System Operacyjny
Tails OS

Maria Budziło, Ivasenko Kateryna

Grudzień 17, 2020

1 Wstęp

Tails to system działający na żywo, którego celem jest zachowanie prywatności i anonimowości użytkownika. Pomaga w anonimowym korzystaniu z Internetu i omijaniu cenzury prawie wszędzie i na każdym komputerze. Nie pozostawia żadnych śladów, chyba że użytkownik zażyczy sobie inaczej.

Jako kompletny system operacyjny przeznaczony do użytku z DVD, pendrive'a lub karty SD może działać niezależnie od oryginalnego systemu operacyjnego komputera. Jest darmowym oprogramowaniem- Free Software- i bazuje na systemie Debian GNU / Linux.

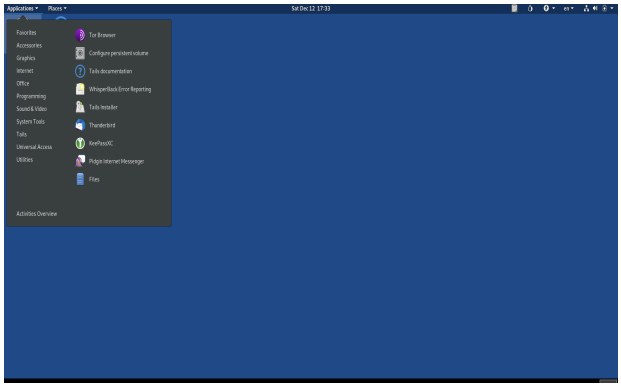
Oficjalne logo OS Tails

2 Podstawowe funkcje i informacje

The Amnesic Incognito Live System w skrócie TAILS to system operacyjny, podobny takim jak Windows lub Mac OS, jednak dzięki specjalnemu projektowi pozwala zachować wysoką anonimowość i prywatność użytkownika, obsługiwany jest na sprzęcie zgodnym z x86 i / lub wirtualnymi maszynami

Tails, jest skoncentrowaną na bezpieczeństwie dystrybucją Linux'a opartą na Debianie 1a, której celem jest zachowanie prywatności i anonimowości. W zestawie Tails OS znajdują się takie aplikacje 1b, które zostały skonfigurowane z myślą o bezpieczeństwie, między innymi: przeglądarka internetowa, komunikator internetowy, klient poczty elektronicznej, Office Suite, edytor obrazu, edytor dźwięku itp. Dodatkowo wszystkie jego połączenia wychodzące są zmuszane do przechodzenia przez Tor'a, a połączenia bezpośrednie (nie anonimowe) są blokowane.

(a) Pulpit czerpiący z Debiana



(b) Aplikacje Tails

System został zaprojektowany do uruchamiania na żywo z DVD lub USB, nie pozostawia śladów (cyfrowych śladów) na urządzeniu, chyba że wyraźnie zostanie to nakazane. Projekt Tor zapewnił większość wsparcia finansowego na rozwój tego projektu.

3 Prywatność i użytkowanie

Oprogramowania można używać w domu, u znajomego lub w lokalnej bibliotece. Po wyjęciu z

komputera DVD lub pamięci USB, na których to Tails jest zainstalowany, można urządzenie ponownie uruchomić za pomocą zwykłego systemu operacyjnego. Jest on bowiem tak skonfigurowany, aby nie używać dysku twardego komputera lub nawet jego partycji wymiany (SWAP). Jedynym miejscem używanym przez Tails jest pamięć RAM, która automatycznie kasowana po wyłączeniu komputera, nie pozostawia żadnego śladu użytkowania Tails. Dlatego to system ten nazywa się „Amnesic", czyli amnezyjny- powodujący utratę pamięci. Pozwala to bowiem na pracę z wrażliwym plikiem na dowolnym komputerze i uniemożliwia odzyskaniu danych po wyłączeniu komputera.

4 Anonimowość online

Tails polega na sieciach przeglądarki Tor, co pozwala chronić prywatność użytkownika w Internecie. Całe oprogramowanie jest skonfigurowane do łączenia się przez Tor'a, a połączenia bezpośrednie (które nie gwarantują już anonimowości) są blokowane.

Tor jest to darmowe oprogramowanie, które pozwala chronić prywatność i gwarantuje poufność w Internecie. Chroni użytkownika, przesyłając komunikację przez rozproszoną sieć przekaźników prowadzonych przez wolontariuszy na całym świecie. Uniemożliwia to każdemu, kto może monitorować połączenia internetowe użytkownika, odnalezienie przeglądanych witryn, a także uniemożliwia tym witrynom odkrywanie, lokalizacji użytkownika.

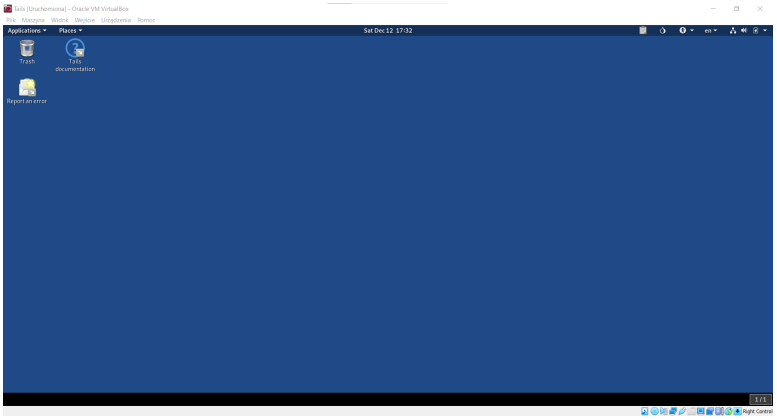
5 Narzędzia do szyfrowania

Tails zawiera również szereg narzędzi do ochrony danych za pomocą silnego szyfrowania. Pozwala na przykład zaszyfrować pamięć USB lub zewnętrzne dyski twarde za pomocą LUKS, standardu Linux dla woluminu szyfrowania.

Umożliwia też automatycznie szyfrować komunikację ze stronami internetowymi przy użyciu HTTPS Everywhere, będącym rozszerzeniem do Firefox'a opracowanym przez Electronic Frontier Foundation. Natomiast dzięki OpenPGP, standardu w swojej dziedzinie, pozwala na szyfrowanie i podpisywanie wiadomości e-mail i dokumentów z klienta poczty elektronicznej Tails, edytora tekstu lub przeglądarki plików. Daje również ochronę rozmów przez komunikatory internetowe za pomocą OTR, narzędzia kryptograficznego zapewniającego szyfrowanie, uwierzytelnianie i zaprzeczanie. I w końcu pozwala na bezpieczne usuwanie plików i czyszczenie miejsca na dysku za pomocą Nautilus Wipe

6 Środowisko GNOME

Tails jako środowiska graficznego używa środowiska GNOME 2. Główną jego wadą jest to, że wymaga sporo zasobów do prawidłowego działania, ale ma też wiele zalet. Mianowicie jest dobrze zintegrowany, co jest plusem szczególnie dla nowych użytkowników Linux'a.



Rysunek 2: Pulpit środowiska GNOME

Bardzo dobrze przetłumaczony i udokumentowany działa względnie dobrze, jeśli chodzi o funkcje ułatwień dostępu. Aktywnie rozwijany oraz mocno wspierany przez Debiana, gdzie jest domyślnym środowiskiem graficznym.

7 Zgodność sprzętowa

System Tails automatycznie wykrywa typ procesora komputera i odpowiednio ładuje jądro 32-bitowe lub 64-bitowe. Jest dostępny niestety tylko na architekturach x86 i x64, natomiast nie działa w architekturze ARM.

8 Instalacja

Instalacja oprogramowania nie jest możliwa przy użyciu zalecanych lub typowych metod instalacji. Tails został zaprojektowany jako system działający na żywo z nośnika wymiennego: DVD, pendrive lub karta SD. Co jest świadomą decyzją, ponieważ ten tryb działania jest lepszy dla tego, co producent chce zapewnić użytkownikom Tails: tzw. niepamięć/ amnezję - fakt, że Tails nie pozostawia śladów na komputerze po zamknięciu sesji.

Jeżeli chodzi o aktualizacje Tails dostarcza je co 6 tygodni. Są one dokładnie testowane, aby upewnić się, że żadna funkcja bezpieczeństwa ani konfiguracja nie jest wadliwa. W momencie próby zaktualizowania systemu samodzielnie przez użytkownika za pomocą apt-get lub Synaptic, może dojść do uszkodzeń sprzętu lub pewnych problemów. Dlatego zaleca się aktualizację, poprzez Tails Upgrader, gdzie po otrzymaniu powiadomienia można rozpocząć aktualizację wg instrukcji.

9 Przeglądarka internetowa

Głównym i tak ważnym dystrybutorem przeglądarki internetowej jest Przeglądarka Tor, która w opcjach pozwala na rozszerzenie JavaScript. Jak wiadomo wiele dzisiejszych witryn internetowych wymaga do poprawnego działania JavaScript. W konsekwencji JavaScript jest domyślnie włączona w Tails, aby uniknąć dezorientacji wielu użytkowników. Dodatkowo rozszerzenie Torbutton, zawarte w Tails, dba o blokowanie niebezpiecznych funkcji JavaScript. Przeglądarka Tor zawiera również suwak bezpieczeństwa i rozszerzenie NoScript, aby opcjonalnie wyłączyć więcej opcji JavaScript. W niektórych przypadkach może to poprawić bezpieczeństwo. Jeśli jednak wyłączymy JavaScript, odcisk przeglądarki będzie się różnił od większości użytkowników Tora. To może natomiast spowodować mniejszą anonimowość użytkownika.

Rysunek 3: Oficjalne logo Tor

10 Sieć

Prawie najważniejszym założeniem Tails'a jest wymuszane kierowanie całego ruchu wychodzącego, do anonimowych sieci, takich jak Tor czy I2P. Natomiast VPN nie jest siecią anonimową, ponieważ administratorzy VPN mogą wiedzieć, skąd pochodzi połączenie i dokąd jest kierowane. Tor zapewnia anonimowość, uniemożliwiając jakiemukolwiek innemu użytkownikowi sieci poznanie zarówno pochodzenia, jak i celu połączenia naszego użytkownika.

W niektórych sytuacjach jednak użytkownik może być zmuszony do korzystania z VPN do łączenia się z Internetem, na przykład przez dostawcę usług internetowych. Obecnie nie jest to możliwe przy użyciu Tails. Jednak nie użytkownik nie pozostaje bez wyjścia. Mostki Tor'a mogą być bowiem bardzo przydatne do ominięcia ograniczeń nałożonych przez dostawcę usług internetowych, przez co nie ma potrzeby na posiadanie VPN.

Czasami natomiast przydatne może być połączenie z VPN przez Tor'a, aby na przykład uzyskać dostęp do usług, które blokują połączenia przychodzące z Tor'a lub aby uzyskać dostęp do zasobów dostępnych tylko w sieci VPN, na przykład w firmie lub uczelni użytkownika. Obecnie niestety w takim wypadku nie jest to łatwe przy użyciu Tails.

11 Oprogramowania Tails

Aby oprogramowanie zawierało się w Tails, musi ono być najpierw dostępne na Debainie. Dodanie oprogramowania Tails, którego nie ma w Debianie, pociąga za sobą dodatkowe obciążenie, które może zagrozić trwałości projektu.

Rysunek 4: Oficjalne logo systemu Debian

Poza tym, bycie w Debianie ma wiele zalet:

- Jest częścią procesu Debiana w zakresie aktualizacji bezpieczeństwa i nowych wersji.
- Jest uwierzytelniany przy użyciu podpisów OpenPGP.
- Jest pod obserwacją społeczności Debiana i jego licznych użytkowników i pochodnych, w tym Ubuntu.

Programiści dodatkowo próbują ograniczyć ilość oprogramowania zawartego w Tails, a dodawanie nowego oprogramowania motywowane jest tylko najpotrzebniejszymi ulepszeniami. Jest tak, ponieważ:

- Próbuje się ograniczać wzrost obrazu ISO i automatycznych aktualizacji.
- Więcej oprogramowania oznacza więcej problemów z bezpieczeństwem.
- Unika się proponowania kilku opcji wykonania tego samego zadania.
- Jeśli pakiet musi zostać usunięty po jego aktualizacji, na przykład z powodu problemu z bezpieczeństwem, może to być nie wygodne dla użytkowników, którzy go używają.

12 Inne kwestie bezpieczeństwa

Zaletą Tails jest to, że działa niezależnie od systemu operacyjnego zainstalowanego na komputerze. Jeżeli dochodzi do sytuacji, w której na przykład komputer został tylko naruszony przez oprogramowanie, działające z poziomu zwykłego systemu operacyjnego (wirus, trojan itp.), wtedy można bezpiecznie używać Tails tak długo jak jest on zainstalowany przy użyciu zaufanego systemu. Jeśli jednak komputer został naruszony przez kogoś posiadającego fizyczny dostęp do niego i kto zainstalował niezaufane fragmenty sprzętu, to używanie Tails może nie być bezpieczne.

Literatura

[1] Tails Official Website
https://tails.boum.org/

[2] Wikimedia Commons
https://commons.wikimedia.org/wiki/Main$_Page$/