

# Bezpieczeństwo komputerowe - lista druga

Bartosz Rajczyk, Paweł Wilkosz

27 października 2019

## 1 Wstęp

Opisane w sprawozdaniu statystyki zostały zebrane przy pomocy programu Wireshark, przy użyciu dwóch metod - nasłuchiwanie samodzielnie utworzonych sieci bezprzewodowych z trzema różnymi SSID oraz nasłuchiwanie wszystkich otwartych sieci po uprzednim ustawieniu karty sieciowej w tryb monitorowania. Wszystkie badania zostały wykonane w Pasażu Grunwaldzkim we Wrocławiu.

## 2 Nazwy sieci poszukiwane przez klientów

Ustawiając kartę sieciową w tryb monitorowania i używając programu Wireshark do przechwycenia tzw. "probe request" zawierających informacje o poszukiwanych sieciach bezprzewodowych zgodnie z protokołem 802.11, mogliśmy sporządzić statystykę dotyczącą popularności sieci automatycznie wyszukiwanych przez urządzenia. Następnie przy pomocy programu TShark z parametrami `-Y 'wlan.fc.type_subtype eq 4' -T fields -e wlan.ssid` wyodrębniliśmy SSID tych sieci.

SSID	poszukiwania
Ø	32039
KFC Hostspot	920
PizzaHut Hotspot	433
eduroam	219
Sydorenko Corp.	219
SaskTel Select Wi-Fi 1	209
5099251212	206
McD-Hotstop	185
kurzawy	121
*Pasaz Grunwaldzki free WiFi*	117
pasaz	111
Aquami	81

Tabela 1: najpopularniejsze poszukiwane SSID sieci

Pierwszy rząd z pustą nazwą sieci to tzw. "SSID Wildcart" pozwalający na dopasowanie dowolnej nazwy sieci. Z przeprowadzonych obserwacji wynika, że najpopularniejsze wyszukiwane nazwy należą do darmowych sieci znajdujących się w pobliżu oraz sieci firmowych. Pośród mniej popularnych SSID można wskazać chociażby:

- TP-Link\_A736-5G - 40 wyszukiwań, najpewniej podstawowa nazwa sieci pochodząca z konkretnego modelu routera
- AndroidAP - 20 wyszukiwań, podstawowa nazwa sieci utworzonej na telefonie z systemem Android

- warszawa centrum - 55 wyszukikań, najpewniej ktoś wsiadł do złego pociągu, bo to na "W" i tamto na "W"

Listę popularności zamykają sieci domowe o bardzo specyficznych nazwach, jak chociażby:

- The King is back - 1 wyszukiwanie
- PatrykToCh.j - 15 wyszukikań
- emilia.zegadlowicza - 4 wyszukiwania

### 3 Połączeni klienci

Przy pomocy zakładki "Statystyka" w programie WireShark można sporządzić listę unikalnych adresów MAC podłączonych do każdej z utworzonych sieci. Poniższa tabela przedstawia porównanie tej liczby pomiędzy sieciami.

nazwa sieci	połączeni klienci
Wrocław Free WiFi	48
Pasaż Grunwaldzki (staff only)	30
Free Wifi Pasaż	21

Tabela 2: liczba klientów w sieciach

### 4 Strony odwiedzane przez klientów

Odwiedzane witryny ustaliłem na podstawie zapytań DNS. Listę wszystkich nazw hosta z zapytań DNS uzyskałem używając programu TShark na odpowiednich plikach z parametrami `-T fields -Y dns -e dns.qry.name`, a następnie używając skryptu podliczyłem wystąpienia każdej z witryn.

strona	Free Wifi	Pasaż (staff)	Wrocław Free
connectivitycheck.gstatic.com	48	14	189
www.google.com	17	5	227
mtalk.google.com	10	0	53
portal.fb.com	10	0	43
client.wns.windows.com	0	14	0
www.facebook.com	0	0	24

Tabela 3: przykładowe popularne adresy

Możemy przyjrzeć się dokładniej najpopularniejszym adresom z sieci Pasaż (staff) oraz Wrocław Free Wifi:

strona	liczba zapytań
3.0.0.0...0.0.2.0.f.f.ip6.arpa	55
252.0.0.224.in-addr.arpa	47
1.0.42.10.in-addr.arpa	45
250.255.255.239.in-addr.arpa	20
clients4.google.com	19
251.0.0.224.in-addr.arpa	18
2.0.0.0.1...2.0.f.f.ip6.arpa	17
dns.msftncsi.com	16

Tabela 4: najpopularniejsze adresy z Pasaż Staff

strona	liczba zapytań
www.google.com	227
connectivitycheck.gstatic.com	189
datasaver.googleapis.com	97
graph.facebook.com	64
proxy.googlezip.net	61
check.googlezip.net	54
mtalk.google.com	53
clients1.google.com	48

Tabela 5: najpopularniejsze adresy z Wrocław Free Wifi

## 5 Protokoły

Listę protokołów używanych w sieci uzyskaliśmy przy pomocy programu TShark z argumentami `-T fields -e frame.protocols`. Uzyskane wyniki:

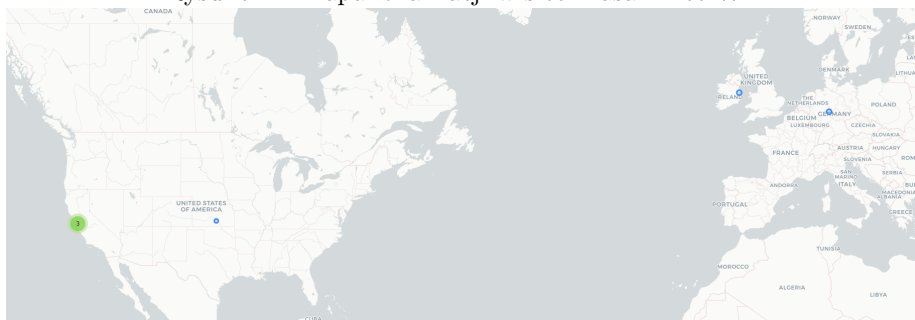
1. SSDP
2. ICMP
3. ARP
4. DNS
5. HTTP
6. TLS1.2
7. TLS1.3
8. MDNS

W wynikach pojawiło się także wiele innych podprotokołów specjalizujących wykorzystanie tamtych. Niestety jedyną stroną, do której udałooby nam się uzyskać nieuprawniony dostęp poprzez login i hasło przesłane bez szyfrowania byłaby strona `cs.pwr.edu.pl/gebala/dyd/` należąca do doktora Gębali, z której testowo pobraliśmy listy zadań. W programie WireShark podgląd pakietu dotyczącego tego zapytania ujawnia typ autoryzacji "Basic" wraz z odpowiednim loginem oraz hasłem.

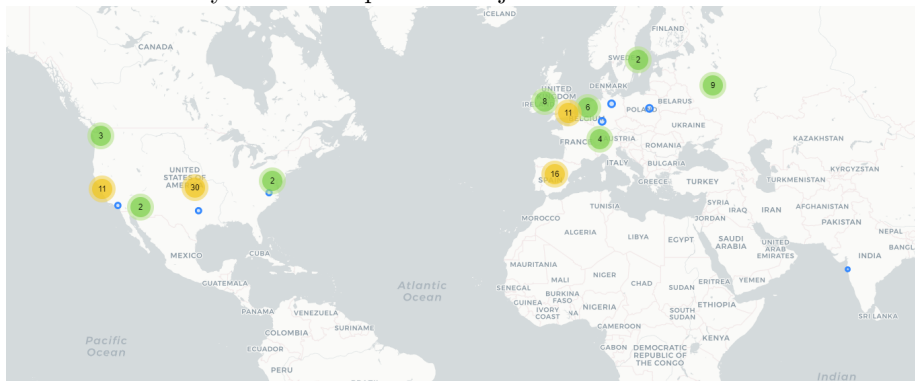
## 6 Mapy lokalizacji

Używając baz danych GeoIP2 dodanych do programu WireShark możemy generować mapy lokalizacji endpointów, z którymi łączyły się rejestrowane urządzenia.

Rysunek 1: mapa lokalizacji w sieci Pasaż Free Wifi



Rysunek 2: mapa lokalizacji w sieci Pasaż Staff



Jak widać, większość połączeń wysyłana jest do Europy oraz Stanów Zjednoczonych, aczkolwiek znalazły się pojedyncze wypadku zapytań np. do Indii.

The map shows the following distribution of COVID-19 cases by country:

- Green (1-5 cases):** Austria (1), Belgium (1), Bulgaria (1), Czechia (1), France (1), Germany (1), Hungary (1), Italy (1), Luxembourg (1), Norway (1), Slovakia (1), Spain (1), Sweden (1), Switzerland (1), United Kingdom (1), United States (1), and the United States of America (1).
- Blue (6-10 cases):** Canada (6), Denmark (6), Finland (6), Greece (6), Ireland (6), Israel (6), Japan (6), Korea (6), Lithuania (6), Netherlands (6), Poland (6), Portugal (6), Romania (6), Serbia (6), Slovenia (6), and the United States of America (6).
- Yellow (11-15 cases):** Canada (11), France (11), Germany (11), Italy (11), and the United States of America (11).
- Orange (16-20 cases):** Canada (16), France (16), Germany (16), Italy (16), and the United States of America (16).

Z przeprowadzonych eksperymentów i analiz wynika, że ludzie nie zwracają wielkiej uwagi na to, w jakiej sieci się znajdują i kto obserwuje przesyłane przez nich dane. Mimo tego że nie udało nam się przechwycić żadnych poufnych informacji, to pozostając w miejscu publicznym z otwartą siecią przez odpowiednio długi czas rośnie prawdopodobieństwo, że zawierający je pakiet zostanie przez nas zarejestrowany. Dodatkowo udało nam się zebrać mnóstwo meta-informacji dotyczących stron odwiedzanych przez ludzi, a nawet nazw ich prywatnych, domowych sieci WiFi, co umożliwiłoby profilowanie ich i wykorzystanie tych danych do niecných celów.