

# Ślady w sieci

Piotr Kucharski

Szkoła Główna Handlowa  
indeks 7431

Społeczeństwo informacyjne, 2007



# Spis

- 1 Logi
  - Dostawca sieci
  - Usługodawcy
  - Inni
- 2 Ślady
  - Strony WWW
  - Sygnalizatory
  - Adres IP
  - Aktywność w sieci
- 3 Zagrożenia i ucieczki



# Dostawca sieci

Prawnie zobligowany do wiedzy:

- kto (komputer lub lokal)
- kiedy
- gdzie

## DHCP

```
lease 194.145.104.252 {  
  starts 5 2007/02/02 16:01:10;  
  ends 5 2007/02/02 17:01:10;  
  hardware ethernet 00:30:05:fc:f7:28;  
  set x-vendor-class = "MSFT 5.0"; }
```



# Dostawca sieci

Prawnie zobligowany do wiedzy:

- kto (komputer lub lokal)
- kiedy
- gdzie

## logi sesji

```
1170623315.819799 IP 194.145.109.200.1356  
> 194.145.96.51.8080: S 2128169041:2128169041(0) win  
65535 <mss 1460,nop,nop,sackOK>  
1170623315.819799 = Sun Feb 4 22:08:35 2007
```



# Dostawca sieci

Prawnie zobligowany do wiedzy:

- kto (komputer lub lokal)
- kiedy
- gdzie

## logi sesji

```
1170623315.819799 IP 194.145.109.200.1356  
> 194.145.96.51.8080: S 2128169041:2128169041(0) win  
65535 <mss 1460,nop,nop,sackOK>
```



# Usługodawcy

- kto (IP)
- kiedy
- co robił (co ściągał, wysyłał)
- dodatkowe informacje zależne od protokołu  
wielkość listu, status, przeglądarka...

## log serwera pocztowego

```
Jan 22 12:43:50 postfix  
E0D282ABF98:  
client=194.145.106.93  
from=<mgol@sgh.waw.pl>,  
to=<chopin@sgh.waw.pl>,  
size=1507, delay=50,  
status=sent
```

## log serwera WWW

```
87.205.88.151 - -  
[14/Feb/2007:18:35:32 +0100]  
"GET /index.php HTTP/1.1"  
200 2472 "-" "Opera/9.02  
(Windows NT)"
```



# Usługodawcy

- kto (IP)
- kiedy
- co robił (co ściągał, wysyłał)
- dodatkowe informacje zależne od protokołu  
wielkość listu, status, przeglądarka...

## log serwera pocztowego

```
Jan 22 12:43:50 postfix  
E0D282ABF98:  
client=194.145.106.93  
from=<mgol@sgh.waw.pl>,  
to=<chopin@sgh.waw.pl>,  
size=1507, delay=50,  
status=sent
```

## log serwera WWW

```
87.205.88.151 - -  
[14/Feb/2007:18:35:32 +0100]  
"GET /index.php HTTP/1.1"  
200 2472 "-" "Opera/9.02  
(Windows NT)"
```



# Usługodawcy

- kto (IP)
- kiedy
- co robił (co ściągał, wysyłał)
- dodatkowe informacje zależne od protokołu  
wielkość listu, status, przeglądarka...

## log serwera pocztowego

```
Jan 22 12:43:50 postfix  
E0D282ABF98:  
client=194.145.106.93  
from=<mgol@sgh.waw.pl>,  
to=<chopin@sgh.waw.pl>,  
size=1507, delay=50,  
status=sent
```

## log serwera WWW

```
87.205.88.151 - -  
[14/Feb/2007:18:35:32 +0100]  
"GET /index.php HTTP/1.1"  
200 2472 "-" "Opera/9.02  
(Windows NT)"
```



# Usługodawcy

- kto (IP)
- kiedy
- co robił (co ściągał, wysyłał)
- dodatkowe informacje zależne od protokołu  
wielkość listu, status, przeglądarka...

## log serwera pocztowego

```
Jan 22 12:43:50 postfix  
E0D282ABF98:  
client=194.145.106.93  
from=<mgol@sgh.waw.pl>,  
to=<chopin@sgh.waw.pl>,  
size=1507, delay=50,  
status=sent
```

## log serwera WWW

```
87.205.88.151 - -  
[14/Feb/2007:18:35:32 +0100]  
"GET /index.php HTTP/1.1"  
200 2472 "-" "Opera/9.02  
(Windows NT)"
```



## Osoby trzecie

Na szczęście z pewnymi ograniczeniami (np. wspólna sieć lub uprzednie zawirusowanie komputera użytkownika)

- podłuchiwanie transmisji (w tym hasła, jeśli ruch nieszyfrowany)
- szpiegowanie (spyware, trojany) użytkownika na jego komputerze (logowanie jego działań, m.in. wpisywanych PIN-ów)
- oszukiwanie użytkowników przy pomocy fałszywych stron (i wyciąganie w ten sposób haseł do kont bankowych)



## Osoby trzecie

Na szczęście z pewnymi ograniczeniami (np. wspólna sieć lub uprzednie zawirusowanie komputera użytkownika)

- podsłuchiwanie transmisji (w tym hasła, jeśli ruch nieszyfrowany)
- szpiegowanie (spyware, trojany) użytkownika na jego komputerze (logowanie jego działań, m.in. wpisywanych PIN-ów)
- oszukiwanie użytkowników przy pomocy fałszywych stron (i wyciąganie w ten sposób haseł do kont bankowych)



## Osoby trzecie

Na szczęście z pewnymi ograniczeniami (np. wspólna sieć lub uprzednie zawirusowanie komputera użytkownika)

- podsłuchiwanie transmisji (w tym hasła, jeśli ruch nieszyfrowany)
- szpiegowanie (spyware, trojany) użytkownika na jego komputerze (logowanie jego działań, m.in. wpisywanych PIN-ów)
- oszukiwanie użytkowników przy pomocy fałszywych stron (i wyciąganie w ten sposób haseł do kont bankowych)



# Ciasteczka (cookies)

Ułatwiają korzystanie z serwisu, pozwalają śledzić użytkownika, czasem w złych celach;

## Cookie: logged

Name	logged
Value	TRUE
Host	www.esgieha.pl
Path	/
Secure	No
Expires	At End Of Session

## Cookie: login

Name	login
Value	chopin
Host	www.esgieha.pl
Path	/
Secure	No
Expires	At End Of Session



# Ciasteczka (cookies)

Ułatwiają korzystanie z serwisu, pozwalają śledzić użytkownika, czasem w złych celach;

## Cookie: logged

Name	logged
Value	TRUE
Host	www.esgieha.pl
Path	/
Secure	No
Expires	At End Of Session

## Cookie: login

Name	login
Value	chopin
Host	www.esgieha.pl
Path	/
Secure	No
Expires	At End Of Session



# Ciasteczka (cookies)

Ułatwiają korzystanie z serwisu, pozwalają śledzić użytkownika, czasem w złych celach;  
a czasem stwarzają zagrożenie (lokalna edycja)

## Cookie: logged

Name	logged
Value	TRUE
Host	www.esgieha.pl
Path	/
Secure	No
Expires	At End Of Session

## Cookie: login

Name	login
Value	mgol
Host	www.esgieha.pl
Path	/
Secure	No
Expires	At End Of Session



# Strony WWW

**skrypty** (Javascript, VBScript) wykonywane po stronie klienta przy przeglądaniu stron WWW pozwalają na zbieranie różnych informacji

**formularze** użytkownicy sami wpisują w formularze na stronach swoje dane, często poufne!

**wyszukiwarki** przy pomocy cookie i/lub IP można połączyć wyszukiwane frazy z użytkownikiem

**google** google, google mail, google desktop, google images, google video, picassa – wszystkie jaja w jednym koszyku?



# Strony WWW

**skrypty** (Javascript, VBScript) wykonywane po stronie klienta przy przeglądaniu stron WWW pozwalają na zbieranie różnych informacji

**formularze** użytkownicy sami wpisują w formularze na stronach swoje dane, często poufne!

**wyszukiwarki** przy pomocy cookie i/lub IP można połączyć wyszukiwane frazy z użytkownikiem

**google** google, google mail, google desktop, google images, google video, picassa – wszystkie jaja w jednym koszyku?



# Strony WWW

**skrypty** (Javascript, VBScript) wykonywane po stronie klienta przy przeglądaniu stron WWW pozwalają na zbieranie różnych informacji

**formularze** użytkownicy sami wpisują w formularze na stronach swoje dane, często poufne!

**wyszukiwarki** przy pomocy cookie i/lub IP można połączyć wyszukiwane frazy z użytkownikiem

**google** google, google mail, google desktop, google images, google video, picassa – wszystkie jaja w jednym koszyku?



# Strony WWW

**skrypty** (Javascript, VBScript) wykonywane po stronie klienta przy przeglądaniu stron WWW pozwalają na zbieranie różnych informacji

**formularze** użytkownicy sami wpisują w formularze na stronach swoje dane, często poufne!

**wyszukiwarki** przy pomocy cookie i/lub IP można połączyć wyszukiwane frazy z użytkownikiem

**google** google, google mail, google desktop, google images, google video, picassa – wszystkie jaja w jednym koszyku?



## Sygnalizatory (beacons)

- Niewielkie lub niewidoczne elementy graficzne w mailach sformatowanych jako HTML
- URL-e "wypisz się z mailingu" służące potwierdzeniu otrzymania mailingu, żeby z większą pewnością spamować na ten adres

### obrazek

```

```



## Sygnalizatory (beacons)

- Niewielkie lub niewidoczne elementy graficzne w mailach sformatowanych jako HTML
- URL-e "wypisz się z mailingu" służące potwierdzeniu otrzymania mailingu, żeby z większą pewnością spamować na ten adres

### złudne wypisanie

Click `<a href="http://bookltd6.net/unsub.php?e=chopin@sgh.waw.pl&m=2721100">here</a>` to unsubscribe.

proszę tam za mnie nie wchodzić



# Adres IP

Tłumaczenie adresu IP na nazwę może wiele powiedzieć:

## nazwa

62.87.148.47	⇒	tvk_gaj-2-46.wroclaw.dialog.net.pl.
194.145.104.81	⇒	NT-F-0510-02.nt.sgh.waw.pl.
213.25.55.153	⇒	pp153.warszawa.sdi.tpnet.pl.
89.171.67.2	⇒	gw-nat.mokotowplaza.waw.pl.



# Adres IP

Instytucje rejestrujące adresy: RIPE, ARIN, APNIC.

## RIPE: whois 194.145.104.81

inetnum	194.145.96.0 - 194.145.111.255
netname	SGH-PL
descr	Szkoła Główna Handlowa
admin-c	PIKU1-RIPE
address	Centrum Informatyczne
address	Al. Niepodleglosci 162
fax-no	+48 22 849 5312
e-mail	chopin@sgh.waw.pl



# Ślady aktywności

Aktywność kreatywna zostawia ślady czasem na zawsze:

- stare strony WWW (Wayback Machine)

<http://web.archive.org/>

- stare postingi na Usenet:

<http://groups.google.com/>

Inne ślady:

- podpis cyfrowy musi być sprawdzany za każdym razem, czy nie jest nieważny
- stare logi przeglądanych stron
- udostępnione dokumenty na komputerze domowym



# Ślady aktywności

Aktywność kreatywna zostawia ślady czasem na zawsze:

- stare strony WWW (Wayback Machine)  
<http://web.archive.org/>
- stare postingi na Usenet:  
<http://groups.google.com/>

Inne ślady:

- podpis cyfrowy musi być sprawdzany za każdym razem, czy nie jest nieważny
- stare logi przeglądanych stron
- udostępnione dokumenty na komputerze domowym



# Ślady aktywności

Aktywność kreatywna zostawia ślady czasem na zawsze:

- stare strony WWW (Wayback Machine)  
<http://web.archive.org/>
- stare postingi na Usenet:  
<http://groups.google.com/>

Inne ślady:

- podpis cyfrowy musi być sprawdzany za każdym razem, czy nie jest nieważny
- stare logi przeglądanych stron
- udostępnione dokumenty na komputerze domowym



# Ślady aktywności

Aktywność kreatywna zostawia ślady czasem na zawsze:

- stare strony WWW (Wayback Machine)  
`http://web.archive.org/`
- stare postingi na Usenet:  
`http://groups.google.com/`

Inne ślady:

- podpis cyfrowy musi być sprawdzany za każdym razem, czy nie jest nieważny
- stare logi przeglądanych stron
- udostępnione dokumenty na komputerze domowym



# Ślady aktywności

Aktywność kreatywna zostawia ślady czasem na zawsze:

- stare strony WWW (Wayback Machine)  
`http://web.archive.org/`
- stare postingi na Usenet:  
`http://groups.google.com/`

Inne ślady:

- podpis cyfrowy musi być sprawdzany za każdym razem, czy nie jest nieważny
- stare logi przeglądanych stron
- udostępnione dokumenty na komputerze domowym



# OS fingerprint

Inni często mogą sprawdzić wersję naszego systemu

- nmap (dowolna osoba znająca nasz adres IP)
- p0f (passive OS fingerprint, w trakcie korzystania z usługi)

## nmap

```
# nmap -O atlas.sgh.waw.pl
Running: Microsoft Windows NT/2K/XP|2003/.NET
OS details: Microsoft Windows 2003 Server,
2003 Server SP1 or XP Pro SP2
```



# Zagrożenia przy zostawianiu śladów

- upublicznienie informacji (konta, hasła)
- kradzież tożsamości
- śledzenie działań użytkownika w e-sferze



## Zagrożenia przy zostawianiu śladów

- upublicznienie informacji (konta, hasła)
- kradzież tożsamości
- śledzenie działań użytkownika w e-sferze



## Zagrożenia przy zostawianiu śladów

- upublicznienie informacji (konta, hasła)
- kradzież tożsamości
- śledzenie działań użytkownika w e-sferze



# Zapobieganie zostawianiu śladów

- wyłączenie cookies (zostawianie tylko tam, gdzie **my** chcemy)
- poczta przez remailery lub przeglądanie WWW przez proxy
- infrastruktura TOR (The Onion Ring)



## Zapobieganie zostawianiu śladów

- wyłączenie cookies (zostawianie tylko tam, gdzie **my** chcemy)
- poczta przez remailery lub przeglądanie WWW przez proxy
- infrastruktura TOR (The Onion Ring)



## Zapobieganie zostawianiu śladów

- wyłączenie cookies (zostawianie tylko tam, gdzie **my** chcemy)
- poczta przez remailery lub przeglądanie WWW przez proxy
- infrastruktura TOR (The Onion Ring)



# Podsumowanie

- w internecie, jak w życiu zostawiamy **ślady**
- ludzie **rzadko zdają sobie sprawę** z tego, jak wielkie ślady
- ale można się **schować...**
- ...choć **nie zawsze** jest po co



# Podsumowanie

- w internecie, jak w życiu zostawiamy ślady
- ludzie rzadko zdają sobie sprawę z tego, jak wielkie ślady
- ale można się schować...
- ...choć nie zawsze jest po co



# Podsumowanie

- w internecie, jak w życiu zostawiamy ślady
- ludzie rzadko zdają sobie sprawę z tego, jak wielkie ślady
- ale można się schować...
- ...choć nie zawsze jest po co



# Podsumowanie

- w internecie, jak w życiu zostawiamy ślady
- ludzie rzadko zdają sobie sprawę z tego, jak wielkie ślady
- ale można się schować...
- ...choć nie zawsze jest po co

