejszego artykułu. Metoda ta umożliwia również uzyskanie dostępu do sieci TOR za pomocą punktów dostępowych, gdzie takie połączenie z Internetem jest zablokowane, lub ukrycie takiej działalności.

Przy dodatkowym założeniu stosowania VPN, braku powstawania na komputerze artefaktów innych niż ulotne, które związane są z użytkowaniem sieci, szyfrowaniu pakietów danych oraz ich metadanych, braku bezpośredniego dostępu śledczych do użytkowanego komputera z otwartą sesją TAILS, analiza ruchu



Ryc. 8. Widok okna konfiguracji połączenia z TOR wykonany w formie zrzutu ekranu sesji na maszynie wirtualnej



Ryc. 9. Widok okna przeglądarki z uruchomioną poglądowo witryną dostępną jedynie z poziomu TOR wykonany w formie zrzutu ekranu sesji na maszynie wirtualnej

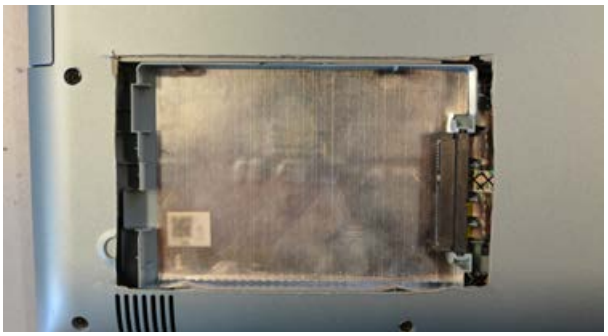
sieciowego oraz jego śledzenie stają się wyjątkowo trudne i pracochłonne, a wręcz niemożliwe. Należy jednak pamiętać, że istnieją narzędzia bazujące na analizie anomalii w ruchu sieciowym pozwalające na typowanie użytkowników stosujących opisane techniki.

Opisywana wersja 5.2 ma również wbudowanego klienta poczty Thunderbird z funkcją obsługi szyfrowanych wiadomości e-mail, aplikację KeePassXC wspomagającą tworzenie i przechowywanie haseł dostępowych, pakiet biurowy LibreOffice, bardzo ciekawą aplikację OnionShare wspierającą przesyłanie plików za pomocą sieci TOR, pakiet narzędzi do obróbki grafiki i dźwięku oraz inne programy użytkowe, w tym diagnostyczne.

Na uwagę zasługuje również fakt potwierdzającej się w wyniku testów oraz analiz materiałów przekazywanych do badań zadowalającej stabilności pracy systemu. Jednocześnie w przypadku nagłego usunięcia z portu USB nośnika zawierającego uruchomioną sesję Linux Tails 5.2 następuje natychmiastowe wyłączenie interfejsu graficznego i po krótkim wylistowaniu błędów oraz kilku procesów systemowych komputer zostaje wyłączony. Znaczenie opisanego powyżej mechanizmu dla organów ścigania autor pozwala sobie pozostawić ocenie czytelnika. Ponadto TAILS stabilnie pracuje w środowisku wirtualnym np. VMware Workstation, gdzie jedynym ograniczeniem funkcjonalności jest brak obsługi Persistent Storage (według dystrybutora pełna funkcjonalność na maszynie jest dostępna w aplikacji *virt-manager* działającej w środowisku Linux).

W praktyce biegłego z zakresu badań informatycznych spotkać można pomysłowe połączenia wyrafinowanych narzędzi utrudniających przeprowadzenie analizy danych, takich jak Linux Tails, oraz różnorodnych fizycznych modyfikacji sprzętu mających za zadanie dodatkowo zabezpieczyć dane przed czynnościami organów ścigania. Materiałem dostarczonym do badań w jednej z takich spraw był komputer przenośny, w którym wycięto część obudowy, tak by ułatwić szybki demontaż dysku twardego, natomiast w czytniku nośników optycznych ujawniona została jedna z dystrybucji TAILS nagrana na płycie DVD, co przedstawiono poglądowo na poniższych zdjęciach:

Ryc. 10. Widok czytnika wraz z nośnikiem Linux Tails



Ryc. 11. Widok modyfikacji w obudowie komputera przedstawionego na zdjęciu powyżej

W kolejnym, bardziej wymagającym analitycznie przypadku autor mimo szczegółowych badań m.in. za pomocą oprogramowania X-Ways Forensics, Magnet AXIOM czy też wirtualizacji systemu operacyjnego zainstalowanego na przekazanej do badań jednostce komputerowej nie ujawnił zgodnie z pytaniem prowadzącego: dokumentacji, wpisów historii przeglądania stron internetowych czy też treści korespondencji dotyczącej wprowadzania do obrotu pewnych nielegalnych substancji. Mimo że historia ujawniona w pamięci przeglądarek internetowych oraz treści plików nie wskazywała nawet na zainteresowanie użytkownika przedmiotowymi zagadnieniami, stała się ona kluczowa dla wskazania dalszego toku postępowania w tej sprawie. Szczegółowa analiza historii wyszukiwania fraz w sieci Internet wskazała bowiem na nagłe i objawiające się w krótkim czasie zainteresowanie użytkownika narzędziami do anonimizacji oraz dostępu do sieci TOR. Stwierdzono również obecność śladów cyfrowych wskazujących na pobranie z sieci Internet jednej z dystrybucji Linux Tails. W toku wcześniejszej analizy na partycji odpowiedzialnej za bootowanie systemu MS Windows (na takiej partycji dostęp do zapisu z poziomu użytkownika systemu MS Windows jest zablokowany) ujawniono również obecność nietypowego pliku tekstowego. Korelacja znaczników czasowych opisanych powyżej zbiorów artefaktów wskazała na kolejność działań opisaną poniżej. Użytkownik w pierwszym kroku wyszukał, a następnie pobrał i zainstalował Linux Tails na nośniku wymiennym. W celu ukrycia wrażliwych dla siebie danych zapisał je w pliku tekstowym umieszczonym, jak wspomniano powyżej, na niewidocznej z poziomu użytkownika MS Windows partycji dysku systemowego (operacja zapisu nie byłaby możliwa dla średniozaawansowanego użytkownika, gdyby użyto nowszych dystrybucji TAILS, takich jak wersja 5.2. Fakt ten może tłumaczyć, dlaczego w przypadkach rozpatrywanych w ramach aktualnych zleceń w materiale dowodowym znajdują się starsze wersje rozwojowe systemu). W istocie przedmiotowy plik zawierał adres witryny sieci TOR, który z uwagi na składnię charakteryzującą się wysoką entropią znaków, jak wspomniano wcześniej (np.: https://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page), jest trudny do zapamiętania. Wspomniany adres prowadził do spersonalizowanej strony użytkownika na witrynie specjalizującej się w obrocie nielegalnymi substancjami. W tym substancjami, których dotyczyło zlecenie badań. Polityka transparentności wspomnianej witryny pozwalała na pisanie publicznych informacji zwrotnych poszczególnym użytkownikom. Ustalono zatem, że na podstawie skarg odbiorców (związanych z zerwaniem kontaktu i niewywiązaniem się dostarczenia zakupionego towaru) przedmiotowa spersonalizowana strona została zablokowana zaraz po dacie czynności związanych z zabezpieczeniem sprzętu przekazanego do badań. Ponadto autor pragnie zwrócić uwagę, że o ile obecność ujawnionego adresu w obszarze dostępnym użytkownikowi MS Windows można spróbować wytłumaczyć nawet procesami geologii cyfrowej, np. związanymi z *cache* przeglądarek internetowych, to pojawienie się pliku w opisanym obszarze nośnika pamięci wskazuje na zachowanie intencjonalne i to z użyciem niespecyficznych, profesjonalnych narzędzi.

Podsumowując powyższą analizę, autor pragnie zwrócić uwagę, że narzędzie Linux Tails w wersji 5.2 stanowi system minimalizujący powstawanie geologicznych dowodów cyfrowych (Altheide, 2014, s. 18), a więc takich, które związane są z autonomiczną pracą systemu komputerowego i powstającą automatycznie oraz nieintencjonalnie. Jednocześnie ilość artefaktów o charakterze archeologii cyfrowej (Altheide, 2014, s. 18), a więc powstających intencjonalnie w wyniku działań użytkownika zbiorów danych, zależy w tym przypadku od jego samoświadomości oraz charakteru i poziomu skomplikowania wykonywanych operacji. W odniesieniu do zastosowań przestępczych kluczowym problemem użytkownika jest żmudność wykonywania niekiedy zwyczajowo prostych operacji, a zatem pokusa do rezygnowania z pewnych zasad bezpieczeństwa. Zachowania takie stanowią pole do wykorzystania najcenniejszych umiejętności informatyka śledczego, jakimi obok wiedzy specjalnej są umiejętności analitycznego myślenia i korelacji faktów, bez których nawet coraz bardziej zaawansowane oprogramowanie *forensics* wciąż będzie bezużyteczne.

Szczególne podziękowania za wymianę myśli naukowej składam Panom: Rafałowi Czechowi, Marcinowi Napiórkowskiemu oraz Krzysztofowi Turowskiemu.

Autor

Bibliografia:

1. Allsopp, W. (2017). *Testy penetracyjne dla zaawansowanych. Hakowanie najlepiej zabezpieczonych sieci na świecie*. Wydawnictwo Helion.
2. Altheide, C., Carvey, H. (2014). *Informatyka śledcza. Przewodnik po narzędziach open source*. Wydawnictwo Helion.
3. Casad, J. (2017). *TCP/IP w 24 godziny. Wydanie VI*. Wydawnictwo Helion.
4. Ciborski, T. (2015). *Ukryta tożsamość. Jak się obronić przed utratą prywatności*. Wydawnictwo Helion.
5. Flow, S. (2022). *Hakuj jak duch. Łamanie zabezpieczeń środowisk chmurowych.* Wydawnictwo Helion.
6. Hayes, D.R. (2021). *Informatyka w kryminalistyce. Praktyczny przewodnik*. Wydanie II. Gliwice. Wydawnictwo Helion.
7. Krawetz N. (2008). *Hacking Ubuntu. Konfiguracja i optymalizacja*. Gliwice. Wydawnictwo Helion.
8. Mider D. (2019). *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów*, „Przegląd Bezpieczeństwa Wewnętrznego" 21/19.
9. Muniz J, Lakhani A. (2014). *Kali Linux. Testy penetracyjne*. Gliwice. Wydawnictwo Helion.
10. Ortega J. M. (2022). *Bezpieczeństwo sieci w Pythonie. Rozwiązywanie problemów za pomocą skryptów i bibliotek*. Wydanie II. Gliwice. Wydawnictwo Helion.
11. Petreley N., Bacon J. (2005). *100 sposobów na Linux*. Gliwice. Wydawnictwo Helion.
12. Sokół R. (2014). *Jak pozostać anonimowym w sieci*. Gliwice. Wydawnictwo Helion.

Źródła rycin:

Ryc. 1: Trasowanie cebulowe, Wikipedia, https://pl.wikipedia.org/wiki/Trasowanie_cebulowe.

Ryc. 2, 3, 4: Hosting Anonymous Website on Tor Network, Abed Samhuri, https://medium.com/axon-technologies/hosting-anonymous-website-on-tor-network-3a82394d7a01.

Ryc. 5: Tor Browser 9.0 już dostępny do pobrania, Sekurak, https://sekurak.pl/tor-browser-9-0-juz-dostepny-do-pobrania/.

Ryc. nr 6, 7, 8, 9, 10, 11: opracowanie własne autora.

Internet:

1. BridgeDB, Tor Project, https://bridges.torproject.org/bridges?transport=obfs4 (dostęp: 28.07.2022).
2. GitHub – icrosoft/avml: AVML – Acquire Volatile Memory for Linux, https://github.com/microsoft/avml (dostęp: 26.07.2022).
3. Hosting Anonymous Website on Tor Network, Abed Samhuri, https://medium.com/axon-technologies/hosting-anonymous-website-on-tor-network-3a82394d7a01 (dostęp: 28.07.2022).
4. Jak zainstalować i poprawnie skonfigurować przeglądarkę Tor 8.0, Ewelina Stój, PurePC, https://www.purepc.pl/jak-zainstalowac-i-poprawnie-skonfigurowac-przegladarke-tor-8-0 (dostęp: 27.07.2022).
5. Narzędzia anonimizujące działania w Internecie jako instrumentarium do prowadzenia operacji informacyjnych w ramach wojny hybrydowej, Przegląd Bezpieczeństwa Wewnętrznego Wydanie Specjalne, Kamil Kucharski, https://www.abw.gov.pl/download/1/1923/kucharski.pdf (dostęp: 28.07.2022).
6. Sieć TOR – wszystko, co trzeba o niej wiedzieć, Bitdefender, https://bitdefender.pl/siec-tor-wszystko-co-trzeba-o-niej-wiedziec/ (dostęp: 28.07.2022.
7. Signing in to a network using a captive portal, https://tails.boum.org/doc/anonymous_internet/tor/index.en.html#hiding (dostęp: 26.07.2022).
8. Tor Browser Bundle, dobreprogramy, https://www.dobreprogramy.pl/tor-browser-bundle,program,windows,6628600948791425 (dostęp: 28.07.2022).
9. Tor Browser 9.0 już dostępny do pobrania, Sekurak, https://sekurak.pl/tor-browser-9-0-juz-dostepny-do-pobrania/ (dostęp: 28.07.2022).
10. Tor (sieć anonimowa), Wikipedia, https://pl.wikipedia.org/wiki/Tor_(sie%C4%87_anonimowa) (dostęp: 28.07.2022).
11. Tails – Accessing the internal hard disk, https://tails.boum.org/doc/advanced_topics/internal_hard_disk/index.en.html (dostęp: 26.07.2022).
12. Tails – Memory erasure, https://tails.boum.org/contribute/design/memory_erasure/ (dostęp: 26.07.2022).
13. Tails – Sponsors, https://tails.boum.org/sponsors/index.en.html (dostęp: 26.07.2022).
14. Trasowanie cebulowe, Wikipedia, https://pl.wikipedia.org/wiki/Trasowanie_cebulowe (dostęp 28.07.2022).
15. Zarys historyczny sieci Darknet oraz aspekty legalnego i nielegalnego wykorzystania technologii Tor, Przegląd Nauk Stosowanych nr 19, Politechnika Opolska Wydział Ekonomii i Zarządzania, Rafał Kokot, Tomasz Turba, https://pns.po.opole.pl/images/PNS_19/PNS19-IX.pdf (dostęp: 28.07.2022).
16. Z systemem Tails nikt nie będzie śledził cię w internecie, https://www.benchmark.pl/aktualnosci/system-tails-gwarantuje-prawdziwa-anonimowosc-w-sieci.html (dostęp: 29.07.2022).