Bezpieczeństwo Komputerowe - lista 1, zadanie 1

Mateusz Kalinowski

28 października 2018

1 Opis:

Najwięcej urządzeń łączyło się do udostępnianych sieci o nazwach sieci znanych i zaufanych miejsc, przykładowo *KFC Wifi, McDonalds Wifi, PasażGrunwaldzki Wifi*. Do innych sieci, których nazwy nie wzbudzały zaufania użytkownicy łączyli się rzadko lub wcale, przykładowo *Iphone(Mateusz), darmoweWifi*. Najwięcej jednak było użytkowników w sieciach ogólnodostępnych udostępnianych przez miejsca publiczne, miały one najlepszy zasięg i największe zaufanie.

Do analizy statystyk bierzemy najbardziej interesujący plik z największą ilością wejść, nasłuchiwanie miało miejsce pd ogólnodostępną siecią w Pasażu Grunwaldzkim.

2 Statystyki:

Liczba użytkowników - liczbę użytkowników w danej sieci podczas danego nasłuchiwania można uzyskać łatwo przy pomocy przefiltrowania protokołu dns. Dokładne numery ip uzytkowników możemy uzyskać w poniższy sposób:

Komenda: `tshark -r file.pcap -T fields -e ip.src -Y "dns.flags.response eq 0" | sort | uniq`

Aby dostać dokładną liczbę należy przepuścić output przez potok wc -l. Z nasłuchiwaną siecią połączonych było 12 użytkowników.

Odwiedzane strony - samą informację o stronach na które wchodzili użytkownicy możemy otrzymać również poprzez przefiltrowanie protokołów DNS. Czyli po prostu sprawdzenie jakie adresy ip obługiwane były przez serwery DNS podczas nasłuchiwania.

Komenda: `tshark -r file.pcap -T fields -e dns.qry.name -Y "dns.flags.response eq 0" | sort | uniq`

Komenda ta zwraca unikatową listę stron, z którymi łączyli sie użytkownicy. Możemy zauważyć na jak różnorodne strony wchodzili użytkownicy. Wśród wyszukiwań możemy zauważyć najpopularniejsze strony takie jak *youtube.com, google.com, facebook.com, instagram.com* jak również różnego rodzaju strony z newsami i wiadomościami takie jak *wprost.com, weszło.com, interia.pl*, można również zauważyć dość nietypowe i mniej popularne strony jak *maxior.pl, umk.pl,...*

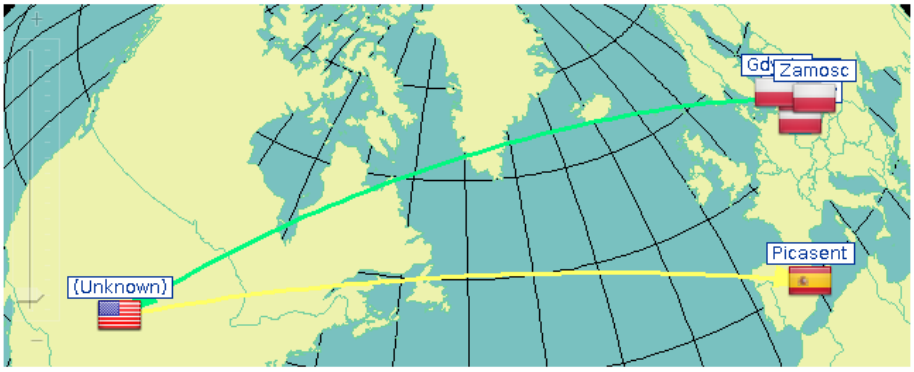
Wykorzystane protokoły i usługi - Większość użytkowników używała protokołu HTTPS czyli wersji HTTP zabezpieczonej protokołem TLS, przez ta-

kie połączenie nie udało sie bezpośrednio dostać do danych użytkowników. Praktycznie wszystkie strony obecnie używają protokołu HTTPS, zdarzają się jednak strony które używają jeszcze niezabezpieczonej wersji HTTP. W takie sytuacji jawne są hasła użytkowników przesyłane metodą HTTP POST, czy ciasteczka z id sesji przesyłane podczas żądania HTTP GET. Można również przejrzeć wszystkie zdjęcia i filmiki pobierane przez użytkowników.

strona	możliwe do uzyskania dane	używany protokół
gry.pl	id sesji z ciasteczek, dane logowania	HTTP
giercownia.pl	id sesji z ciasteczek	HTTP
weszło.com	dane z rejestracji, logowania, id sesji	HTTP
soso.com	wyszukiwane frazy	HTTP
facebook.com	-	HTTPS
google.com	-	HTTPS
...	-	

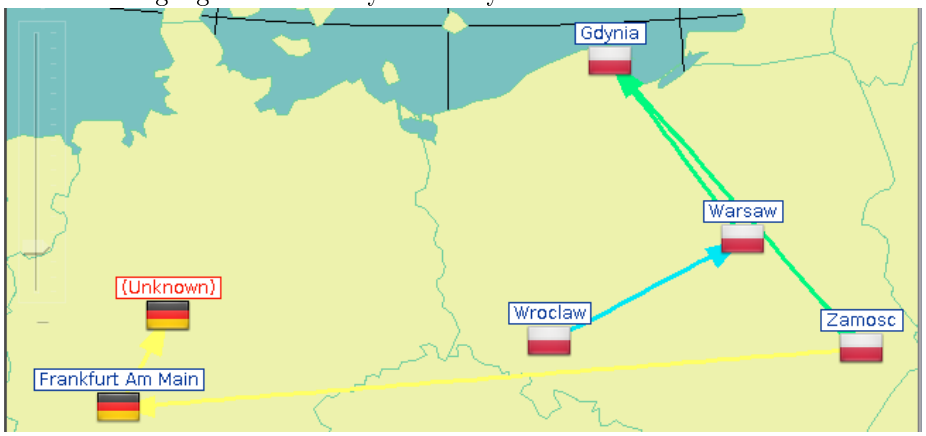
Ponadto można znaleźć chińską przeglądarkę *soso.com* korzystającą dalej z protokołu HTTP w której można przejrzeć szukane frazy filtrem `http.host==soso.com`.

Lokalizacje serwerów - Informacje z jakimi lokalizacjami łączyły sie komputery są łatwo dostępne w programie visual route, po wpisaniu nazwy wyszukiwanego hosta.



weszlo.com - polska strona sportowa

google.com - amerykańska wyszukiwarka internetowa



wprost.pl - polski serwis informacyjny