Zue hakeły shakowały pehłatego… A tak serio? No, to już trochę więcej do opowiedzenia. Postanowiłem zgodnie z poranną obietnicą w socialkach, opisać wydarzenia z dzisiejszego poranka.

Coś się stało? Internet obiegła wieść, że mnie, PHT, shakowano. Znaczy shakowano jeden z serwerów należących do mnie jako admina. Nie powiem, że nie – w pierwszej chwili zrobiło mi się gorąco. Czyżby i na mnie przyszła kolej? Ale! doczytałem maila i przypomniał mi się najsłynniejszy tekst Jokera – „Why so serious?”. A co dokładniej? Dowiecie się w dalszej części artykułu.

Dla mnie dzień zaczął się około 7:30, gdy wstałem do pracy. Pierwszą czynnością jaką zrobiłem to automatyczne i mimowolne sprawdzenie telefonu, czy nie ma aby jakiś alertów. BYŁ. Mail. Jego tytuł był na tyle sugestywny, że zrobiło mi się ciepło, za ciepło i od razu się rozbudziłem.

Poniżej treść maila.

Od LeakCrew <leakscrew@protonmail.com>
Odpowiedz | Przekaż | Archiwizuj | Niechciana | Usuń | Więcej
Temat **PEHAT HACKED** 06:34
Do Ja <piotr.jasiek@s-m-s.pl>

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? Poniewaz 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 !!!!

Postanowiłem pokrótce przeanalizować ten tekst. Pierwszą rzeczą, jaka się rzuca

to sugestywny mail. Jak się okazuje to „grupa” (tak sugeruje mail) „LeakCrew”. Nazwa brzmi jakby prosto z generatora hackerskich nazw, ale wróćmy do analizy.

Pierwszy plus dla naszego/naszych „atakujących” (z maila wiemy, że to autorzy owego „włamu”), użyli Protonmaila. To z pewnością na tym etapie uniemożliwi mi ustalenie kim oni są… No tak, dobry cracker (kojarzy mi się z cancer) jest anonimowy. Przejdźmy dalej.

> Witamy Pana chackiera ktory nie wie co to jest .httacces

Ortografie pominę, dlaczego? Później wyjaśnię. Od razu rzuca się prześmiewcza, pogardliwa forma. Czyżby sprawa osobista? Tak. .httacces? Nie, nie znam nie używam apache.

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

Jak już pisałem nie używam apache… Tak tylko podkreślam, bo jak się później okaże – będzie to ważna kwestia.

> Dane ktore sa na twoim „dedyku” wyciekly wiec rurkuj :

Na moim dedyku? Oh wait, chodzi o VPS-a z którego korzysta SMS ze względów technicznych?

> http://pastebin.com/Q6xBwrsf

Pozwoliłem sobie dodać odsyłacz, by każdy mógł zobaczyć tą wstawkę bezpośrednio.

> Jestesmy super partia k***o

Aha… Lubię ludzi, którzy klną, a potem to cenzurują. Przypominają mi się Ci gimbajutuberzy którzy klną po cichu „bo stara w piwnicy”.

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

„PPS”? A nie jest tak, że najpierw się używa PS, potem PPS, PPPS itd? No tak. Na wykopie jest armia gimbów czekających na polecenie DDoS-owania odświeżaniem strony/skanowaniem nmapem adresów które podają crackerzy nie umiejący nawet używać polskich znaków. Serio, zróbcie mi „laske” i oddajcie mamie kabel od internetu.

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

O! Nareszcie jakieś konkrety! A więc!

- „oblesnym” – no, lubię sobie czasem beknąć po obiedzie, ale i tak trener niemieckiej reprezentacji mnie przebija
- „pryszczatym” – nie przypominam sobie, abym był pryszczaty… Komuś pomyliły się osoby czy tylko pojechał, bo tak?
- „zadufanym w sobie fanem internetów” – no tak, bo jak jesteś informatykiem powinieneś nienawidzić internet?
- „gwiezdnych wojen” – nie, sorry. Nie jesteś droidem, którego szukałem. Sprzedam Cię ludziom pustyni razem z Twoim telefonem
- „metasploita” – tak, przydatne narzędzie. Gdybyś go kiedykolwiek użył, może faktycznie włamałbyś się gdziekolwiek
- „chipsów paprykowych” – nie, wole kebabowe top chipsy z biedronki. Najlepiej żeby do tego było piwo „Miłosław” białe.

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

Gnębię ludzi? A. W sensie chodzi o to, że punktuje ludziom ich błędy i mówię jasno, co robią źle? No tak. Przepraszam, mam mało cierpliwości. Wyłudzam kasę? Aha. W sensie, że zrobiłem zbiórkę na domenę i serwer mailowy? Gdybym miał konto na YouTube i miał z tego hajs albo jakiś inny Patronite też byłby ból w odbycie, bo mam profit od czytelników?

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

Tak, teraz powinno być PPS. Na psy? W sensie na policję. Logi i IP z tora? No ok…

> Pozdrawiamy LeakCrew
>
> BLACKHACK RULEZ !!!!

Końcówki już nie komentuje. Przejdźmy teraz do pastebina. Link do pasty dostałem również na IRC-u.

W tym momencie wiem już czego będę szukał w logach. Nie IP z Tora – tak, nasz crackerski team pokazał mi swój IP

Poniżej treść wklejki.

> Dzis zamieszczamy troche danych pewnego dzialacza w branzy it-sec Piotra „pehata” Jaśka
> Otoż ten osobnik jest tak arogancki ze zasluguje na kare.

Kurcze… Nie „pehata” a „pht”, nie „Jaśka” a „Jasiek”. To nazwisko się nie odmienia. Drugie zdanie to takie masło maślane, że szkoda na nie literek. Pomijam że jakich kurwa danych?

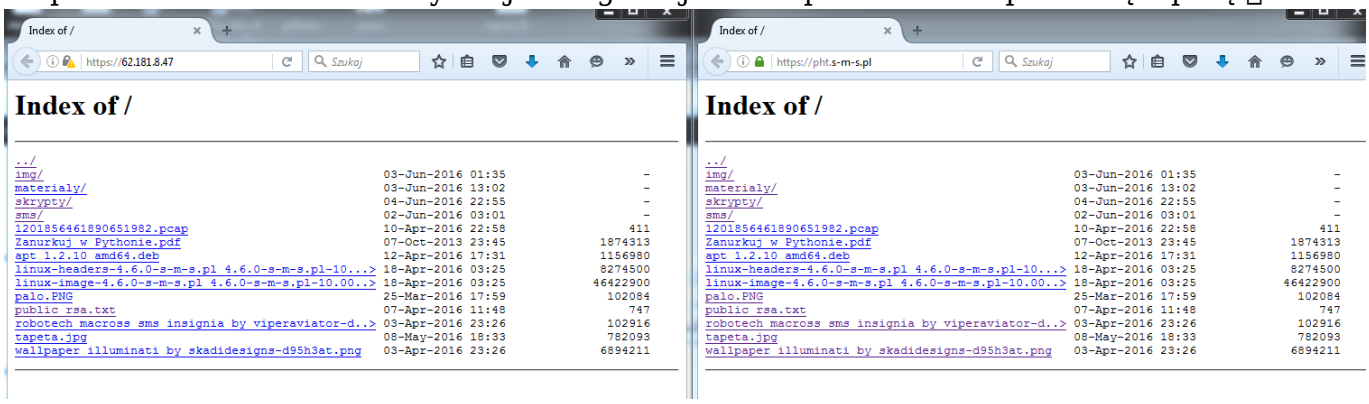
> Jego serwery hehe pierdololo „dedyk” okazal sie byc zwyklym vpsem za narne dzingi.

Jak już pisałem, pisaliśmy o tym ze nie korzystamy już z „hehe pierdololo «dedyk»”’a. Za co? „narne dzingi”. Nie rozumiem, więc nie komentuje.

> Jego fajne dane sa w glebokim ukryciu
> https://62.181.8.47

À propos fajnych danych… ten sam index zgłasza się pod https://pht.s-m-s.pl. Przypadek?

Bardziej błąd w konfiguracji. Fakt, mea culpa. Zanim opublikuje artykuł – naprawię to.
Po prostu nie ustawiłem domyślnej konfiguracji dla https'a i wrzuca pierwszą lepszą



> Screeny i klucz rsa do shella sa w paczce.

Mówiąc o paczce: zaraz poruszę temat w osobnym akapicie.

> Adres shella52.181.8.47:22

A to jakiś inny serwer

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

„Sadzimy", znaczy się, że chłopaki nietutejsze To adres pod którym zarejestrowane jest stowarzyszenie

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

No to, że link ma „drivesdk" na końcu wiele mówi. Właśnie; paczka. Ale to zaraz.

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

Można prosić link? Chętnie udostępnię.

> Kim jestesmy?

No! Konkrety.

Znanymi z roznych zajebistych wlamow .

Ja was nie kojarzę. Nikt was nie kojarzy

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

Czuję się, jakby ktoś przepuścił to przez Google Translate… Nawet nie wiem jak przeczytać to… No ok, nie mają ksyw. Spoko, jakieś losowe noname'y z „darknetów".

Pozdrowienia dla hackiera z białowieży

Co?

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

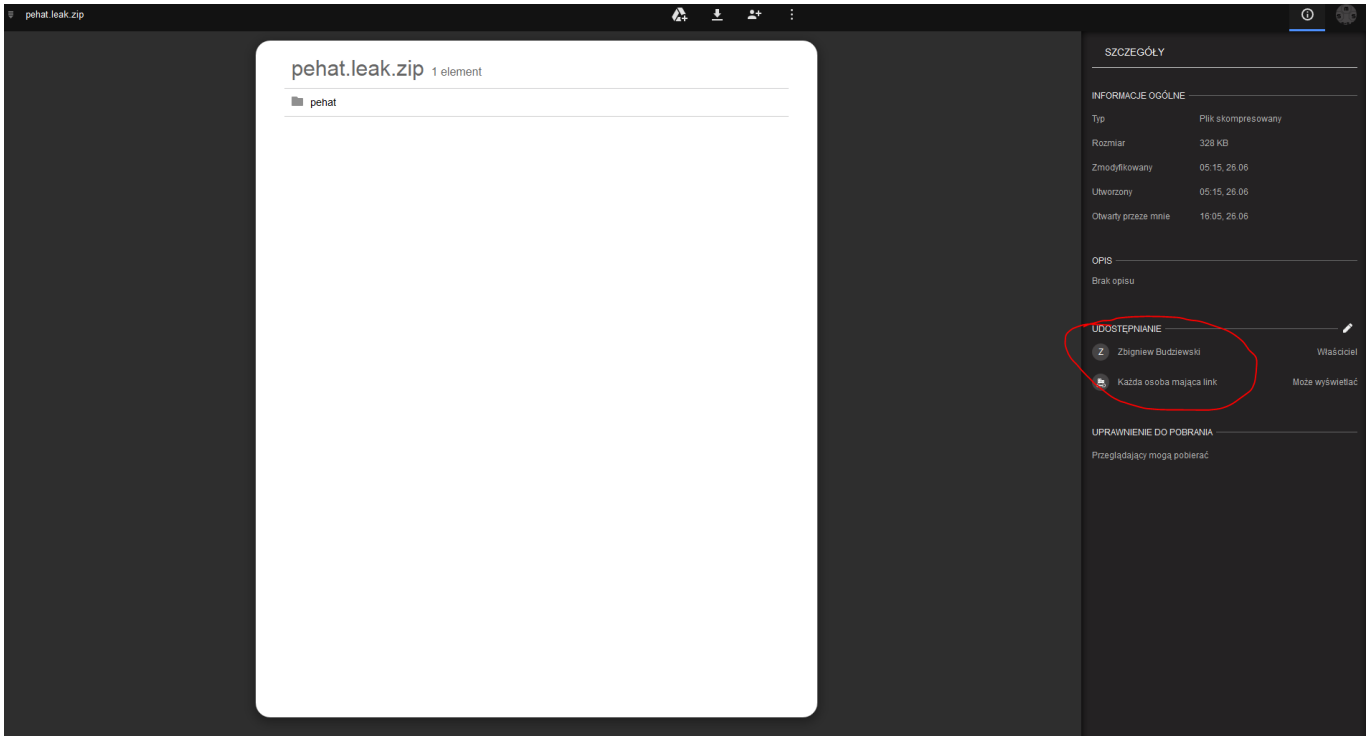
Dobrze użyte „PS". Brawo. Mocne 2/10, ale:

- „dupę" a nie „duoe"
- „nmapa", nie „nmaoa"
- I najważniejsze: „Chuj" piszemy przez „ch", by był dłuższy.

Niech cebula bedzie z wami. Humus habeus papa

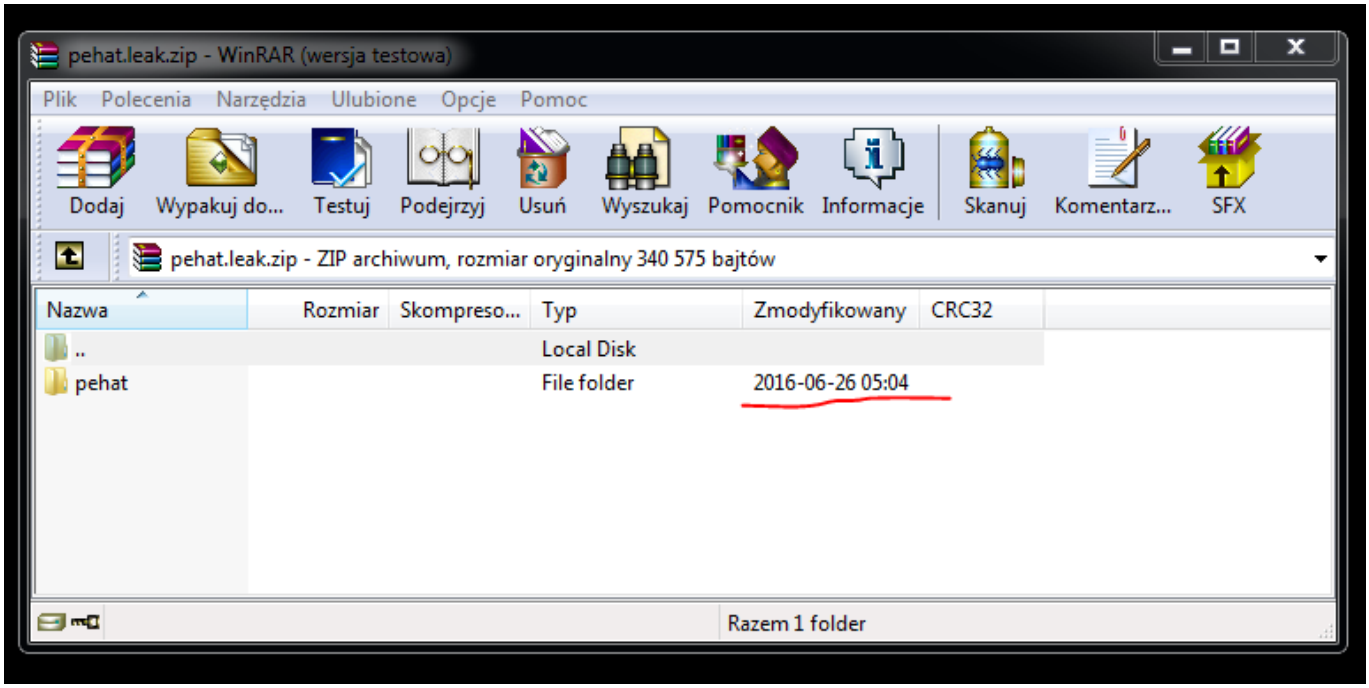
Śmieszkowanie z papieża? Spoko

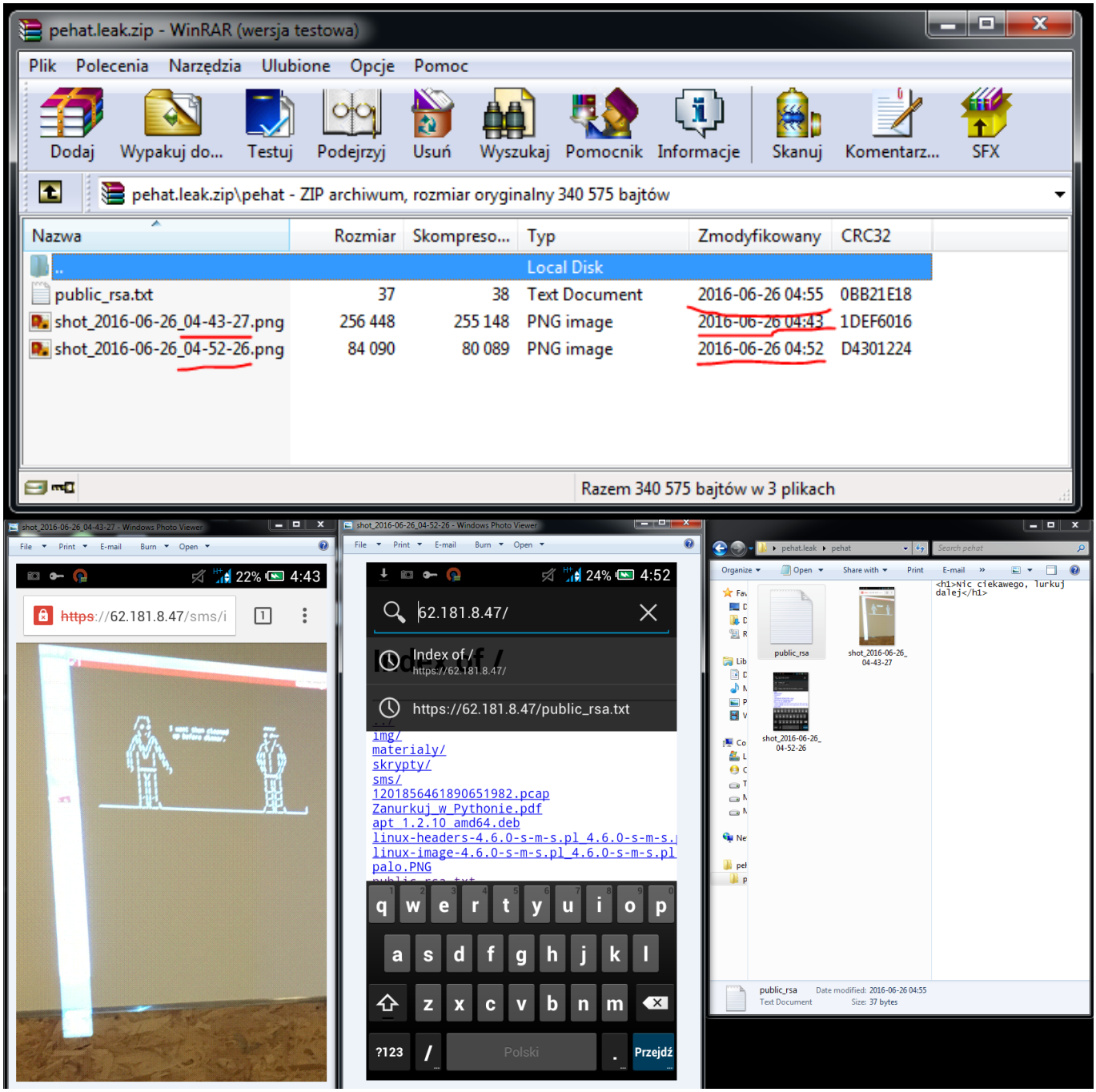
Teraz zajmijmy się paczką.



Paczkę wrzucono z konta niejakiego Zbigniewa Budziewskiego. Kim jest? Tym zajmiemy się później.

Przeskanowałem ją za pomocą Virustotala. Czysta. Zajrzyjmy do niej.





Paczka jest pełna danych. Zacznijmy od pierwszego zrzutu: Widać na nim datę utworzenia paczki. Co za tym idzie – zakończenie „ataku”. To mówi nam w którym miejscu w logach szukać śladów po intruzie.

Drugi screen to listing paczki, daty screenów i data utworzenia pobranego pliku. To już dokładna informacja kiedy dane „wyciekły”.

Trzeci screen jest moim ulubionym. Widać na nim jak intruz korzysta z OpenVPN-a. Na telefonie. Z dokładna datą. Widzimy też, że używa połączenia GSM, a nie WiFi. W ten sposób intruz dostarczył mi danych potrzebnych do przygotowania dowodów do ewentualnego zgłoszenia na policję :).

Jak już pisałem, wyświetlony został index domyślny na HTTPS-a – czyli default. Zajrzyjmy do logów. Pamiętajmy, że szukamy logów adekwatnych dla zakresu czasowego 4:00-5:04 rano 26.06.2016.

Source code

```
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)"
```

Szybki grep bazując na danych zdobytych z paczki „intruz” korzysta z przeglądarki na telefonie podając nam klienta. Jak widać wykonując swoje „zajebiste włamy” zapomniał, że można go zidentyfikować za pomocą korelacji danych. Używa OpenVPN-a, a więc przyjrzyjmy się samemu serwerowi.

Source code

```
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
```

Na porcie 80 widać taki oto widok:

Co znaczy, że VPN jest publiczny. Niby ślepa uliczka, ale… Znamy daty, adresy oraz klienta

jakim posługiwał się intruz. Zacznijmy szukać pod innym kątem. Wiemy, że połączył się z IRC-em z odkrytego adresu IP.

```
~androirc@adsl-178-39-201-224.adslplus.ch
[07:18:55]        LeakCrew  http://pastebin.com/Q6xBwrsf
[07:33:21]  Update Checker  A HexChat update is available! You can download it from here:
[07:33:21]                  http://dl.hexchat.net/hexchat/HexChat%202.12.1-2%20x64.exe
```

Szybki grep i widzimy, że intruz wpadł w moja pułapkę. Rano napisałem, że opublikuje informacje na temat całego zajścia. Wiedziałem, że intruz będzie sprawdzał czy coś wrzucę.

Source code

```
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
"http://blog.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
"http://blog.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 "http://blog.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 "http://blog.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 "http://blog.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 "http://blog.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 "http://blog.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"
```

Jak widać kluczem do całości jest telefon komórkowy intruza:

```
NOKIA N73 Build/JDQ396
```

Poszukajmy więc śladów tego telefonu.

Zrzuciłem wszystkie logi które miałem dla gołego NGINX-a i otrzymałem taki wynik.

Source code

```
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
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
/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)"
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"
```

Jak widzimy, w ostatniej linii znajduje się wpis z 23.06.2016. Jest to IP z....

Source code

```
root@vps:~/logi# whois 94.254.243.166
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '94.254.192.0 - 94.254.255.255'

% Abuse contact for '94.254.192.0 - 94.254.255.255' is
'registry@playmobile.pl'

inetnum:        94.254.192.0 - 94.254.255.255
netname:        P4NET
descr:          Playonline
descr:          P4 Sp. z o.o.
country:        PL
admin-c:        TEAM4-RIPE
tech-c:         TEAM4-RIPE
status:         ASSIGNED PA
mnt-by:         P4-MNT
mnt-lower:      P4-MNT
mnt-domains:    P4-MNT
mnt-routes:     P4-MNT
```

```
created:        2009-03-13T16:17:29Z
last-modified:  2011-04-12T22:13:31Z
source:         RIPE

role:           P4 Team
address:        P4 Sp. z o.o.
address:        ul. Tasmowa 7
address:        02-677 Warszawa
address:        Poland
phone:          +48 22 3194000
fax-no:         +48 22 3194001
tech-c:         PA5419-RIPE
tech-c:         PJ2582-RIPE
tech-c:         GC9860-RIPE
tech-c:         MK9263-RIPE
tech-c:         GC13723-RIPE
admin-c:        AS2985-RIPE
admin-c:        SK2147-RIPE
admin-c:        GS4534-RIPE
nic-hdl:        TEAM4-RIPE
mnt-by:         P4-MNT
created:        2006-03-11T21:32:24Z
last-modified:  2013-12-12T15:42:12Z
source:         RIPE # Filtered
abuse-mailbox:  abuse@project4.pl

% 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

% This query was served by the RIPE Database Query Service version
1.87.4 (ANGUS)
```

Dokładnie tak. Play. Mamy kolejną poszlakę.W tym miejscu należałoby ustalić:

1. Komu 23/Jun/2016 o 15:16:05 nadano adres 94.254.243.166
2. 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
3. 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.

Uzyskanie nakazu na takie dane dla policji to około 24-48 godzin. O ile policjantowi się chce. Więc już teraz udowodniłem, że nasz intruz wcale nie jest tak anonimowy jak zapewniał. Pójdzmy o krok dalej. sprawdzmy wszystkie dostepne mi logi SMS. Te post-migracyjne, jak i przed nią, szukając tego konkretnego urządzenia. Najpierw zrzuciłem więc wszystkie logi do osobnego katalogu, rozpakowałem i przegrepowałem szukając naszego intruza.

Source code

```
root@vps:~/logi# cat * | grep -i "NOKIA N73 Build/JDQ39" | grep -v
"26/Jun/2016"
94.254.243.166 - - [23/Jun/2016:15:16:06 +0200] "GET / HTTP/1.1" 200
29877 "-" "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/2016:15:16:07 +0200] "GET /wp-
content/plugins/wp-
synhighlight/themes/default/geshi/bash.css?ver=4.5.3 HTTP/1.1" 200
1696 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:07 +0200] "GET /wp-
content/plugins/contact-form-7/includes/css/styles.css?ver=4.4.2
HTTP/1.1" 200 1099 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:07 +0200] "GET /wp-
content/themes/flint/style.css?ver=1.5.0 HTTP/1.1" 200 15686
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:07 +0200] "GET /wp-
```

content/themes/flint/css/bootstrap.min.css?ver=3.0.0 HTTP/1.1" 200 122540 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:08 +0200] "GET /wp-content/plugins/google-calendar-events/assets/css/vendor/jquery.qtip.min.css?ver=2.2.1 HTTP/1.1" 200 1813 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:08 +0200] "GET /wp-content/plugins/google-calendar-events/assets/css/default-calendar-grid.min.css?ver=3.1.1 HTTP/1.1" 200 9427 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:08 +0200] "GET /wp-content/plugins/google-calendar-events/assets/css/default-calendar-list.min.css?ver=3.1.1 HTTP/1.1" 200 8183 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:08 +0200] "GET /wp-content/plugins/wp-synhighlight/themes/default/wp-synhighlighter.css HTTP/1.1" 200 1457 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:09 +0200] "GET /wp-content/plugins/slider-wd/css/wds_frontend.css?ver=1.1.38 HTTP/1.1" 200 2672 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:09 +0200] "GET /wp-content/plugins/slider-wd/css/wds_effects.css?ver=1.1.38 HTTP/1.1" 200 8037 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:09 +0200] "GET /wp-

```
content/plugins/slider-wd/css/font-awesome-4.0.1/font-
awesome.css?ver=4.0.1 HTTP/1.1" 200 22736 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:10 +0200] "GET /wp-
includes/js/jquery/jquery.js?ver=1.12.4 HTTP/1.1" 200 97184
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:10 +0200] "GET /wp-
includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1" 200 10056
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:10 +0200] "GET /wp-
content/plugins/wp-synhighlight/themes/default/wp-synhighlighter.js
HTTP/1.1" 200 2414 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:11 +0200] "GET /wp-
content/plugins/slider-wd/js/jquery.mobile.js?ver=1.1.38 HTTP/1.1" 200
6418 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:12 +0200] "GET /wp-
content/plugins/slider-wd/js/wds_frontend.js?ver=1.1.38 HTTP/1.1" 200
2567 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:12 +0200] "GET /wp-
content/plugins/wp-power-stats/wp-power-stats.js HTTP/1.1" 200 1295
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:12 +0200] "GET /wp-
content/plugins/contact-
form-7/includes/js/jquery.form.min.js?ver=3.51.0-2014.06.20 HTTP/1.1"
```

```
200 15248 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:13 +0200] "GET /wp-
content/plugins/contact-form-7/includes/js/scripts.js?ver=4.4.2
HTTP/1.1" 200 11819 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:13 +0200] "GET /wp-
content/themes/flint/js/bootstrap.min.js?ver=3.0.0 HTTP/1.1" 200 36816
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:13 +0200] "GET /wp-
content/themes/flint/js/skip-link-focus-fix.js?ver=9f3e2cd HTTP/1.1"
200 766 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:13 +0200] "GET /wp-
content/plugins/google-calendar-
events/assets/js/vendor/jquery.qtip.min.js?ver=2.2.1 HTTP/1.1" 200
35478 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:14 +0200] "GET /wp-
content/plugins/google-calendar-
events/assets/js/vendor/moment.min.js?ver=4.5.3 HTTP/1.1" 200 46645
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:14 +0200] "GET /wp-
content/plugins/google-calendar-events/assets/js/default-
calendar.min.js?ver=3.1.1 HTTP/1.1" 200 5092 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:14 +0200] "GET /wp-
content/plugins/google-calendar-
```

```
events/assets/js/vendor/imagesloaded.pkgd.min.js?ver=3.1.8 HTTP/1.1"
200 5407 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:14 +0200] "GET /wp-
includes/js/wp-embed.min.js?ver=4.5.3 HTTP/1.1" 200 1403
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:14 +0200] "GET /wp-
content/uploads/slider-wd/IMG_20150212_124136.jpg HTTP/1.1" 200 66362
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:15 +0200] "GET /wp-
includes/js/wp-emoji-release.min.js?ver=4.5.3 HTTP/1.1" 200 9802
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:15 +0200] "GET /wp-
content/uploads/2016/01/1370865635_0.jpg HTTP/1.1" 200 43621
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:15 +0200] "POST /wp-admin/admin-
ajax.php HTTP/1.1" 200 69 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:15 +0200] "GET /wp-
content/uploads/2016/01/DSC4770-150x150.jpg HTTP/1.1" 200 6123
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:16 +0200] "GET /wp-
content/uploads/2016/01/DSC4769-150x150.jpg HTTP/1.1" 200 7460
"http://blog.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"
```

```
94.254.243.166 - - [23/Jun/2016:15:16:16 +0200] "GET /wp-content/plugins/slider-wd/css/font-awesome-4.0.1/fonts/fontawesome-webfont.woff?v=4.0.1 HTTP/1.1" 200 44476 "http://blog.s-m-s.pl/wp-content/plugins/slider-wd/css/font-awesome-4.0.1/font-awesome.css?ver=4.0.1" "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/2016:15:16:16 +0200] "GET /wp-content/uploads/2016/01/DSC4772-150x150.jpg HTTP/1.1" 200 7374 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:17 +0200] "GET /wp-content/uploads/2016/01/DSC4774-150x150.jpg HTTP/1.1" 200 8112 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:18 +0200] "GET /wp-content/plugins/slider-wd/images/ajax_loader.gif HTTP/1.1" 200 1475 "http://blog.s-m-s.pl/wp-content/plugins/slider-wd/css/wds_frontend.css?ver=1.1.38" "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/2016:15:16:18 +0200] "GET /wp-content/uploads/2016/01/DSC4776-150x150.jpg HTTP/1.1" 200 7839 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:18 +0200] "GET /wp-content/uploads/2016/01/YT2-e1455993080284-768x504.png HTTP/1.1" 200 118098 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:19 +0200] "GET /wp-content/plugins/google-calendar-events/assets/js/vendor/moment-timezone-with-data.min.js?ver=4.5.3 HTTP/1.1" 200 185042 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:19 +0200] "GET /wp-
content/uploads/2015/12/happy-first-birthday-e1455993006582.jpg
HTTP/1.1" 200 27325 "http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:20 +0200] "GET /wp-
content/uploads/2016/01/yt-e1455993066229.png HTTP/1.1" 200 122627
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:24 +0200] "GET /wp-
content/uploads/slider-wd/IMG_20150212_214319.jpg HTTP/1.1" 200 64351
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:24 +0200] "GET /wp-
content/uploads/2016/05/cropped-OnBlack.png HTTP/1.1" 200 428305
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:36 +0200] "GET /wp-
content/uploads/slider-wd/IMG_20150819_004414.jpg HTTP/1.1" 200 70767
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:41 +0200] "GET /wp-
content/uploads/slider-wd/IMG_20150212_214329.jpg HTTP/1.1" 200 59486
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:43 +0200] "GET /z-pamietnika-
admina-zosia-samosia-robi-migracje/ HTTP/1.1" 200 32004
"http://blog.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"
94.254.243.166 - - [23/Jun/2016:15:16:47 +0200] "GET /wp-
content/plugins/akismet/_inc/form.js?ver=3.1.11 HTTP/1.1" 200 700
```

```
"http://blog.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/2016:15:16:47 +0200] "GET /wp-
includes/js/comment-reply.min.js?ver=4.5.3 HTTP/1.1" 200 1078
"http://blog.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/2016:15:16:49 +0200] "GET /wp-
content/uploads/2016/06/Drawing1.png HTTP/1.1" 200 18640
"http://blog.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/2016:15:16:49 +0200] "GET /wp-
content/uploads/2016/06/home1.png HTTP/1.1" 200 4950
"http://blog.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/2016:15:16:49 +0200] "GET /wp-
content/uploads/2016/06/az1.png HTTP/1.1" 200 4481
"http://blog.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/2016:15:16:50 +0200] "GET /wp-
content/uploads/2016/06/home3.png HTTP/1.1" 200 53934
"http://blog.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/2016:15:16:50 +0200] "POST /wp-admin/admin-
ajax.php HTTP/1.1" 200 69
"http://blog.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/2016:15:16:52 +0200] "GET /wp-
content/uploads/2016/06/lol.png HTTP/1.1" 200 763499
"http://blog.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
"http://blog.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
"http://blog.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
"http://blog.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
"http://blog.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
"http://blog.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 "http://blog.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"
```

w pierwszej chwili w oczy rzuciła mi się ta linijka:

```
94.254.243.166 - - [23/Jun/2016:15:27:14 +0200] "POST /wp-comments-post.php HTTP/1.1" 302 5 "http://blog.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"
```

Oznaczała ona bowiem, że intruz zostawił komentarz na stronie 23 czerwca o 15:27. Wiedziałem w którym artykule, więc szybko sprawdziłem.

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

Jak widać – mamy motyw. Mamy również dane, które mogą ze stuprocentową pewnością wskazać sprawcę owego „wycieku”. Dane te pozwalają nam bez powiadamiania policji zidentyfikowac sprawce, ponieważ znamy jego metodologie działania oraz widzimy korelacje z wydarzeniami. Natomiast cała wklejka i mail to marne próby zszargania wizerunku mojego i SMS. Po konsultacji z prawnikiem zostałem zapewniony, że w tym przypadku zarówno ja i stowarzyszenie SMS wygrałoby sprawę o zniesławienie. Ale my sie nie gniewamy

Oczywiście rozchodzi się o stronę securweb.pl która była hostowana na jednym z należących do mnie serwerów hostingowych, ale po naruszeniach bezpieczeństwa dokonanych na shellu oraz hostingu dostęp został zamknięty a strona zablokowana (czyt. położona) zgodnie z umową, którą zawarlismy z osobą prowadzącą tę stronę.

To tyle co udało się ustalic analizując logi i dane z plików. Sam gdrive powiedział mi, że wrzucił to niejaki Zbigniew Budziewski. Wklepałem to w facebooka i moim oczom ukazał się fikcyjny profil autora securweb.pl.

~~Zdecydowałem się udostępnić link do profilu~~, ponieważ mam 100% pewność, iż profil nie należy do realnej osoby a jest tzw lurkkontem służącym do ukrycia prawdziwej

tożsamości K0sm3na/iktora/Grześka.

PS.

O godzinie 21:42 na IRC'u znów pojawił się user LeakCrew. Poniżej wrzucam log z rozmowy w której pojawia się pytanie czy się nie gniewam i że był to niewinny żart.

Source code

```
[21:42:57] *** Joins: LeakCrew (~androirc@219.250.174.195)
[21:43:03] <LeakCrew> http://pastebin.com/Q6xBwrsf
[21:43:20] <LeakCrew> Wstyd panie
[21:43:23] <prezes> siemka LeakCrew :D
[21:43:46] <prezes> LeakCrew, jak tam?
[21:44:03] <LeakCrew> Do dupy
[21:44:07] <prezes> czemu?
[21:44:16] *** Joins: Wolf480pl (wolf480pl@faris.wolf480.pl)
[21:44:30] <prezes> LeakCrew, ale żes dojebał temu pht
co nie Wolf480pl?
[21:44:56] <Wolf480pl> dunno, ja tam w szczegóły nie wchodziłem
[21:45:21] <prezes> koles podobno od rana w cbśp siedzi u ziomeczków
i kapuje
[21:45:38] <prezes> LeakCrew, żebys nie miał abwery na chacie
[21:45:47] <prezes> LeakCrew, dobrze ze masz tora
[21:45:58] <LeakCrew> Prezes =pehat
[21:46:07] <prezes> kek :D
[21:46:11] <prezes> nie udało mi sie :D
[21:46:19] <prezes> ten whois mnie zdradził :D
[21:47:17] <LeakCrew> Oj tam
[21:47:29] <LeakCrew> To byl zart z tym leakiem
[21:47:47] <LeakCrew> Przeciez nie wlamalismy sie
[21:47:55] <prezes> hehe :D no i tak był potraktowany :D
[21:48:15] <LeakCrew> Nie bylo kodeksu karnego
[21:48:27] <prezes> :D był :D
[21:48:33] <LeakCrew> Tor is ewrybady
[21:48:33] <prezes> zniesławienie :D
[21:48:42] <prezes> ale co ja tam wiem :D
[21:48:45] <LeakCrew> Ta pranie pieniedzy chyba
[21:48:48] <LeakCrew> :)
```

[21:48:50] <prezes> toż to niewinny żart :D
[21:48:56] <prezes> LeakCrew, daj linka na wykop
[21:48:57] <prezes> a nie
[21:49:01] *** Joins: teqwve (~teqwve@vhost:futuregadgetlab.cern)
[21:49:07] <prezes> bo tego nie podałeś tylko
[21:49:20] <LeakCrew> Nie mam konta na f b
[21:49:30] <LeakCrew> Wiec nie zaloze
[21:49:34] <prezes> a co ma fb do wykopu :D
[21:49:44] <LeakCrew> Czekaj maciek ma
[21:49:45] <prezes> ej to piszesz ze lata po wykopie i straszysz mnie mirkami a nie wrzucasz
[21:49:48] <prezes> o
[21:49:52] <prezes> to niech maciek wrzuci
[21:49:58] <LeakCrew> Bo logowanir przez fb
[21:50:16] <LeakCrew> Miroslawie xD
[21:50:27] * prezes nie siedzi na mirkach.
[21:50:33] * prezes woli kurachany
[21:50:44] <LeakCrew> Mirek siedzi na piotrze
[21:50:58] <LeakCrew> :)
[21:51:10] <prezes> :D
[21:51:20] <LeakCrew> Kasuje ta paste z pastebinu
[21:51:22] <prezes> LeakCrew, skąd klikasz miśku :D
[21:51:39] <LeakCrew> Ruch na serwie ci podskoczyl?
[21:51:55] <LeakCrew> DDOs mial byc
[21:52:02] <LeakCrew> Przez wykopka
[21:52:10] <LeakCrew> Ale nie wyszlo
[21:52:13] <prezes> LeakCrew, kek :D
[21:52:17] <LeakCrew> Klikam z Wawy
[21:52:40] <prezes> LeakCrew, słabo, ze nie macie z maćkiem mocy na ddosa :D to smutne :D
[21:53:01] <LeakCrew> My to nie lukasz S.
[21:53:04] <LeakCrew> :D
[21:53:19] <prezes> a to słabisna, teraz każdy ma botnet :)
[21:53:22] <LeakCrew> Ani sergiusz ruskie servery
[21:53:33] <LeakCrew> Po uj botnet
[21:53:43] <LeakCrew> Nie niszczymy
[21:53:52] <LeakCrew> I nie podmieniamy stron
[21:54:06] <LeakCrew> To jest za bardzo gimbusiarskie

[21:54:37] <prezes> no niby :D ale są tacy co to robią :D
[21:54:54] <LeakCrew> Ta cebulaki z hydry xD
[21:55:10] <LeakCrew> Gimbo janusze internetow
[21:55:16] <LeakCrew> xD
[21:55:18] <prezes> ja tam nie gadam z takimi :D jeszcze mi podmienią strone :(
[21:55:42] <LeakCrew> Akurat na ta wersje wp nie ma exploita
[21:55:50] <prezes> ty a ja mam :D
[21:55:54] <prezes> ale mniejsza
[21:56:00] <prezes> nie kasuj wklejki :D
[21:56:02] <prezes> śmieszna jest
[21:56:07] <LeakCrew> Nie
[21:56:31] <LeakCrew> Bo jeszcze ci sie wlamia i bedziemy mieli wzuty sumienia
[21:56:44] <prezes> :D
[21:56:53] <LeakCrew> Mamy sqli na forum.abw.gov.pl
[21:56:54] <prezes> no pewnie używajac tego klucza z paczki
[21:57:06] <prezes> LeakCrew, ale tam każdy ma :D
[21:57:31] <LeakCrew> Ten klucz nie dziala
[21:57:43] <LeakCrew> Ale haselko masz pinkne
[21:58:05] <prezes> a no wiem :D
[21:58:50] <LeakCrew> Gdyby nie tor to mieli bysmy cbs? Watpie. Te pajace nic nie robia
[21:59:13] <LeakCrew> Btw happynidzas sa z cbsp
[21:59:20] <LeakCrew> Tzn byli
[21:59:23] <prezes> ;>
[22:00:14] <prezes> LeakCrew, ogólnie, wiesz, ze ten klucz, który znaleźliście to klucz publiczny nie?
[22:00:28] <LeakCrew> Wiemy
[22:00:37] <LeakCrew> To byla podpucha
[22:00:42] <prezes> wiec jak miałby działac :D
[22:00:48] <LeakCrew> Zrobiona przez ciebir
[22:00:48] <prezes> LeakCrew> Ten klucz nie dziala
[22:00:54] <LeakCrew> To byl joke
[22:00:55] <prezes> kek
[22:01:01] <LeakCrew> I sie udal
[22:01:13] <LeakCrew> Teraz czas na maklera
[22:01:19] <Wolf480pl> no tak, bo przecież plik nazywał się

```
private_rsa.txt
[22:01:20] <LeakCrew> Tylko cii ;)
[22:01:58] <LeakCrew> Piotr zestresowales sie po otwarciu mejla?
[22:02:00] <prezes> nigdy sie nie nazywał sie private rsa :)
[22:02:24] <prezes> Każdy taki mail traktuje poważnie, do momentu
gdy zobacze co serio w nim jest :)
[22:03:07] <LeakCrew> Nastepnym razem dostaniesz mejl z naglowkami nsa
[22:03:10] <LeakCrew> :)
[22:03:32] <prezes> LeakCrew, spoko! o ile już ich nie mam, wiesz taka
praca.
[22:03:51] <LeakCrew> Btw niebezpiecznika j z3s nie wtajemniczalismy
[22:04:03] <prezes> szkoda :(
[22:04:09] <prezes> tzreba było :)
[22:04:14] <prezes> trzeba*
[22:04:26] <LeakCrew> Po uj
[22:04:35] <LeakCrew> To mial byc zart
[22:04:43] <LeakCrew> I zostal zartem
[22:05:09] <prezes> No spoko :)
[22:05:30] <LeakCrew> Nie gniewasz sie na nas?
[22:05:51] <prezes> ja? Ja sie na nikogo nigdy nie gniewam
[22:06:08] <LeakCrew> Tylko biegam na milicje
[22:06:10] <LeakCrew> :)
[22:06:31] <prezes> po co na milicje;>
[22:09:14] <prezes> LeakCrew, ja wole sam poczytac logi i metadane :)
```

Przejdźmy teraz do chronologii wydarzeń

1. 15-16 23.06.2016 – „Intruz” przegląda s-m-s.pl i komentuje wpis.
2. 4:31-5:56 26.06.2016 – „Intruz” pobiera dane z publicznie dostępnego hosta. W jego przekonaniu znalazł poufne dane.
3. 5:04 26.06.2016 – Intruz tworzy paczkę i wrzuca pasty na pastebina.
4. 6:34 26.06.2016 – Na mojej skrzynce pojawia się mail wysłany z Protonmaila.
5. 6:50 26.06.2016 – Na kanałach IRC pojawiają się linki do pasty.
6. 7:18 26.06.2012 – Na IRC przez prywatną wiadomość dostaję link do pasty.
7. 7:30 26.06.2016 – Odczytuję maila.
8. 7:40 26.06.2016 – Publikacja pasty i info na socialkach, zastawiam pułapkę
9. 13:00 26.06.2016 – Zaczynam czytać logi.
10. 14:00 26.06.2016 – Już wszystko wiem, piszę ten artykuł dokonując analizy logów.

11. 20:00 26.06.2016 – Artykuł gotowy.
12. 21:42 26.06.2012 – LeakCrew znów się odzywa i zapewnia, że to wszytsko to był tylko żart.

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

Podsumowanie

Ten artykuł powinien byc przestrogą dla każdej organizacji oraz osoby publicznej, że nie należy odpuszczać chociaż na chwilę tematu bezpieczeństwa. Jesli to zrobimy, możemy gorzko pożałować. O ile w tym przypadku nie wyciekło nic wrażliwego, intruzem mógł się okazać doświadczony specjalista od bezpieczeństwa, haker, cracker lub osoba która zna nasz sposób zabezpieczania systemów. W takiej sytuacji nie tylko możemy zostać skompromitowani wyciekiem danych ale również przejęciem naszej witryny czy tożsamości, co może okazać się niszczące dla naszej organizacji i spowodować, że cały zbudowany autorytet zniknie, a nasza włożona praca pójdzie na marne. Najlepiej ujęto to na IRC-u podczas konwersacji na temat całego zajścia:

> <toligniew> prezes: jak to jest być celebrytą?
> <Wolf480pl> hmm.. prezesa nie ma ale chyba mogę co nie co powiedzieć za niego:
> <Wolf480pl> jak jesteś celebrytą to randomowe nooby z internetu próbują cię „zhackować” i jak znajdą gdzieś automatyczny indeks www na twoim serwerze
> <Wolf480pl> a na nim twój klucz publiczny
> <Wolf480pl> to się hypeują „wow wow zhackowałem pehata”

Co dalej?

Dalszymi krokami jakie zostaną podjęte po dzisiejszych wydarzeniach będzie ponowne zwiększenie poziomu bezpieczeństwa insfrastruktury SMS. Tymsamym SMS oficjalnie informuje, iz rusza z programem testów, audytów oraz szkoleń dla jednostek użytku publicznego działających w oparciu o ustawę o stowarzyszeniach. Tyczy się to stowarzyszeń,

fundacji i wszystkich jednostek działających na rzecz społeczności. Zgłoszenia do programu można nadsyłać na piotr.jasiek@blog.s-m-s.pl. Pod tym samym adresem można uzyskać więcej informacji.