Łukasz Basa

Zabezpieczamy domową sieć przed stronami wyłudzającymi od nas dane

Jest wieczór. Za oknem prószy śnieg. Kładziesz się właśnie, aby odpocząć, gdy nagle twój telefon krótko wibruje – dostałeś/aś wiadomość. Obojętnym wzrokiem zerkasz na ekran i widzisz treść SMSa: „Wysyłka pod wskazany adres jest droższa. Prosimy dopłacić 1 PLN, brak dopłaty oznacza anulowanie zamówienia. http://...". Podnosisz się gwałtownie, do twojej głowy wpada myśl: „o nie... mój nowy Xbox nie dojdzie na czas!". W tym samym czasie po drugiej stronie globu przestępca zaciera ręce. Czeka, aż ktoś kliknie w zastawioną przez niego pułapkę i tym samym umożliwi mu uzyskanie loginów i haseł do systemów bankowych.

14+

DOWIESZ SIĘ

- Jakie zagrożenia mogą wiązać się z klikaniem w linki przesłane w wiadomościach SMS lub e-mail.
- Co to jest i jak działa „DNS".
- Jak skonfigurować własny, lokalny serwer DNS, który zablokuje oszukańcze domeny internetowe.

POTRZEBNA WIEDZA

- Posiadanie dowolnego modelu Raspberry Pi lub innego starego, nieużywanego komputera,
- Podstawowa wiedza z zakresu sieci komputerowych.
- Podstawowa znajomość systemu operacyjnego Linux (ułatwi to pracę).

W INTERNECIE GRASUJĄ PRAWDZIWI PRZESTĘPCY!

Powyższa historia, co prawda zmyślona, mogła się wydarzyć naprawdę. Żyjemy w czasach globalnej wioski i wszystkie elementy naszego życia przenoszą się do sieci. Wiedzą o tym także przestępcy, którzy już dawno zaczęli wykorzystywać Internet do tego, aby wzbogacić się czyimś kosztem.

W ostatnim czasie bardzo popularne są ataki internetowych oszustów na internautów. Za pomocą masowej korespondencji e-mail lub SMS przestępcy rozsyłają komunikaty, które mają na celu zachęcić do wejścia na fałszywą stronę internetową i podania wrażliwych informacji (na przykład loginów czy haseł). Ta technika wyłudzania danych nazywa się **phishing** i była szeroko omawiana w poprzednim numerze PJR.

W tym artykule zajmiemy się budowaniem narzędzia, które ochroni naszą sieć domową przed tego typu atakami i jednocześnie pozwoli nam dokładnie zrozumieć, jak działa DNS.

Ważna informacja

Zanim zaczniesz konfigurować swój własny serwer DNS, skonsultuj to najpierw ze swoimi rodzicami lub opiekunami. Warto pamiętać, że pozostawienie takiego urządzenia włączonego 24 godziny na dobę generuje dodatkowe koszty zużycia prądu. Należy również pamiętać o umieszczeniu go w bezpiecznym miejscu, które nie spowoduje zagrożenia pożarem w przypadku jego nadmiernego przegrzania się.

CO TO JEST ADRES IP?

Szacuje się, że sieć Internet składa się z około 50 miliardów urządzeń (nie tylko komputerów i telefonów, ale także kamer, oczyszczaczy powietrza czy inteligentnych żarówek), które są ze sobą połączone i potrafią się komunikować. Część z nich ma tak zwany publiczny adres IP. Jest to adres, pod którym można to urządzenie znaleźć w sieci.

Aby dokładniej to zrozumieć, wyobraź sobie, że wchodzisz na stronę internetową, na której umieszczone jest śmieszne zdjęcie z kotem. Żeby wyświetlić zdjęcie na twoim komputerze, serwer, na którym ono się znajduje, musi je do ciebie wysłać. Wyobraźmy więc sobie, że połączenie sieciowe pomiędzy serwerem a twoim komputerem to koperta, w której znajduje się obrazek naszego kotka. Na kopercie trzeba wpisać twój adres domowy, aby przesyłka mogła dotrzeć. Tak samo jest w Internecie – każde urządzenie ma swój adres. Przykładowy adres IP wygląda tak:

```
216.58.215.78
```

Składa się on z 4 części nazywanych oktetami. Oddzielone są one od siebie kropką. Każdy z oktetów może przyjmować wartości liczbowe od 0 do 255. Wadą (dla człowieka) tej notacji jest to, że bardzo trudno zapamiętać taki adres. Na przykład ten powyższy to adres wyszukiwarki Google. Wyobraź sobie, że za każdym razem musiałbyś wpisywać ten ciąg cyfr zamiast www.google.com. Niewygodne, prawda? Dlatego też wymyślono DNS.

CO TO JEST DNS?

DNS (Domain Name System) to rozproszony system informatyczny, który ma na celu zamianę domen internetowych (łatwych do zapamiętania dla ludzi) na odpowiadające im adresy IP (zrozumiałe dla komputerów). Gdy wpisujesz w przeglądarkę internetową adres https://www.google.com/, twój komputer wysyła zapytanie do serwera DNS o to, jaki adres IP kryje się pod tą nazwą. Dzięki temu może odpowiednio zaadresować pakiety sieciowe, które będzie tam wysyłał.

Każdy komputer (ale także tablet, telefon, telewizor czy inne podłączone do sieci urządzenie) ma w swojej konfiguracji informację o adresie serwera DNS, z którego ma korzystać, do tłumaczenia domen na adresy IP. Adres ten najczęściej jest wskazywany w sposób automatyczny przez router, do którego jesteśmy podłączeni, i jest to serwer DNS zarządzany przez naszego dostawcę Internetu.

Nic nie stoi na przeszkodzie, abyś postawił/a serwer DNS samodzielnie w sieci domowej i, za jego pomocą, przekierował/a złośliwe domeny na nieistniejące adresy IP. Dzięki temu, nawet jeżeli ktoś z domowników kliknie w złośliwy link, to jego urządzenie nie będzie w stanie wejść na stronę przestępców.

WARTO WIEDZIEĆ

W Internecie dostępnych jest wiele publicznych serwerów DNS. Do najbardziej popularnych należą adresy:

- `8.8.8.8` oraz `8.8.4.4` – serwery DNS od Google
- `1.1.1.1` oraz `1.1.1.2` – serwery DNS od Cloudflare
- `9.9.9.9` – serwery DNS od Quad9

STAWIAMY WŁASNY SERWER DNS!

Serwer DNS możemy zainstalować w zasadzie na dowolnym komputerze. Może to być stary „pecet", którego już nie używamy, może to być mniejsze urządzenie, takie jak na przykład komputer Raspberry Pi, ale równie dobrze może to być nasza stacja robocza. Warto jednak pamiętać, że decydując się na postawienie takiego serwera w naszej sieci domowej, musimy zapewnić, że w każdej chwili będzie on dostępny dla innych urządzeń (czyli krótko mówiąc, będzie on cały czas włączony). W innym przypadku urządzenia, które znajdują się w naszej sieci, nie będą w stanie tłumaczyć nazw domenowych na adresy IP, a tym samym przestanie nam działać Internet. Aby się przed tym zabezpieczyć, można wskazać drugi adres (zapasowy) publicznego serwera DNS dostępnego w Internecie (zobacz ramka „Warto wiedzieć").

Na potrzeby tego projektu wybrałem leżący u mnie w szufladzie komputer Raspberry Pi z systemem operacyjnym Linux Raspberry Pi OS. Jest to małe urządzenie, które zajmuje mniej miejsca niż router Wi-Fi i jednocześnie ma bardzo niski pobór prądu. Więcej na temat tych komputerów, jak również dostępnych dla nich systemów operacyjnych, przeczytasz na stronie ich producenta: https://www.raspberrypi.org.

INSTALACJA I KONFIGURACJA PI-HOLE

Skoro mamy już urządzenie z zainstalowanym systemem Linux, możemy zabrać się za instalację oprogramowania Pi-hole. Jest to aplikacja, która zmienia nasz komputer w pełnoprawny serwer DNS i umożliwia zarządzanie nim przy użyciu wygodnego panelu WWW. Dodatkowym atutem tej aplikacji jest możliwość pobierania z Internetu list domen do blokowania, co zwiększy nasze bezpieczeństwo w sieci. Więcej na temat tego rozwiązania można przeczytać na stronie https://pi-hole.net.

Pierwszym krokiem będzie zalogowanie się na Raspberry Pi za pomocą protokołu SSH (secure shell). Jest to szyfrowany protokół komunikacyjny często wykorzystywany przez administratorów do zarządzania serwerami. Aby z niego skorzystać, będziemy potrzebowali klienta SSH na komputerze. W przypadku macOS oraz Linux jest to standardowa komenda w terminalu. W systemie Microsoftu jest ona dostępna dopiero od Windows 10. W przypadku starszych systemów operacyjnych Windows można wykorzystać popularny program PuTTY.

CIEKAWOSTKA

Czy wiesz, że adres IP urządzenia możesz uzyskać za pomocą narzędzia **ping**, które dostępne jest w większości systemów operacyjnych? Uruchom wiersz poleceń (w systemach Windows *Start->Uruchom->cmd*) i wpisz polecenie:

```
ping raspberrypi.local
```

```
Last login: Wed Jan  6 17:39:42 on ttys000
lukasz@macbook-lukasz ~ % ping raspberrypi.local
PING raspberrypi.local (192.168.68.117): 56 data bytes
64 bytes from 192.168.68.117: icmp_seq=0 ttl=64 time=58.458 ms
64 bytes from 192.168.68.117: icmp_seq=1 ttl=64 time=1.645 ms
64 bytes from 192.168.68.117: icmp_seq=2 ttl=64 time=104.168 ms
64 bytes from 192.168.68.117: icmp_seq=3 ttl=64 time=113.873 ms
64 bytes from 192.168.68.117: icmp_seq=4 ttl=64 time=3.279 ms
^C
--- raspberrypi.local ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.645/56.285/113.873/47.768 ms
lukasz@macbook-lukasz ~ %
```

Ilustracja 1. Wynik polecenia „ping" wskazujący nam adres IP serwera

Dzięki tej prostej komendzie udało nam się dowiedzieć, że nasz serwer działa i ma adres `192.168.68.117` w naszej sieci lokalnej.

Składnia polecenia SSH nie jest skomplikowana. Jako argumenty podajemy nazwę użytkownika, kolejno znak „@", a następnie adres IP serwera. W moim przypadku składnia wygląda jak na Ilustracji 2. Standardowym użytkownikiem jest „pi", a hasłem „raspberry" (uwaga: wielkość liter ma znaczenie!).

```
lukasz@macbook-lukasz ~ % ssh pi@192.168.68.117
pi@192.168.68.117's password:
Linux raspberrypi 5.4.79+ #1373 Mon Nov 23 13:18:15 GMT 2020 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan  6 16:58:14 2021 from 192.168.68.116

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~ $
```

Ilustracja 2. Logowanie do serwera z użyciem „SSH"

Kolejnym krokiem jest aktualizacja systemu operacyjnego i zainstalowanych na nim pakietów (oprogramowania). Wykonujemy to za pomocą komend:

```
apt update
apt upgrade
```

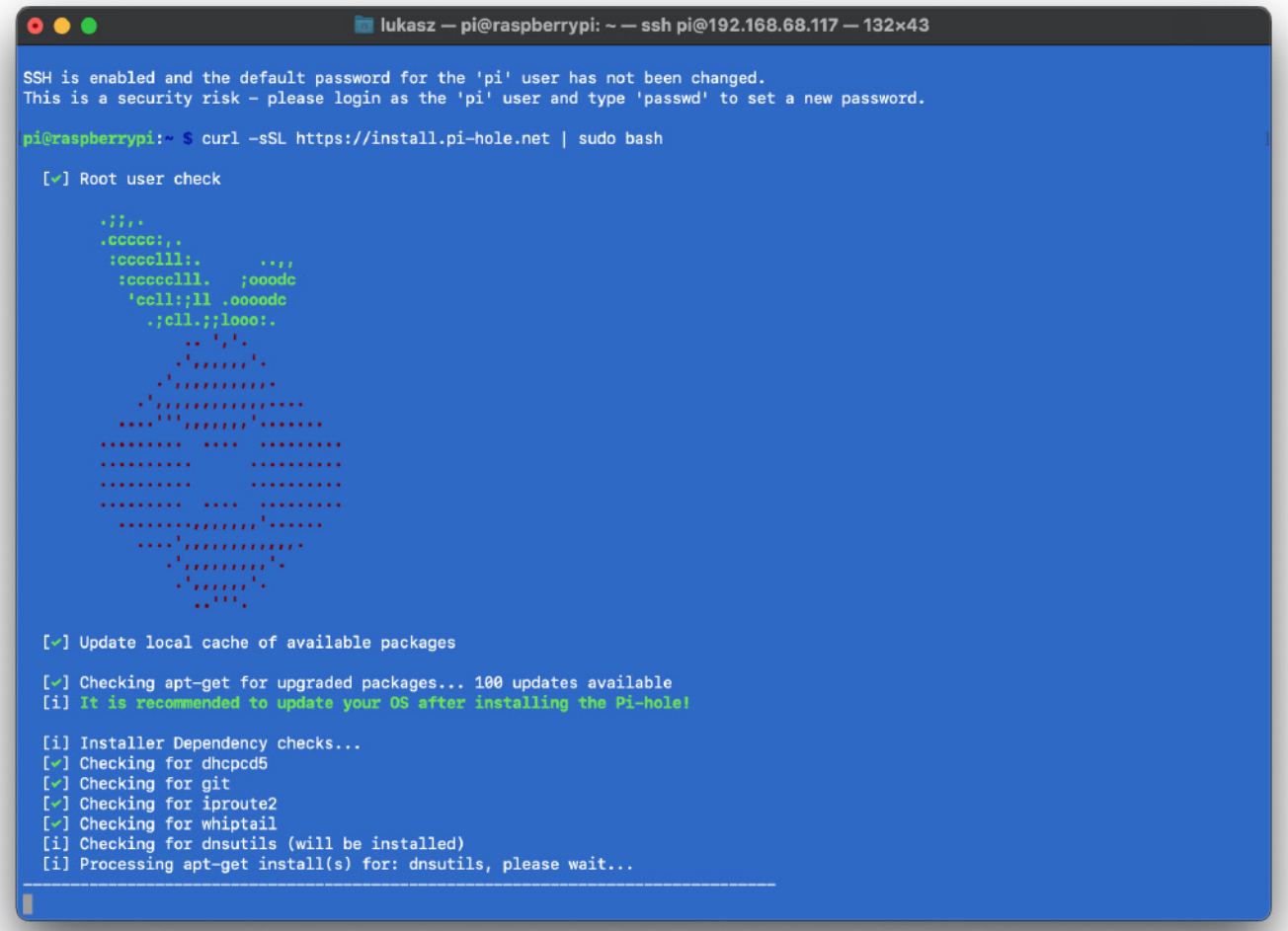
W zależności od aktualności obrazu naszego systemu ta operacja może potrwać od kilku do kilkunastu minut. Należy uzbroić się w cierpliwość.

Po zakończonej aktualizacji możemy przystąpić do instalacji oprogramowania Pi-hole. Nie będzie to skomplikowane, ponieważ jego twórcy przygotowali dla nas skrypty, które przeprowadzą nas krok po kroku przez ten proces. Wpisujemy komendę, której wynikiem będzie pobranie ze strony producenta skryptu instalacyjnego i jego uruchomienie:

```
curl -sSL https://install.pi-hole.net | sudo bash
```

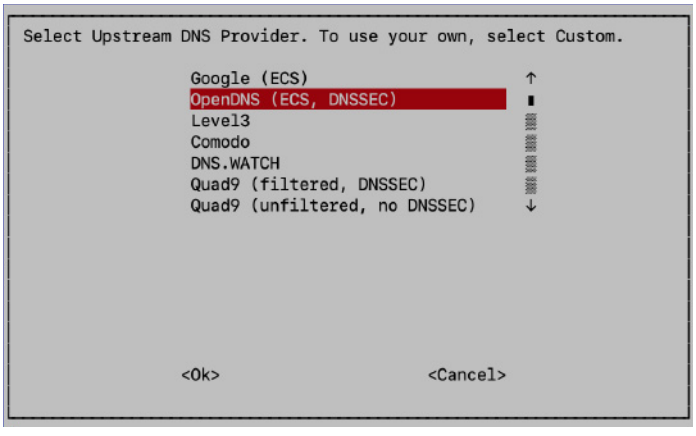
Podczas instalacji skrypt będzie zadawał nam pytania i informował o postępie prac. Większość ekranów sprowadza się do kliknięcia przycisku „OK" i akceptacji zaproponowanych przez instalator parametrów.

Warto jednak zwrócić szczególną uwagę na ekran „Select Upstream DNS Provider". Musimy podjąć tu bardzo ważną decyzję. Otóż skąd nasz serwer ma mieć całą



Ilustracja 3. Instalator „Pi-hole'

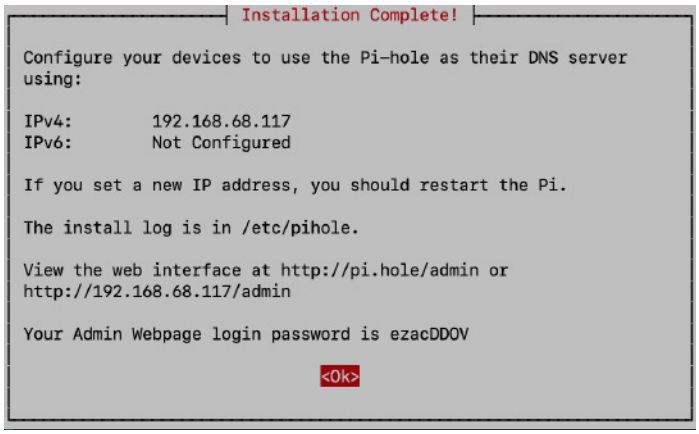
wiedzę o domenach i przypisanych im adresach IP? DNS to sieć hierarchiczna. Dlatego też jej członkowie wymieniają pomiędzy sobą informacje o domenach. Są w tej sieci serwery wyższego rzędu (ważniejsze), od których te niższego rzędu pobierają informacje. Taki właśnie serwer musimy teraz wybrać. Ja na potrzeby tego projektu wybrałem serwery OpenDNS, które są szybkie i nie zbierają danych o użytkownikach. Godną uwagi opcją jest także Quad9 – to serwery amerykańskie, które dodatkowo szczycą się tym, że bronią nas przed stronami ze złośliwym oprogramowaniem. Nie jest to dla nas aż tak istotne, ponieważ w ramach tego projektu zbudujemy samodzielnie taką usługę, ale będzie ona koncentrowała się w szczególności na zagrożeniach dla użytkowników z naszego kraju.



Ilustracja 4. Wybór nadrzędnego serwera DNS

Przez kolejne ekrany przechodzimy, akceptując sugerowane przez instalator ustawienia. Na końcu instalacji

zobaczymy ekran „Installation Complete!”. Znajdziemy tu adres panelu WWW, z którego możemy skorzystać do zalogowania się na nasz Pi-hole, jak również hasło (które warto sobie skopiować na bok i zachować).



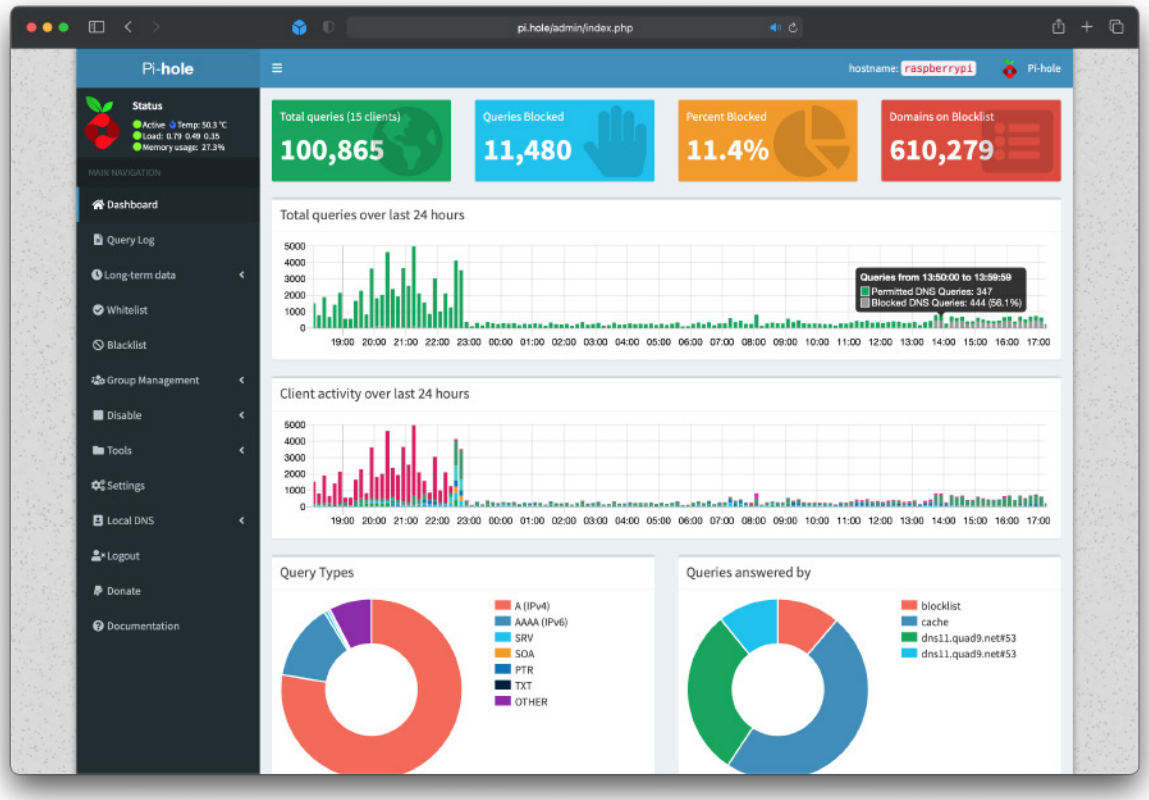
Ilustracja 5. Ekran z podsumowaniem

LOGUJEMY SIĘ DO PI-HOLE

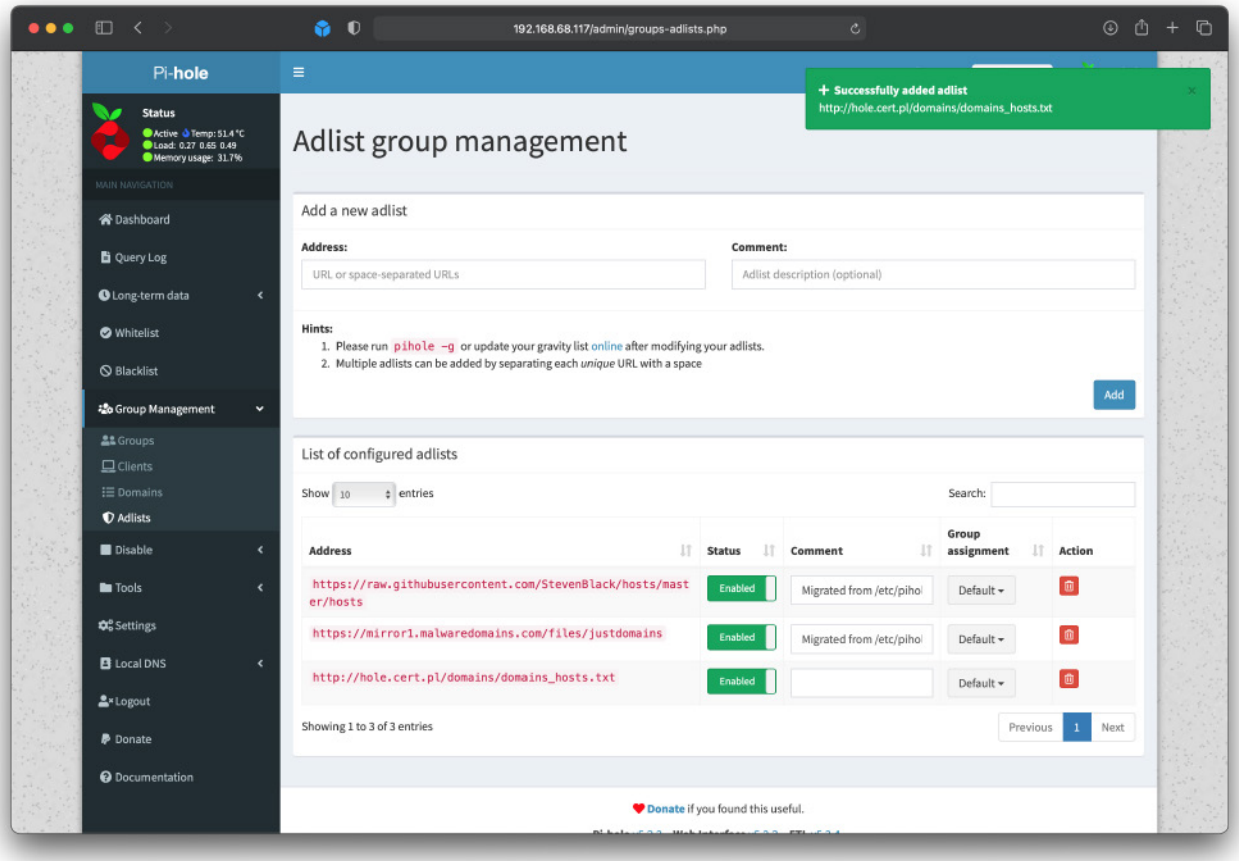
Przyszedł czas, aby zalogować się do naszego nowego serwera DNS i skonfigurować go pod nasze potrzeby. W tym celu otwieramy przeglądarkę internetową i w pasku wpisujemy adres podany na ekranie z podsumowania instalacji. W moim przypadku będzie to http://192.168.68.117/admin. Na głównym ekranie zobaczymy podstawowe statystyki ruchu (które w chwili obecnej są puste, ale nie ma się co martwić). Klikamy przycisk „login” w menu po lewej stronie i podajemy hasło. Na Ilustracji 6 pokazana jest moja instalacja Pi-hole po kilku dniach używania. Jak widać, istotny odsetek ruchu jest blokowany. Nie są to tylko strony wyłudzające dane, ale również różne hosty odpowiedzialne za szpiegowanie, analitykę ruchu czy męczące reklamy.

LISTA OSTRZEŻEŃ PRZED NIEBEZPIECZNYMI STRONAMI OD CERT POLSKA

CERT Polska (Computer Emergency Response Team) to zespół odpowiedzialny za rejestrowanie i obsługę zdarzeń, które naruszają bezpieczeństwo sieci. Działa on w strukturach Naukowej i Akademickiej Sieci Komputerowej (NASK) i zajmuje się aktywnym reagowaniem w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników In-



Ilustracja 6. Panel administratora po zalogowaniu



Ilustracja 7. Dodawanie listy złośliwych domen

ternetu. Wspólnie z operatorami telekomunikacyjnymi CERT prowadzi walkę ze stronami wyłudzającymi dane osobowe czy też dane do logowania. CERT zajmuje się monitoringiem i identyfikacją złośliwych stron, a także udostępnia formularz (dostępny na stronie internetowej https://incydent.cert.pl/phishing), który pozwala każdemu internaucie na zgłaszanie zagrożenia.

Lista domen identyfikowanych jako złośliwe jest publicznie dostępna i aktualizowana co 5 minut. Wykorzystamy ją, aby nasz serwer DNS pobierał, a następnie blokował podejrzane adresy, broniąc nas tym samym przed zagrożeniami. Lista dostępna jest w różnych formatach (między innymi zwykły tekst, JSON, XML). My wykorzystamy format „hosts", który będzie zrozumiały dla serwera DNS.

Rozwijamy menu „Group Management", które znajduje się po lewej stronie naszego panelu Pi-hole, a następnie wybieramy opcję „Adlists". W polu „Address" wpisujemy: http://hole.cert.pl/domains/domains_hosts.txt i klikamy przycisk „Add" (Ilustracja 7).

Aby lista została pobrana i przetworzona przez nasz serwer, należy wejść w menu „Tools", a następnie „Update Gravity" i kliknąć przycisk „Update". To jednorazowa czynność, dzięki której wszystkie niezbędne listy zostaną pobrane i uwzględnione w konfiguracji blokowania domen. Standardowo lista ta będzie aktualizowana przez nasz serwer automatycznie raz w tygodniu. Jeżeli jesteśmy użytkownikiem zaawansowanym i chcemy zmienić ten interwał, należy zalogować się z użyciem SSH na nasz serwer, a następnie zmodyfikować ustawienia CRON w katalogu /etc/cron.d. Ja na swoje potrzeby ustawiłem aktualizację raz na 24 godziny.

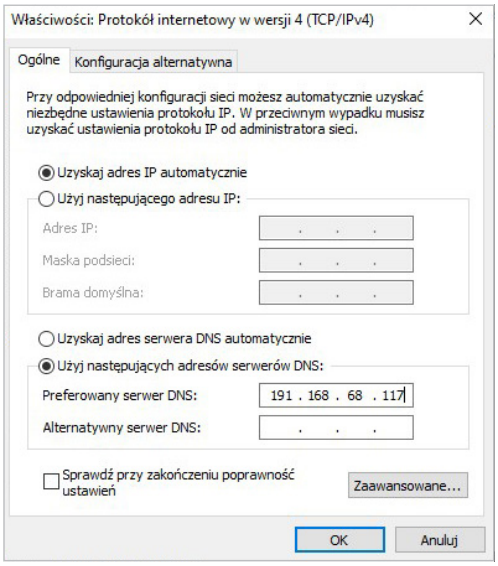
Nasz serwer działa i jest gotowy do obsługi naszych zapytań o domeny.

KONFIGURACJA KOMPUTERA I SIECI

Pozostało nam jedynie zmusić nasz komputer (lub wszystkie komputery w sieci domowej) do wykorzystywania nowego serwera DNS. Aby zrobić to na swo-

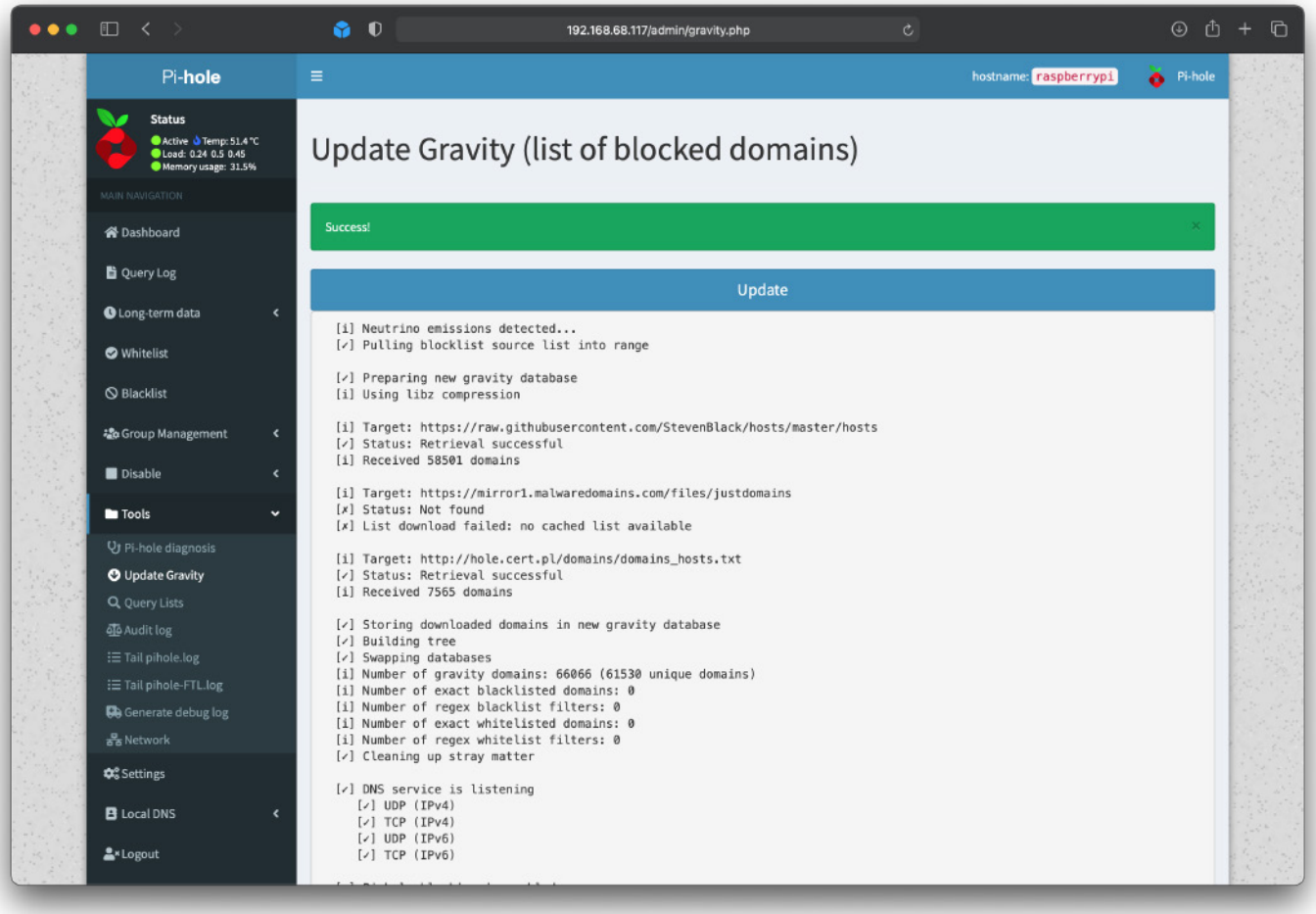
im komputerze, należy zmienić ustawienia połączenia sieciowego i podać adres IP naszego serwera. Czynność ta wykonywana jest inaczej w zależności od systemu operacyjnego.

W przypadku systemów Windows 10 można to zrobić poprzez *Panel Sterowania -> Sieć i Internet -> Połączenia sieciowe*. Należy kliknąć prawym przyciskiem myszy połączenie sieciowe, z którego korzystamy (może się nazywać na przykład Wi-Fi), wybrać opcję „Właściwości", zaznaczyć pozycję „Protokół internetowy w wersji 4 (TCP/IPv4)" i kliknąć „Właściwości". Zaznaczamy opcję „Użyj następujących adresów serwerów DNS", a następnie wpisujemy adres naszego serwera. Operację zatwierdzamy, klikając przycisk „OK". Więcej o zmianie ustawień protokołu TCP/IP można przeczytać na stronie Microsoftu: https://support.microsoft.com/pl-pl/windows/zmienianie-ustawień-protokołu-tcp-ip-bd0a07af-15f5-cd6a-363f-ca2b6f391ace.



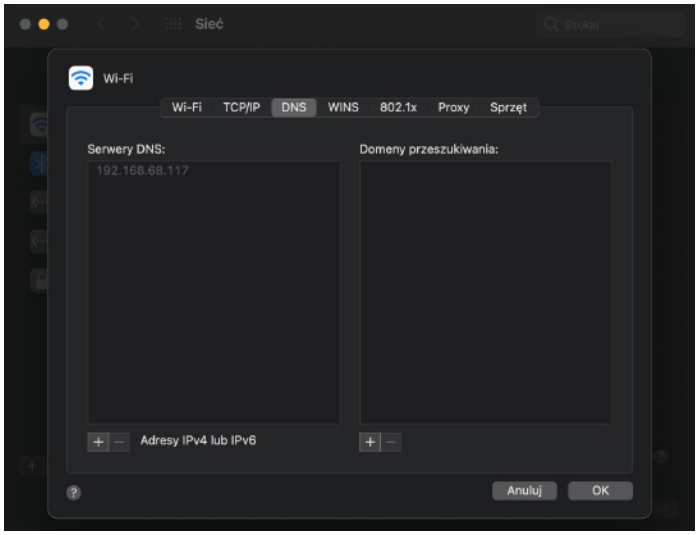
Ilustracja 9. Konfiguracja „DNS" w systemie Windows 10

W przypadku komputera z systemem macOS klikamy *Preferencje systemowe -> Sieć*. Wybieramy nasze połą-



Ilustracja 8. Pobranie list złośliwych domen

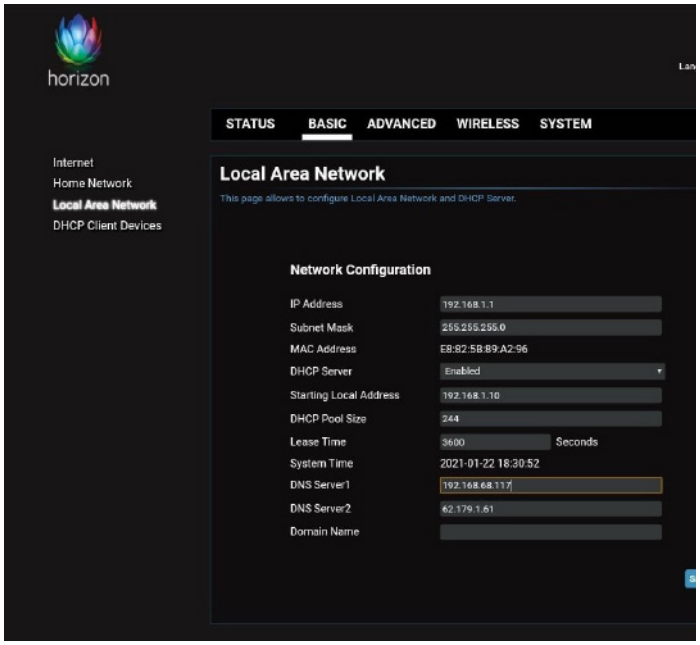
czenie sieciowe z menu po lewej stronie (na przykład Wi-Fi), klikamy przycisk „Zaawansowane” i w zakładce DNS podajemy adres naszego serwera. Więcej na temat ustawień sieci można znaleźć na stronach firmy Apple: https://support.apple.com/pl-pl/guide/mac-help/mchlp2718/mac.



Ilustracja 10. Konfiguracja „DNS” w systemie „macOS Big Sur”

To wszystko. Nasz komputer powinien już korzystać z postawionego przez nas serwera DNS i blokować złośliwe strony. Poprawne działanie naszej konfiguracji możemy sprawdzić poprzez zalogowanie się do panelu administracyjnego. Powinniśmy tam zobaczyć listę domen, z którymi łączy się nasz komputer.

Jeżeli chcemy, aby wszystkie nasze domowe urządzenia korzystały z nowego serwera Pi-hole, musimy zmienić ustawienia routera, podając w ustawieniach DNS adres IP Raspberry Pi. Dzięki takiej konfiguracji nasz router za pomocą protokołu DHCP (Dynamic Host Configuration Protocol) będzie przyznawał urządzeniom w sieci lokalnej ich adresy IP wraz ze wskazaniem adresu IP naszego serwera DNS. Jak to skonfigurować? Nie ma tu niestety uniwersalnej instrukcji i w zależności od wykorzystywanego modelu musisz samodzielnie poszukać dokumentacji do swojego urządzenia.



Ilustracja 11. Przykładowa konfiguracja routera

Łukasz Basa

Bezpiecznik, entuzjasta technologii, miłośnik alternatywnych metod parzenia kawy.

KONTAKT@BEZPIECZNY.BLOG
HTTPS://BEZPIECZNY.BLOG

ZAPAMIĘTAJ

- Protokół DNS służy do tłumaczenia domen internetowych na adresy IP.
- Warto używać serwerów DNS, które zapewniają ci dodatkową ochronę przed złośliwymi stronami WWW.

ĆWICZ W DOMU

- Spróbuj wykorzystać swój nowy serwer DNS do blokowania natrętnych reklam lub innych stron, które nie są mile widziane w twojej sieci.
- Zajrzyj do logów w panelu serwera i zobacz, jak wiele zapytań generuje twój komputer, gdy wchodzi na stronę internetową.