ANALIZA POWŁAMANIOWA OKIEM AMATORA – CASE STUDY

Piotr Jasiek

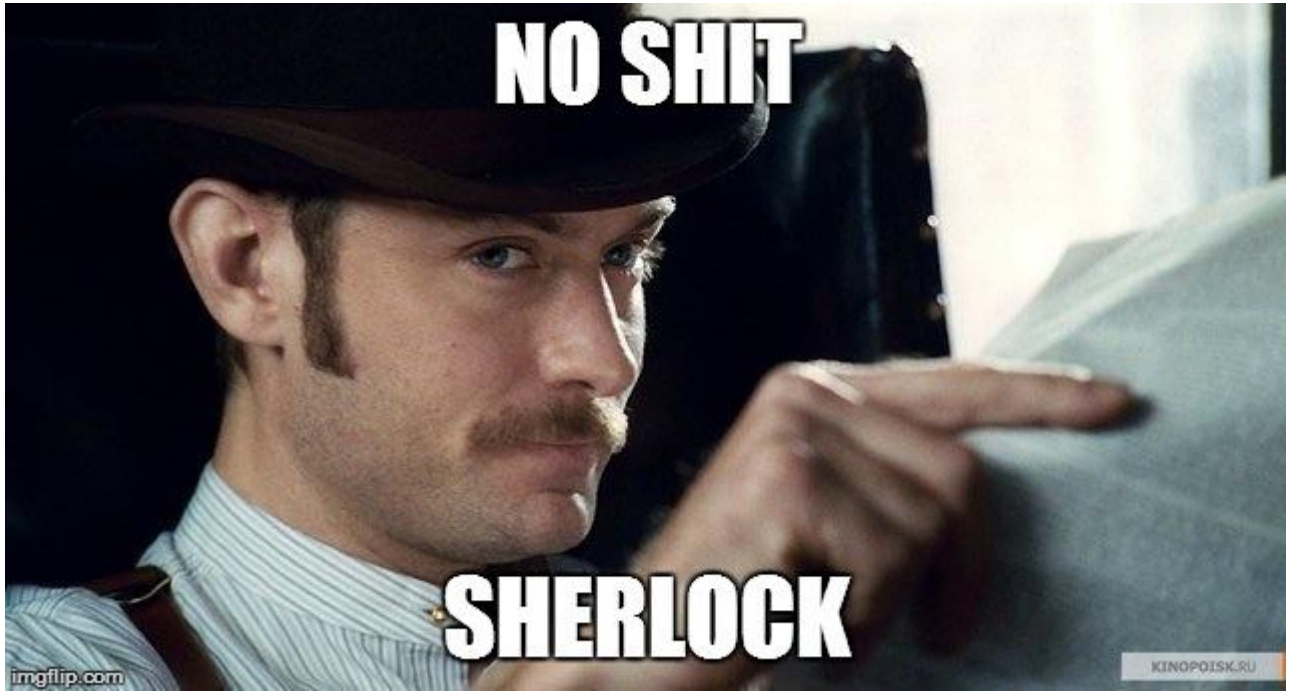
S.M.S. ?

NO SYSTEM IS SAFE

Protokół komunikacji :D:D:D:D

S.M.S. ?

NO SYSTEM IS SAFE



Analiza powłamaniowa okiem amatora - case study

Analiza jako pojęcie w kryminologii

- Analiza kryminalna - poszukiwanie relacji i zależności pomiędzy informacjami dotyczącymi przestępstw. Nie należy mylić "analizy kryminalnej" z prowadzeniem postępowania dowodowego czy postępowania wyjaśniającego. Zastosowanie analizy kryminalnej pozwala na ustalenie lub przewidywanie powiązań pomiędzy zgromadzonymi faktami, co pozwala na budowanie, weryfikowanie i eliminację wersji śledczych.

Informatyka śledcza

NO SYSTEM IS SAFE

- Z angielskiego *Computer Forensics* jest jedną z gałęzi nauk sądowych, której zadaniem jest dostarczenie dowodów w formie cyfrowej, ustalenie przebiegu zdarzeń oraz motywów, którymi kierował się sprawca lub ofiara.

Źródła informacji w informatyce śledczej

- - dyskietki
- - taśmy do backupów
- - dyski twarde
- - pamięci przenośne
- - serwery
- - portale społecznościowe
- - dyski w chmurze
- - przeglądarki internetowe

Źródła informacji w informatyce śledczej

NO SYSTEM IS SAFE

Kiedy informatyk śledczy wkracza do akcji?

NO SYSTEM IS SAFE

- defraudacji środków finansowych
- łamania prawa pracy
- kradzieży danych
- szpiegostwa przemysłowego
- łamania praw autorskich
- ujawnienia tajemnicy handlowej
- kradzieży i użycia danych osobowych
- spraw kryminalnych (handel narkotykami, terroryzm, morderstwa, samobójstwa, przestępczość zorganizowana, pedofilia).

Do sedna – Co? Kto? Kiedy?

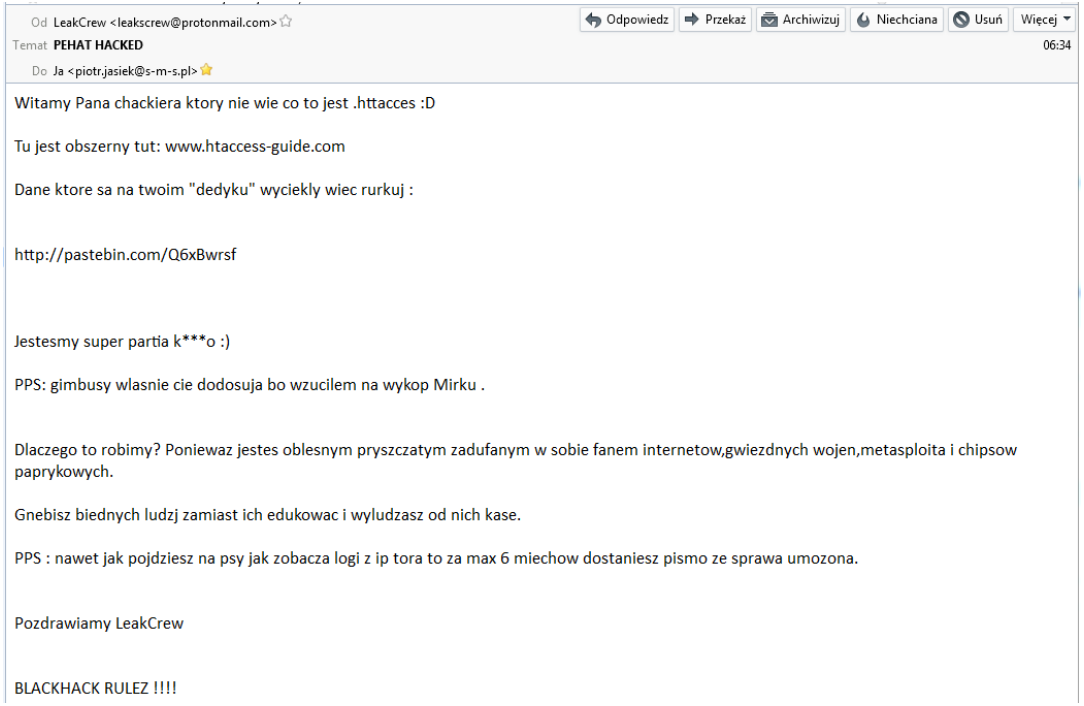
NO SYSTEM IS SAFE

- 15-16 23.06.2016 – „Intruz” przegląda s-m-s.pl i komentuje wpis.
- 4:31-5:56 26.06.2016 – „Intruz” pobiera dane z publicznie dostępnego hosta. W jego przekonaniu znalazł poufne dane.
- 5:04 26.06.2016 – "Intruz" tworzy paczkę i wrzuca pasty na pastebina.
- 6:34 26.06.2016 – Na mojej skrzynce pojawia się mail wysłany z Protonmaila.
- 6:50 26.06.2016 – Na kanałach IRC pojawiają się linki do pasty.
- 7:18 26.06.2012 – Na IRC przez prywatną wiadomość dostaję link do pasty.
- 7:30 26.06.2016 – Odczytuję maila.
- 7:40 26.06.2016 – Publikacja pasty i info na socialkach, zastawiam pułapkę
- 13:00 26.06.2016 – Zaczynam czytać logi.
- 14:00 26.06.2016 – Już wszystko wiem, piszę artykuł dokonując analizy logów.
- 20:00 26.06.2016 – Artykuł gotowy.
- 21:42 26.06.2012 – "Intruz" znów się odzywa i zapewnia, że to wszystko to był tylko żart.

Analiza danych i upewnianie się, że dowody poszlakowe są prawdziwe zajęło mi około sześć godzin, przy czym cały czas miałem również inne zajęcia. W rzeczywistości było to pracy na jakieś trzy godziny pracy.

"Na początku był chaos..." znaczy mail

NO SYSTEM IS SAFE



Od LeakCrew <leakscrew@protonmail.com>
Temat PEHAT HACKED
Do Ja <piotr.jasiek@s-m-s.pl>

Odpowiedz | Przekaż | Archiwizuj | Niechciana | Usuń | Więcej

06:34

Witamy Pana chackiera ktory nie wie co to jest .httacces :D

Tu jest obszerny tut: www.htaccess-guide.com

Dane ktore sa na twoim "dedyku" wyciekly wiec rurkuj :

http://pastebin.com/Q6xBwrsf

Jestesmy super partia k***o :)

PPS: gimbusy wlasnie cie dodosuja bo wzucilem na wykop Mirku .

Dlaczego to robimy? Ponieważ jestes oblesnym pryszczatym zadufanym w sobie fanem internetow,gwiezdnych wojen,metasploita i chipsow paprykowych.

Gnebisz biednych ludzj zamiast ich edukowac i wyludzasz od nich kase.

PPS : nawet jak pojdziesz na psy jak zobacza logi z ip tora to za max 6 miechow dostaniesz pismo ze sprawa umozona.

Pozdrawiamy LeakCrew

BLACKHACK RULEZ !!!!

Przejdźmy teraz do pastebina. Link do pasty dostałem również na IRC-u.

NO SYSTEM IS SAFE

Pastebin najlepszy do umieszczania wycieków?

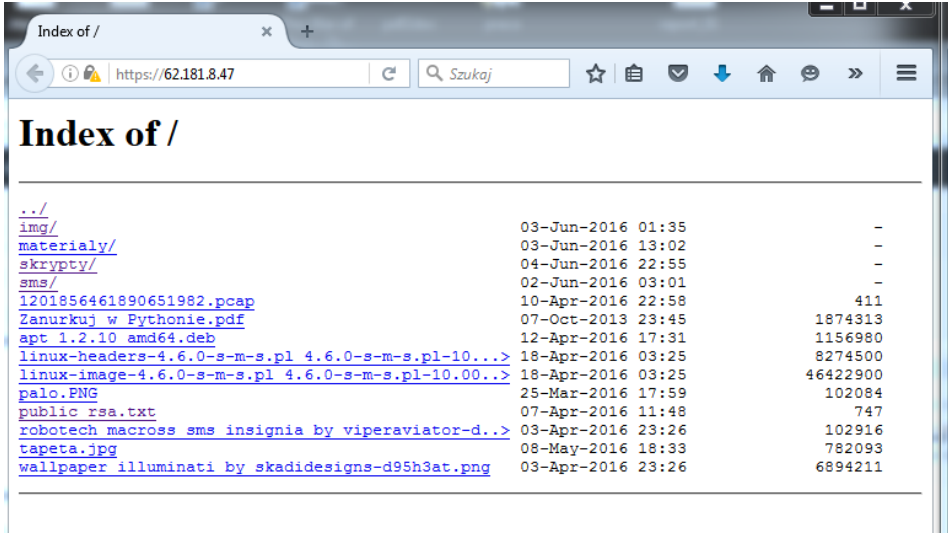
NO SYSTEM IS SAFE

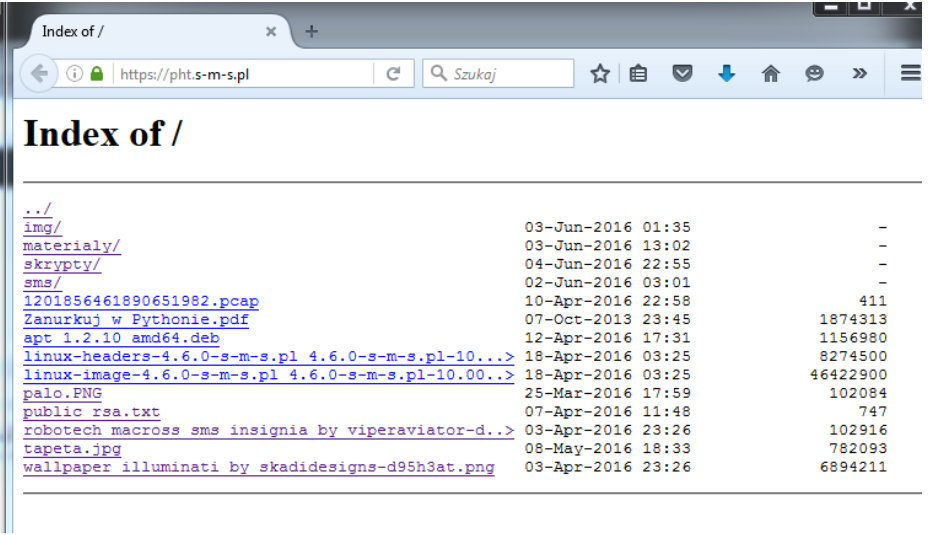
text 1.00 KB raw download clone

```
Dzis zamieszczamy troche danych pewnego działacza w branzy it-sec Piotra "pehata" Jaśka


Otoż ten osobnik jest tak arogancki ze zasluguje na kare.

Jego serwery hehe pierdololo "dedyk" okazal sie byc zwyklym vpsem za narne dzingi.


Jego fajne dane sa w glebokim ukryciu :D

https://62.181.8.47

Screeny i klucz rsa do shella sa w paczce.

Adres shella52.181.8.47:22

Adres bloga s-m-s.pl (jest tam adres gdzie mieszka ale sadzimy ze ul.Kochanowskiego w wawie to zadupie)

Link do paczki : https://drive.google.com/file/d/0Bz8A2Qf3Z_-CVDZ2TVB6X2xzNU0/view?usp=drivesdk

Nawet jak skasuja ten post to i tak ta paczka bedzie krazyc po darknetach i torenntach.

Kim jestesmy?

Znanymi z roznych zajebistych wlamow .

Nie mamy fajnych hackierskich nickow tak jak ten osobnik ale ma dzis Peha(t) :D

Pozdrowienia dla hackiera z białowieży

PS: Gimbazjalisci ruszcie duoe . zainstalujcie nmaoa bo nastawiane ma na tej maszynie w huj uslug.

Niech cebula bedzie z wami. Humus habeus papa :D
```

Mea culpa.

NO SYSTEM IS SAFE

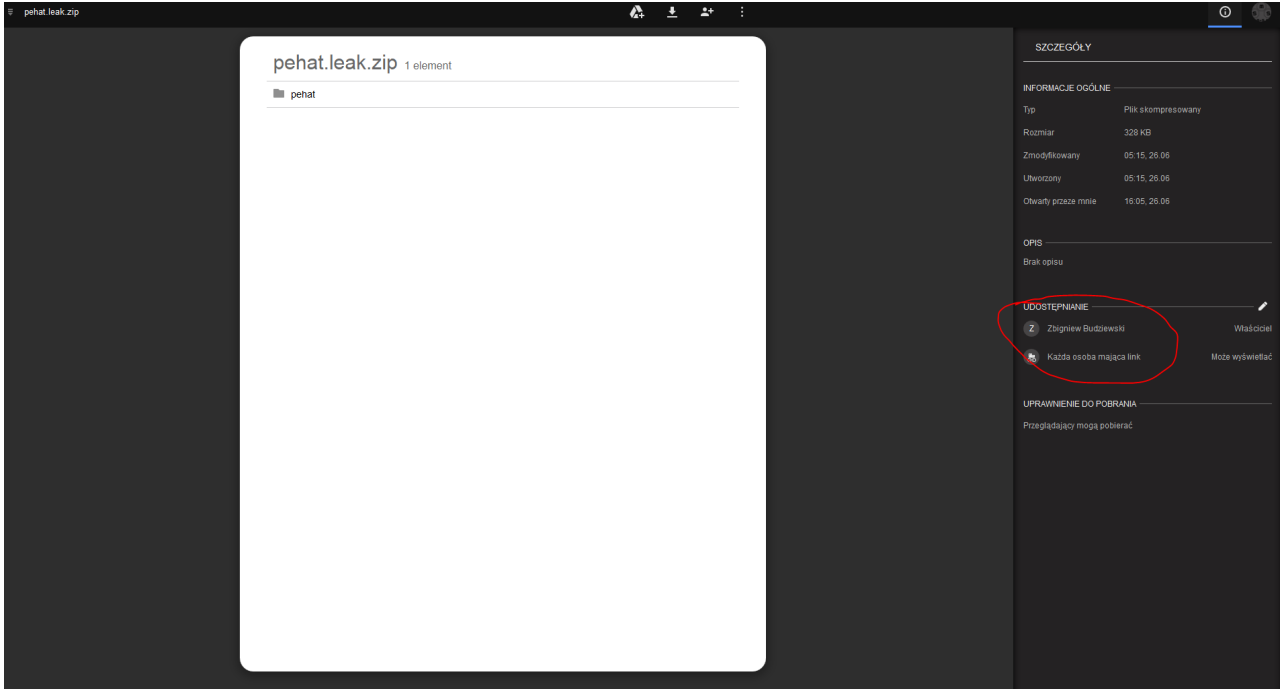




Analiza powłamaniowa okiem amatora - case study

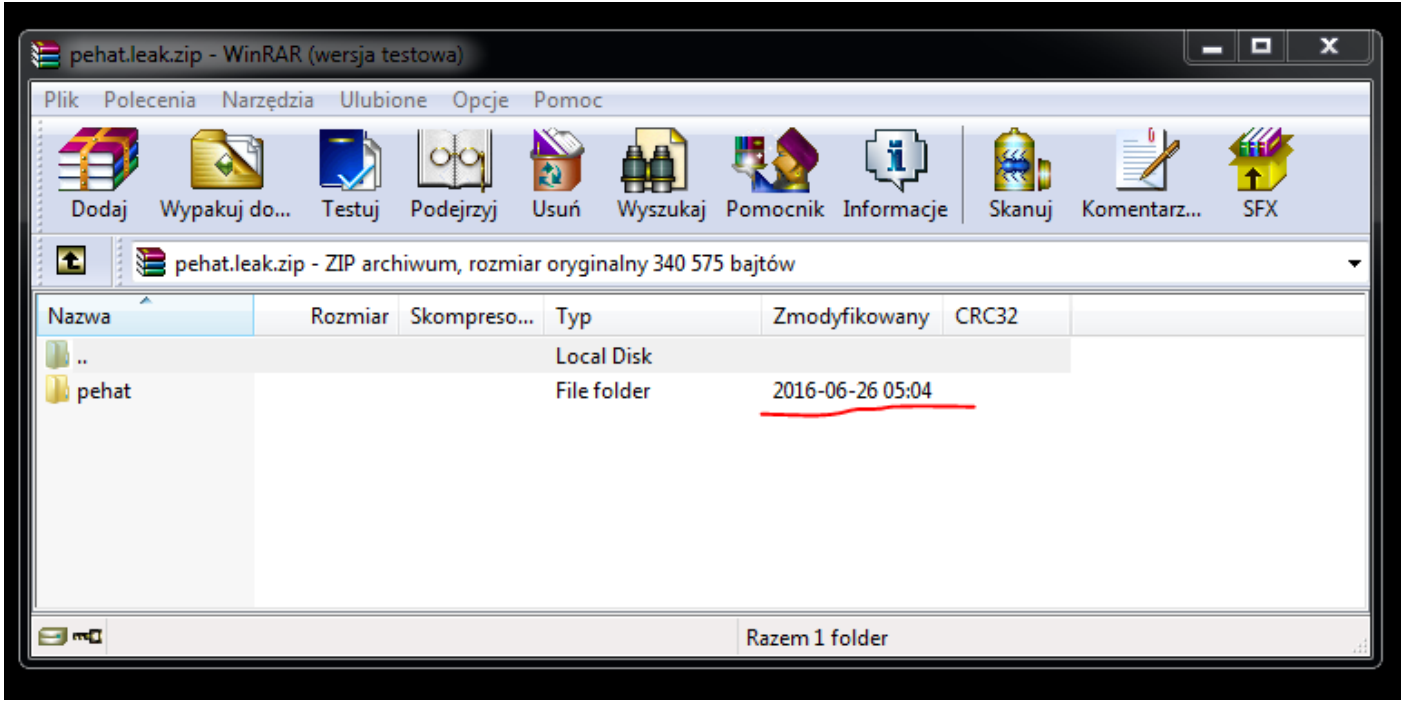
Teraz zajmijmy się paczką.

NO SYSTEM IS SAFE



Wyciek.zip

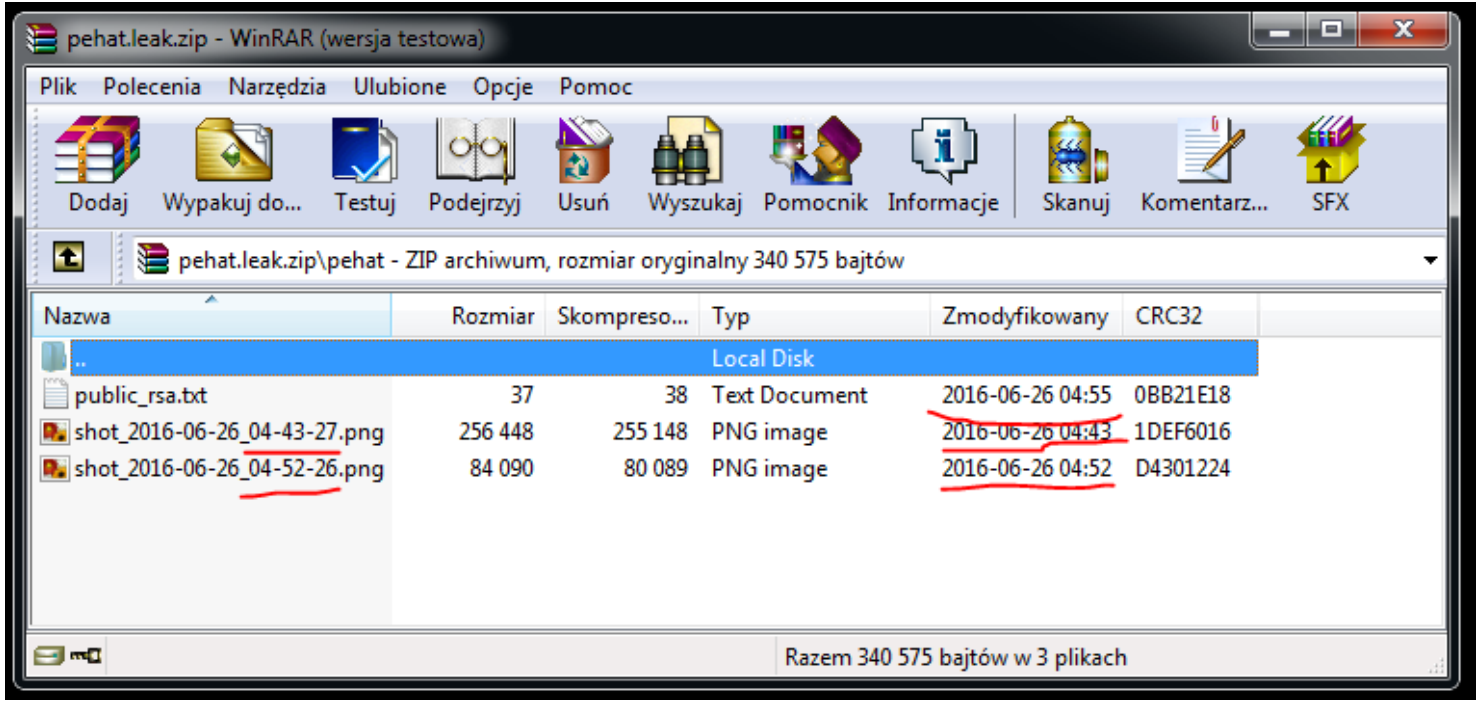
NO SYSTEM IS SAFE



Analiza powłamaniowa okiem amatora - case study

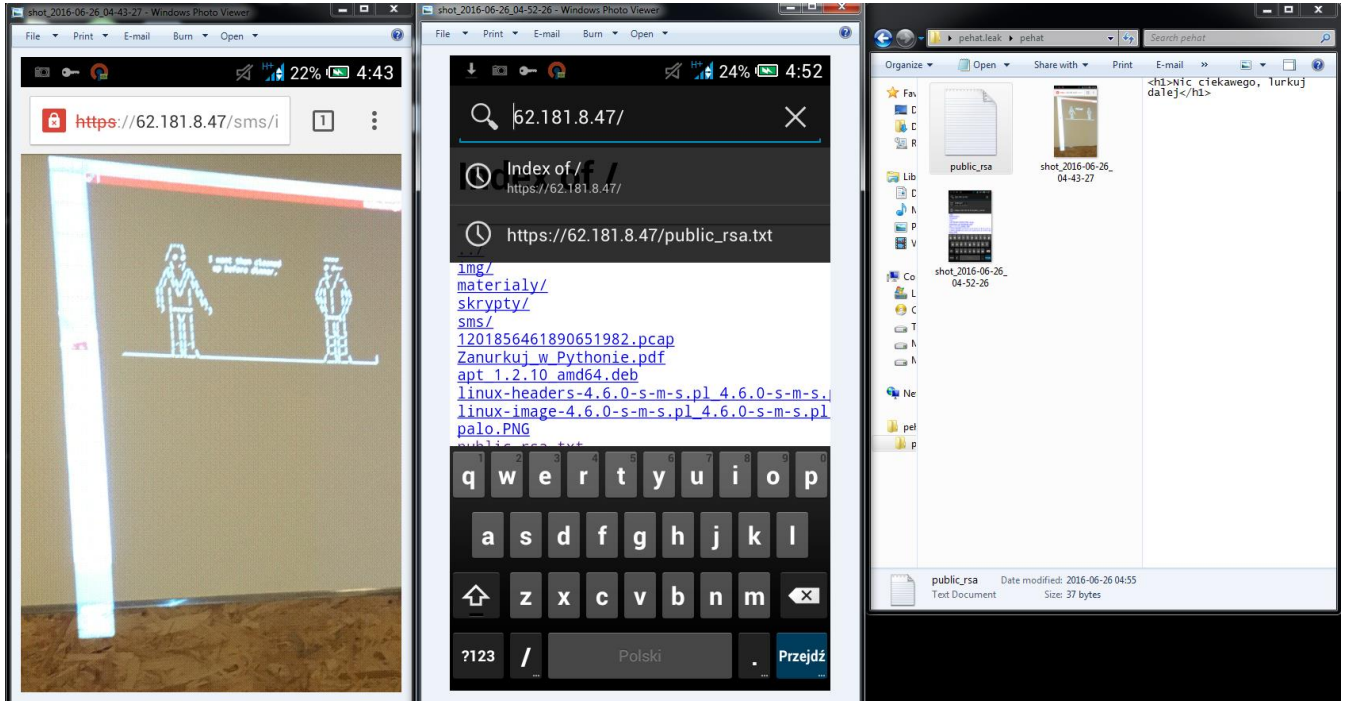
Wyciek.zip - szczegóły

NO SYSTEM IS SAFE



Screenshot najlepszym dowodem

NO SYSTEM IS SAFE



Analiza powłamaniowa okiem amatora - case study

Czytamy logi cz. 1

NO SYSTEM IS SAFE


```
root@vps:/var/log/nginx# cat access.log.1 | grep -i "\[26/Jun/2016" | grep -i Android

66.249.75.197 - - [26/Jun/2016:03:55:33 +0200] "GET / HTTP/1.1" 301 178 "-" "Mozilla/5.0 (Linux; Android 6.0.1;
Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.96 Mobile Safari/537.36 (compatible;
Googlebot/2.1; +http://www.google.com/bot.html)"

78.46.11.126 - - [26/Jun/2016:04:31:17 +0200] "GET / HTTP/1.1" 200 67 "-" "Dalvik/1.6.0 (Linux; U; Android 4.2.2;
NOKIA N73 Build/JDQ39)"

78.46.11.126 - - [26/Jun/2016:04:33:11 +0200] "GET / HTTP/1.1" 200 67 "-" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA
N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/1537D7"

78.46.11.126 - - [26/Jun/2016:04:33:12 +0200] "GET /favicon.ico HTTP/1.1" 200 67 "http://62.181.8.47/" "Mozilla/5.0
(Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile
Safari/1537D7"

78.46.11.126 - - [26/Jun/2016:04:47:24 +0200] "GET /public_rsa.txt HTTP/1.1" 200 67 "-" "Dalvik/1.6.0 (Linux; U;
Android 4.2.2; NOKIA N73 Build/JDQ39)"

78.46.11.126 - - [26/Jun/2016:04:52:19 +0200] "GET / HTTP/1.1" 200 67 "-" "Mozilla/5.0 (Linux; U; Android 4.2.2;
pl-pl; NOKIA N73 Build/JDQ39) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.2 Mobile Safari/781749"

78.46.11.126 - - [26/Jun/2016:04:52:20 +0200] "GET /favicon.ico HTTP/1.1" 200 67 "http://62.181.8.47/" "Mozilla/5.0
(Linux; U; Android 4.2.2; pl-pl; NOKIA N73 Build/JDQ39) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.2 Mobile
Safari/781749"

78.46.11.126 - - [26/Jun/2016:04:53:50 +0200] "GET /1201856461890651982.pcap HTTP/1.1" 200 67 "-" "Dalvik/1.6.0
(Linux; U; Android 4.2.2; NOKIA N73 Build/JDQ39)"

78.46.11.126 - - [26/Jun/2016:04:55:18 +0200] "GET /public_rsa.txt HTTP/1.1" 200 67 "-" "Dalvik/1.6.0 (Linux; U;
Android 4.2.2; NOKIA N73 Build/JDQ39)"

78.46.11.126 - - [26/Jun/2016:04:56:22 +0200] "GET /materialy/ebook-pl-helion-Linux.Tablice.Informatyczne.pdf
HTTP/1.1" 200 67 "-" "Dalvik/1.6.0 (Linux; U; Android 4.2.2; NOKIA N73 Build/JDQ39)"
```

Identyfikacja adresu IP

NO SYSTEM IS SAFE


```
root@vps:~# nmap 78.46.11.126

Starting Nmap 7.12 ( https://nmap.org ) at 2016-06-26 16:55 CEST
Nmap scan report for static.126.11.46.78.clients.your-server.de (78.46.11.126)
Host is up (0.026s latency).
Not shown: 975 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
49/tcp    open  tacacs
80/tcp    open  http
110/tcp   open  pop3
119/tcp   open  nntp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
465/tcp   open  smtps
992/tcp   open  telnets
995/tcp   open  pop3s
1080/tcp  open  socks
1723/tcp  open  pptp
2121/tcp  open  ccproxy-ftp
3389/tcp  open  ms-wbt-server
5555/tcp  open  freeciv
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 288.48 seconds
```

Ciekawostka z portu 80

NO SYSTEM IS SAFE

IRC sposobem na powiadomienie

NO SYSTEM IS SAFE

Czytamy logi cz. 2

NO SYSTEM IS SAFE


```
root@vps:~# cat /var/log/sms/sms_access.log | grep -i "178\.39\.201\.224"

178.39.201.224 - - [26/Jun/2016:13:31:16 +0200] "GET / HTTP/1.1" 200 15355 "https://www.google.ch/" "Mozilla/5.0 (Linux; Android 4.2.2;
NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:31:16 +0200] "GET
/wp-content/plugins/google-calendar-events/assets/css/vendor/jquery.qtip.min.css?ver=2.2.1 HTTP/1.1" 404 7107 "https://www.google.ch/"
"Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:31:16 +0200] "GET
/wp-content/plugins/google-calendar-events/assets/css/default-calendar-grid.min.css?ver=3.1.1 HTTP/1.1" 404 7102 "https://www.google.ch/"
"Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:31:16 +0200] "GET
/wp-content/plugins/google-calendar-events/assets/css/default-calendar-list.min.css?ver=3.1.1 HTTP/1.1" 404 7100 "https://www.google.ch/"
"Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:31:36 +0200] "GET /kernel-v4-6-rc2-dostepny-w-repozytorium-s-m-s/ HTTP/1.1" 200 12721 "
https://s-m-s.pl/" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0
Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:31:41 +0200] "GET /favicon.ico HTTP/1.1" 200 5 "
https://s-m-s.pl/kernel-v4-6-rc2-dostepny-w-repozytorium-s-m-s/" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:32:09 +0200] "GET /favicon.ico HTTP/1.1" 200 5 "https://s-m-s.pl/" "Mozilla/5.0 (Linux; Android 4.2.2;
NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:45:18 +0200] "GET /kontakt/ HTTP/1.1" 200 6885 "https://s-m-s.pl/" "Mozilla/5.0 (Linux; Android 4.2.2;
NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:45:28 +0200] "GET /favicon.ico HTTP/1.1" 200 5 "https://s-m-s.pl/kontakt/" "Mozilla/5.0 (Linux;
Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:45:41 +0200] "GET /kontakt/ HTTP/1.1" 200 6885 "https://s-m-s.pl/" "Mozilla/5.0 (Linux; Android 4.2.2;
NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

178.39.201.224 - - [26/Jun/2016:13:45:52 +0200] "GET /favicon.ico HTTP/1.1" 200 5 "https://s-m-s.pl/kontakt/" "Mozilla/5.0 (Linux;
Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"
```

Wspólny mianownik


```
NOKIA N73 Build/JDQ396
```

Sprawdźmy wszystkie logi

NO SYSTEM IS SAFE


```
root@vps:~/logi# ls
access.log    access.log.10  access.log.12  access.log.14  access.log.3
access.log.5  access.log.7  access.log.9  error.log.1  error.log.3  error.log.5
access.log.1  access.log.11  access.log.13  access.log.2   access.log.4
access.log.6  access.log.8  error.log     error.log.2  error.log.4
```

c.d.

NO SYSTEM IS SAFE


```
root@vps:~/logi# cat * | grep -i "NOKIA N73 Build/JDQ39"
78.46.11.126 - - [26/Jun/2016:04:31:17 +0200] "GET / HTTP/1.1" 200 67 "-" "Dalvik/1.6.0 (Linux; U; Android 4.2.2;

NOKIA N73 Build/JDQ39)"
78.46.11.126 - - [26/Jun/2016:04:33:11 +0200] "GET / HTTP/1.1" 200 67 "-" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73
Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/1537D7"

78.46.11.126 - - [26/Jun/2016:04:33:12 +0200] "GET /favicon.ico HTTP/1.1" 200 67 "http://62.181.8.47/" "Mozilla/5.0 (Linux;
Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/1537D7"

78.46.11.126 - - [26/Jun/2016:04:47:24 +0200] "GET /public_rsa.txt HTTP/1.1" 200 67 "-" "Dalvik/1.6.0 (Linux; U; Android 4.2.2;
NOKIA N73 Build/JDQ39)"

78.46.11.126 - - [26/Jun/2016:04:52:19 +0200] "GET / HTTP/1.1" 200 67 "-" "Mozilla/5.0 (Linux; U; Android 4.2.2; pl-pl; NOKIA
N73 Build/JDQ39) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.2 Mobile Safari/781749"

78.46.11.126 - - [26/Jun/2016:04:52:20 +0200] "GET /favicon.ico HTTP/1.1" 200 67 "http://62.181.8.47/" "Mozilla/5.0 (Linux; U;
Android 4.2.2; pl-pl; NOKIA N73 Build/JDQ39) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.2 Mobile Safari/781749"

78.46.11.126 - - [26/Jun/2016:04:53:50 +0200] "GET /12018564618906519 82.pcap HTTP/1.1" 200 67 "-" "Dalvik/1.6.0 (Linux; U;
Android 4.2.2; NOKIA N73 Build/JDQ39)"

78.46.11.126 - - [26/Jun/2016:04:55:18 +0200] "GET /public_rsa.txt HTTP/1.1" 200 67 "-" "Dalvik/1.6.0 (Linux; U; Android 4.2.2;
NOKIA N73 Build/JDQ39)"

78.46.11.126 - - [26/Jun/2016:04:56:22 +0200] "GET /materialy/ebook-pl-helion-Linux.Tablice.Informatyczne.pdf HTTP/1.1" 200 67
"-" "Dalvik/1.6.0 (Linux; U; Android 4.2.2; NOKIA N73 Build/JDQ39)"

94.254.243.166 - - [23/Jun/2016:15:16:05 +0200] "GET / HTTP/1.1" 301 178 "-" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73
Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"
```

Nie-torowy adres IP

NO SYSTEM IS SAFE


```
% Information related to '94.254.240.0/20AS201019'

route:          94.254.240.0/20
descr:          PLAY-Internet
origin:         AS201019
mnt-by:         P4-MNT
created:        2016-01-07T13:41:24Z
last-modified:  2016-01-20T13:15:37Z
source:         RIPE
```

Pytania do dowodów poszlakowych

- Komu 23/Jun/2016 o 15:16:05 nadano adres 94.254.243.166?
- Czy ta osoba w czasie między 26/Jun/2016:04:31:17 a 26/Jun/2016:04:56:22 łączyła się z hostem 78.46.11.126 za pomocą OpenVPN-a na 1194 porcie?
- Czy ta osoba w czasie między 26/Jun/2016:13:31:16 a 26/Jun/2016:13:45:52 łączyła się z hostem 178.39.201.224 w jakikolwiek sposób umożliwiający tunelowanie danych?

Inna aktywność „intruza”

NO SYSTEM IS SAFE


```
root@vps:~/logi# cat * | grep -i "NOKIA N73 Build/JDQ39" | grep -v "26/Jun/2016"
[...]
94.254.243.166 - - [23/Jun/2016:15:16:52 +0200] "GET /wp-content/uploads/2016/06/lol.png HTTP/1.1" 200 763499 "
https://s-m-s.pl/z-pamietnika-admina-zosia-samosia-robi-migracje/" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

94.254.243.166 - - [23/Jun/2016:15:16:54 +0200] "GET /wp-content/uploads/2016/06/sms1.png HTTP/1.1" 200 50459 "
https://s-m-s.pl/z-pamietnika-admina-zosia-samosia-robi-migracje/" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

94.254.243.166 - - [23/Jun/2016:15:16:55 +0200] "GET /wp-content/uploads/2016/06/home2.png HTTP/1.1" 200 102147 "
https://s-m-s.pl/z-pamietnika-admina-zosia-samosia-robi-migracje/" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

94.254.243.166 - - [23/Jun/2016:15:17:15 +0200] "GET /favicon.ico HTTP/1.1" 200 5 "https://s-m-s.pl/z-pamietnika-admina-zosia-samosia-robi-migracje/"
"Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

94.254.243.166 - - [23/Jun/2016:15:27:14 +0200] "POST /wp-comments-post.php HTTP/1.1" 302 5 "
https://s-m-s.pl/z-pamietnika-admina-zosia-samosia-robi-migracje/" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

94.254.243.166 - - [23/Jun/2016:15:27:15 +0200] "GET /z-pamietnika-admina-zosia-samosia-robi-migracje/ HTTP/1.1" 200 32781 "
https://s-m-s.pl/z-pamietnika-admina-zosia-samosia-robi-migracje/" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"

94.254.243.166 - - [23/Jun/2016:15:27:23 +0200] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 69 "
https://s-m-s.pl/z-pamietnika-admina-zosia-samosia-robi-migracje/" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73 Build/JDQ39) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"
```

„Intruz” komentuje

NO SYSTEM IS SAFE


```
94.254.243.166 - - [23/Jun/2016:15:27:14 +0200] "POST /wp-comments-post.php HTTP/1.1" 302 5 "
https://s-m-s.pl/z-pamietnika-admina-zosia-samosia-robi-migracje/" "Mozilla/5.0 (Linux; Android 4.2.2; NOKIA N73
Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2763.0 Mobile Safari/537.36"
```

„Ten” komentarz

NO SYSTEM IS SAFE

2 thoughts on “Z pamiętnika admina: Zosia Samosia robi migracje.”

Leszek says:

A co z securwe .pl?

Ponoc byl hostowany u Cb a lezy 😕

23 czerwca 2016
15:27

Edit Reply

pht says:

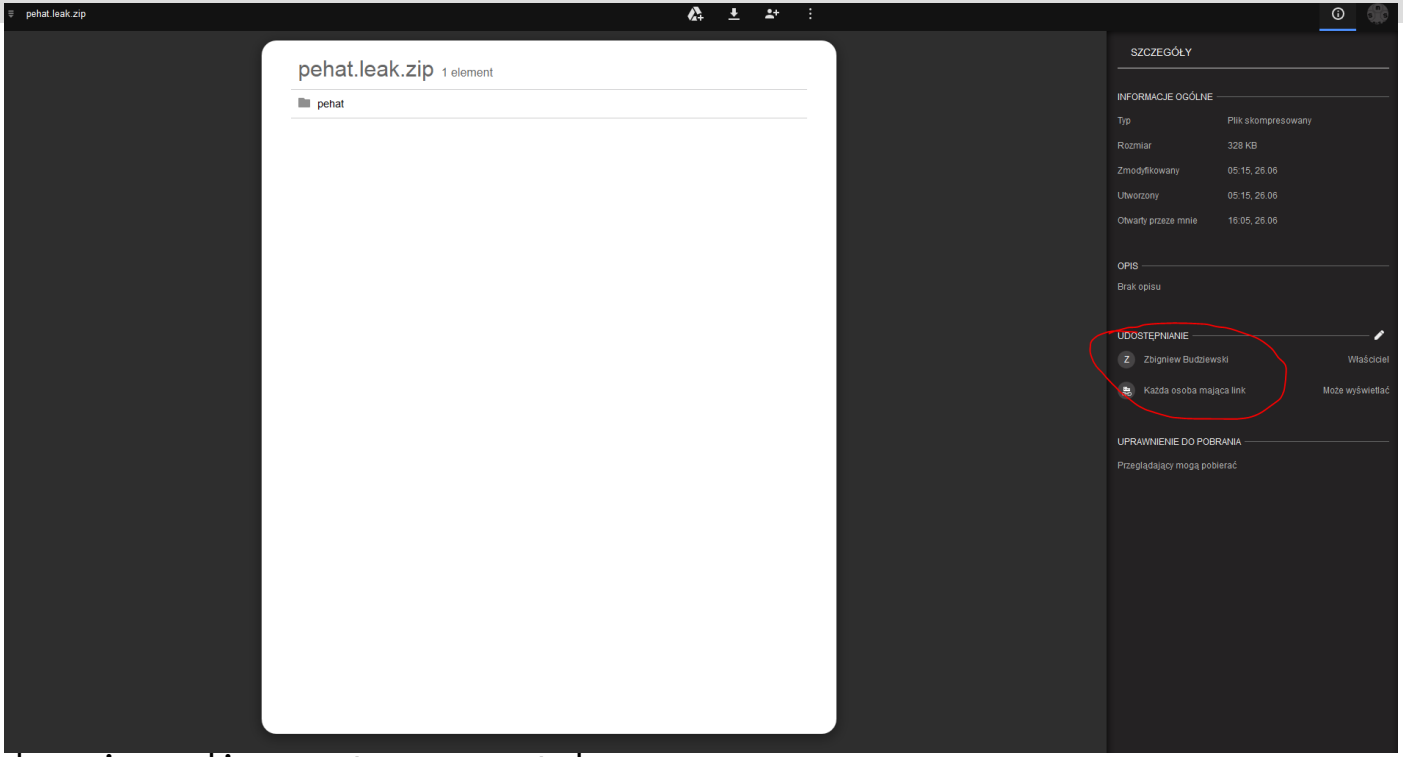
Admin wspomnianej przez Ciebie strony porzucił projekt. Poza tym zostały mu odebrane wszelakie dostepy z względu na naruszenia bezpieczeństwa jakich się dopuszczał.

24 czerwca 2016
01:31

Edit Reply

Nie masz hackerbox'a użyj Google'a

NO SYSTEM IS SAFE



Pytania?

NO SYSTEM IS SAFE

SCP - Social and Contact Page ☺

NO SYSTEM IS SAFE

https://www.facebook.com/smspolska

https://twitter.com/smspoland

piotr.jasiek@s-m-s.pl