Trend Micro
Research Paper
2012

The "Police Trojan"

AN IN-DEPTH ANALYSIS

By: David Sancho and Feike Hacquebord

CONTENTS

Introduction....1
Technical Analysis....1
  Technical Findings....4
Network Analysis....6
Connections to other Malware Campaigns....10
Possible Infection Starting Point....11
Conclusion....11
Appendix....12
  Associated Email Addresses....12
  C&C Servers....12
  Other IP Addresses....12
  Possibly Associated Domains....12

INTRODUCTION

A ransomware is a kind of malware that withholds some digital assets from victims and asks for payment for the assets' release. Ransomware attacks were first seen in Russia in 2005–2006 and have since changed tactics and targets.

The most recent wave of ransomware attacks targeted users in a very specific way—tracking their geographic locations and scaring them with their respective countries' police forces while holding their entire systems captive. These attacks have come to be known as the "Police Trojan" attacks.

Trend Micro has been tracking this campaign since the beginning and is now ready to show some of our conclusions after the investigation. A mix of well-tuned social engineering tactics as well as an advanced and very dynamic networking model shows that the Police Trojan's creators are well-organized, apart from being persistent and creative.

TECHNICAL ANALYSIS

Based on purely technical analysis, we found that the Police Trojan is a run-of-the-mill ransomware Trojan. After infecting a user's system, it contacts a command-and-control (C&C) server that detects what country the victim is from. If the victim's country is in the ransomware's list, it downloads a localized graphic with the appropriate language and police force logo then hijacks the victim's screen so he/she cannot do anything until he/she has paid a fine.

On first run—when run with no parameters, the Police Trojan creates a copy of itself in an innocuous-looking folder such as:

```
c:\Documents and Settings\%user%\Application
Data\adobeflash\adobeflash.exe
```

Afterward, it creates a persistency mechanism—a simple registry entry in the *autorun* registry hive. Note how it uses a *-b* parameter to distinguish between the first and subsequent executions:

```
HKCU\Software\Microsoft\Windows\
CurrentVersion\Run\
["c:\Documents and
Settings\%user%\Application
Data\adobeflash\adobeflash.exe -b"]
```

Then it starts itself in a special installation mode. To do this, it runs itself again but this time with an *-i* parameter (we assume *"i"* stands for "install"):

```
c:\Documents and Settings\%user%\Application
Data\adobeflash\adobeflash.exe -i
```

During the installation—when run with an *-i* parameter, the Trojan injects the installation code into *explorer.exe* so that all HTTP connections that will be described next happen from that process. The first thing it does is to connect to the first of a set of four hardcoded C&C servers and a specific HTTP server path from a set of 15.

In the samples we have seen, the C&C servers always pointed to the same IP address. The attackers do not use four different C&C servers, as the four spots always point to the same IP address.

After the first contact, the server must reply with one of two possible strings—"ok" or "del." The "ok" string allows the sequence to proceed. The "del" string, on the other hand, makes the Trojan delete itself from the system, along with the registry key it created.

Based on our observation, the C&C servers reply with "ok" when a client comes from a country that the attackers' localization efforts support. The following are the "target countries" we have seen:

- Germany
- Spain
- France
- Italy
- Belgium
- Great Britain
- Austria

Requests coming from any other country return a "del" command, which helps avoid infecting systems from places other than those specifically targeted.

Once the client receives an "ok" command to the first request, it continues the sequence described below. It sends a request to find what geographical area it is connecting from. The server provides a link to download the bitmap image representing the logo of the police force of the appropriate location.

- *> /loc/gate.php?getip=getip*
- *< 1.2.3.4* (your IP address)
- *> /loc/gate.php?getpic=getpic*
- *< http://<C&C ip address>/pic/ES.bmp*

The Trojan then downloads the bitmap image and stores it as:

```
c:\Documents and Settings\%user%\Application
Data\adobeflash\pic.BMP
```

The image is displayed when in ransomware mode—when run with the *-b* parameter.

The following list the URL paths though we have only seen servers and clients use */loc/gate.php:*

- *cow/gate.php*
- *like/gate.php*
- *mozy/gate.php*
- *leex/gate.php*
- *zuum/gate.php*
- *plea/gate.php*
- *code/gate.php*
- *zerro/gate.php*
- *milk/gate.php*
- *tron/gate.php*
- *prog/gate.php*
- *in/gate.php*
- *pic8/gate.php*
- *zip/gate.php*
- *loc/gate.php*

At some point, the Trojan also tries to update itself by accessing the following URL:

```
/loc/gate.php?user=lesnik1&upg=upg
```

In ransomware mode—when run with the *-b* parameter, the Trojan creates two threads:

- *Thread 1:* A never-ending loop that displays *pic.BMP* and waits for the user to enter his/her *Ukash* or *Paysafe* personal identification number (PIN), which means the victim has paid the ransom.
- *Thread 2:* Another loop that constantly checks the process list to look for processes named:
  - *regedit.exe*
  - *msconfig.exe*
  - *seth.exe*
  - *utilman.exe*
  - *narrator.exe*

Once the Trojan finds one of these, it kills the process. This is, in effect, a black list of processes that the ransomware's author absolutely does not want to run on the system.

Regedit.exe and *msconfig.exe* are familiar to any system administrator or power user. These are the *Registry Editor* and the *System Configuration* tools, respectively. The other binaries are special programs that the *Windows OS* calls by means of specific key combinations. They are legitimately used to enable accessibility. It is possible to rename the *Command Prompt* program—*cmd.exe,* to one of the names above and therefore gain access to the hijacked computer by pressing the right key sequence. The ransomware's author denies the use of this trick on the part of the administrator of the victim's computer by killing the programs as soon as these are opened. These are the sequences for documentation purposes:

- *Seth.exe:* Press the *Shift* key five times.
- *Utilman.exe:* Press the *Windows* and *U* keys at the same time.
- *Narrator.exe:* In the login screen, click *Ease of Access* then *Narrator*. This is also accessible from the real *utilman.exe* tool.

The Police Trojan also has a few other small capabilities. One of these is that before calling home to download the appropriate image, it checks if *pinok.txt* file exists in the installation folder. If it does, the Trojan looks inside it for specific content. This file is created once the ransomware determines that the user has entered his/her *Ukash* or *Paysafe* PIN and that the PIN has been verified.

The Police Trojan employs two checks for *pinok.txt*—one for *Ukash* and another for *Paysafe*. The following shows how it checks for *Ukash:*

- The PIN must be exactly 19 bytes long.
- It must contain the string, *"633718XXX,"* where *XXX* is a short list of three-digit combinations.
- It must not contain any string found in the following hardcoded list:
    - *"0000000000000001"*
    - *"0000000000000011"*
    - *"1111111111111111"*
    - *"2222222222222222"*
    - *"3333333333333333"*
    - *"4444444444444444"*
    - *"5555555555555555"*
    - *"6666666666666666"*
    - *"7777777777777777"*
    - *"8888888888888888"*
    - *"9999999999999999"*
    - *"12345"*
    - *"6789"*
    - *"9876"*
    - *"54321"*
    - *"1111"*
    - *"2222"*
    - *"3333"*
    - *"4444"*
    - *"5555"*
    - *"6666"*
    - *"7777"*
    - *"8888"*
    - *"9999"*
    - *"0000"*

Some of the rules contradict others, which reinforces our theory that the code is dirty. Moreover, in our sample, when we create a valid *pinok.txt* file, the program fails.

If the victim ends up paying and entering a valid PIN, it is submitted to the C&C server, along with other system-related information:

```
/loc/gate.php?user=[affiliate_id]&uid=
[unique_id]&os=[OS_number]&pin=[UKash_
PaysafePIN]
```

The Police Trojan also supports a *-u* parameter that does not do anything much. It just exits.

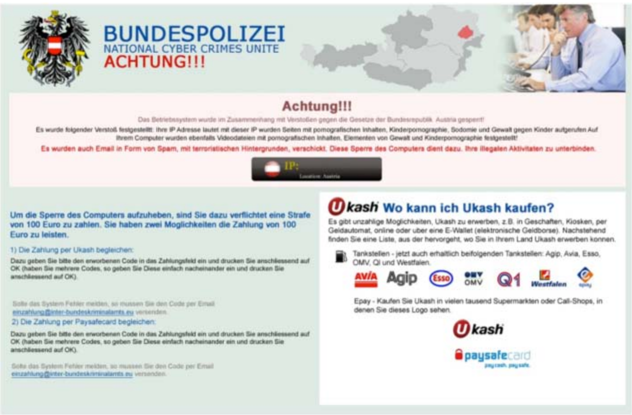
The name of the mutex that the Trojan uses to check if it is already running is *jwergwekrkwerlw.* This is hardcoded in the code but since it looks random, it does not provide any clue to aid in our analysis.

The Police Trojan contains a debugging code that displays errors in Russian. Warnings such as "Error copying file" or "Mutex found, stop not passed, we delete ourselves" look like remnants from the development process that the author did not bother to remove from the final version but definitely pointed us to its origin.

Technical Findings

It is interesting to note that we saw different C&C login requests of the same kind but with different user names. Since the user name appears to be hardcoded into the binary, along with the C&C server to connect to, this could mean that the cybercriminals recompiled the binary on a per-user basis. We also saw user names such as *affiliate_18,* which suggests that the cybercriminals' infection model was by means of an affiliate network that relies on partners for distribution, most likely by means of porn pages. This theory matches our expectation that there must be an affiliate download site where partners can download a ready-made Trojan using their own user names and the C&C server of the day already embedded. This also explains the very low detection rates across the board. Each Trojan is custom compiled with different configurations and applies two layers of packing and obfuscation on top. Given the rate at which the attackers are changing C&C servers, this recompilation must be happening very often that is why security companies are having a difficult time obtaining good detections.

Figures 1–7 show the images downloaded to infected systems, depending on what regions these are in. Note how the police forces' logos perfectly match the victims' respective geographical areas even though the languages used are not native in all cases.



BUNDESPOLIZEI
NATIONAL CYBER CRIMES UNITE
ACHTUNG!!!

Achtung!!!

Das Betriebssystem wurde im Zusammenhang mit Verstoßen gegen die Gesetze der Bundesrepublik Austria gesperrt!

Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornographie festgestellt!

Es wurden auch Email in Form von Spam, mit terroristischen Hintergrunden., verschickt. Diese Sperre des Computers dient dazu. Ihre illegalen Aktivitaten zu unterbinden.

IP:
Location: Austria

Um die Sperre des Computers aufzuheben, sind Sie dazu verflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Moglichkeiten die Zahlung von 100 Euro zu leisten.

1) Die Zahlung per Ukash begleichen:

Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drucken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drucken Sie anschliessend auf OK).

Solte das System Fehler melden, so mussen Sie den Code per Email einzahlung@inter-bundeskriminalamts.eu versenden.

2) Die Zahlung per Paysafecard begleichen:

Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drucken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drucken Sie anschliessend auf OK).

Solte das System Fehler melden, so mussen Sie den Code per Email einzahlung@inter-bundeskriminalamts.eu versenden.

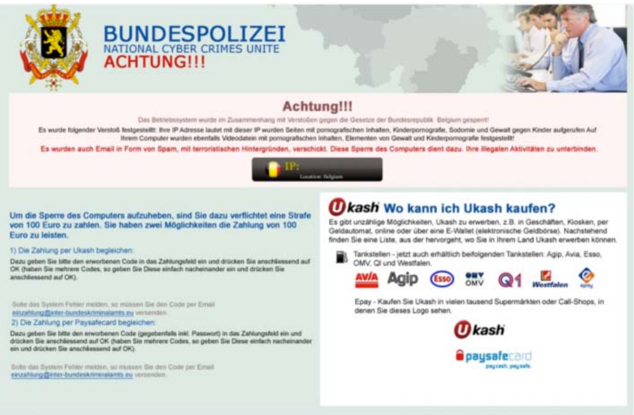
Ukash Wo kann ich Ukash kaufen?

Es gibt unzahlige Moglichkeiten, Ukash zu erwerben, z.B. in Geschaften, Kiosken, per Geldautomat, online oder uber eine E-Wallet (elektronische Geldborse). Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben konnen.

Tankstellen - jetzt auch erhaltich beifolgenden Tankstellen: Agip, Avia, Esso, OMV, Ql und Westfalen.

Epay - Kaufen Sie Ukash in vielen tausend Supermarkten oder Call-Shops, in denen Sie dieses Logo sehen.

Figure 1: Image users from Austria see



BUNDESPOLIZEI
NATIONAL CYBER CRIMES UNITE
ACHTUNG!!!

Achtung!!!

Das Betriebssystem wurde im Zusammenhang mit Verstoßen gegen die Gesetze der Bundesrepublik Belgium gesperrt!

Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornografie, Sodomie und Gewalt gegen Kinder aufgerufen Auf Ihrem Computer wurden ebenfalls Videodatein mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Email in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu. Ihre illegalen Aktivitäten zu unterbinden.

IP:
Location: Belgium

Um die Sperre des Computers aufzuheben, sind Sie dazu verflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.

1) Die Zahlung per Ukash begleichen:

Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK).

Solte das System Fehler melden, so müssen Sie den Code per Email einzahlung@inter-bundeskriminalamts.eu versenden.

2) Die Zahlung per Paysafecard begleichen:

Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK).

Solte das System Fehler melden, so mussen Sie den Code per Email einzahlung@inter-bundeskriminalamts.eu versenden.

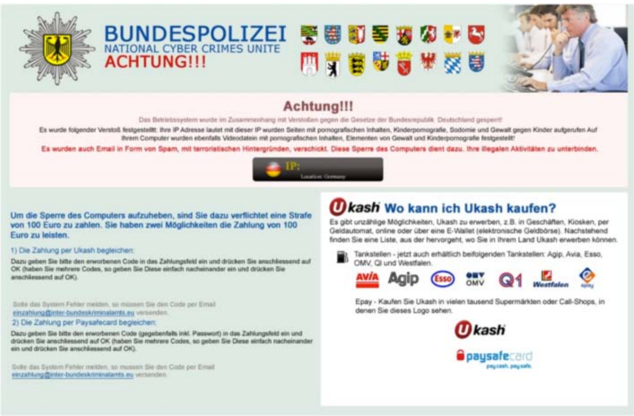
Ukash Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z.B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse). Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich beifolgenden Tankstellen: Agip, Avia, Esso, OMV, Ql und Westfalen.

Epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

Figure 2: Image users from Belgium see



BUNDESPOLIZEI
NATIONAL CYBER CRIMES UNITE
ACHTUNG!!!

Achtung!!!

Das Betriebssystem wurde im Zusammenhang mit Verstoßen gegen die Gesetze der Bundesrepublik Deutschland gesperrt!

Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornografie, Sodomie und Gewalt gegen Kinder aufgerufen Auf Ihrem Computer wurden ebenfalls Videodatein mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Email in Form von Spam, mit terroristischen Hintergründen., verschickt. Diese Sperre des Computers dient dazu. Ihre illegalen Aktivitäten zu unterbinden.

IP:
Location: Germany

Um die Sperre des Computers aufzuheben, sind Sie dazu verflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.

1) Die Zahlung per Ukash begleichen:

Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK).

Solte das System Fehler melden, so müssen Sie den Code per Email einzahlung@inter-bundeskriminalamts.eu versenden.

2) Die Zahlung per Paysafecard begleichen:

Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK).

Solte das System Fehler melden, so mussen Sie den Code per Email einzahlung@inter-bundeskriminalamts.eu versenden.

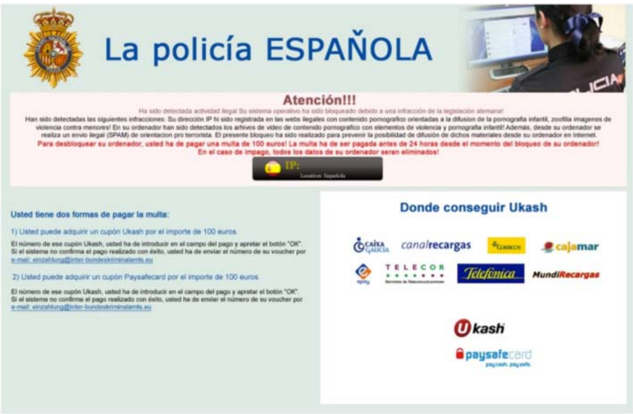
Ukash Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z.B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse). Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich beifolgenden Tankstellen: Agip, Avia, Esso, OMV, Ql und Westfalen.

Epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

Figure 3: Image users from Germany see



La policía ESPAŇOLA

Atención!!!

Ha sido detectada actividad ilegal Su sistema operativo ha sido bloqueado debido a una infracción de la legislación alemana!

Han sido detectadas las siguientes infracciones: Su dirección IP hi sido registrada en las webs ilegales con contenido pornografico orientadas a la difusion de la pornografia infantil, zoofilia imagenes de violencia contra menores! En su ordenador han sido detectados los arhivos de video de contenido pornografico con elementos de violencia y pornografia infantil! Además, desde su ordenador se realiza un envio ilegal (SPAM) de orientacion pro terrorista. El presente bloqueo ha sido realizado para prevenir la posibilidad de difusión de dichos materiales desde su ordenador en Internet.

Para desbloquear su ordenador, usted ha de pagar una multa de 100 euros! La multa ha de ser pagada antes de 24 horas desde el momento del bloqueo de su ordenador! En el caso de impago, todos los datos de su ordenador seran eliminados!

IP:
Location: Española

Usted tiene dos formas de pagar la multa:

1) Usted puede adquirir un cupón Ukash por el importe de 100 euros.

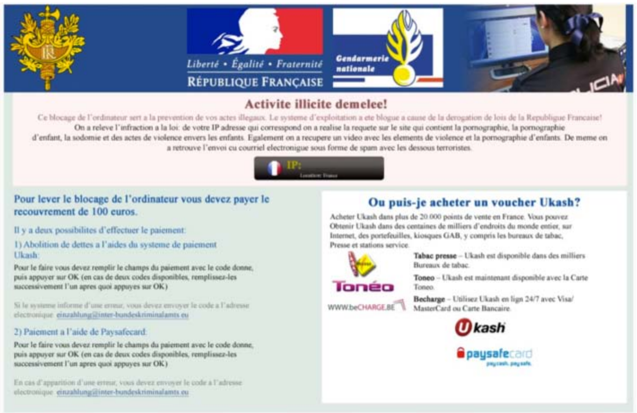
El número de ese cupón Ukash, usted ha de introducir en el campo del pago y apretar el botón "OK". Si el sistema no confirma el pago realizado con éxito, usted ha de enviar el número de su voucher por e-mail: einzahlung@inter-bundeskriminalamts.eu

2) Usted puede adquirir un cupón Paysafecard por el importe de 100 euros.

El número de ese cupón Ukash, usted ha de introducir en el campo del pago y apretar el botón "OK". Si el sistema no confirma el pago realizado con éxito, usted ha de enviar el número de su voucher por e-mail: einzahlung@inter-bundeskriminalamts.eu

Donde conseguir Ukash

Figure 4: Image users from Spain see



Activite illicite demelee!

Ce blocage de l'ordinateur sert a la prevention de vos actes illegaux. Le systeme d'exploitation a ete blogue a cause de la derogation de lois de la Republigue Francaise!
On a releve l'infraction a la loi: de votre IP adresse qui corresspond on a realise la requete sur le site qui contient la pornographie, la pornographie d'enfant, la sodomie et des actes de violence envers les enfants. Egalement on a recupere un video avec les elements de violence et la pornographie d'enfants. De meme on a retrouve l'envoi cu courriel electronigue sous forme de spam avec les dessous terroristes.

IP:
Location: France

Pour lever le blocage de l'ordinateur vous devez payer le recouvrement de 100 euros.

Il y a deux possibilites d'effectuer le paiement:

1) Abolition de dettes a l'aides du systeme de paiement Ukash:

Pour le faire vous devez remplir le champs du paiement avec le code donne, puis appuyer sur OK (en cas de deux codes disponibles, remplissez-les successivement l'un apres quoi appuyes sur OK)

Si le systeme informe d'une erreur, vous devez envoyer le code a l'adresse electronique einzahlung@inter-bundeskriminalamts.eu

2) Paiement a l'aide de Paysafecard:

Pour le faire vous devez remplir le champs du paiement avec le code donne, puis appuyer sur OK (en cas de deux codes disponibles, remplissez-les successivement l'un apres quoi appuyes sur OK)

En cas d'apparition d'une erreur, vous devez envoyer le code a l'adresse electronique einzahlung@inter-bundeskriminalamts.eu

Ou puis-je acheter un voucher Ukash?

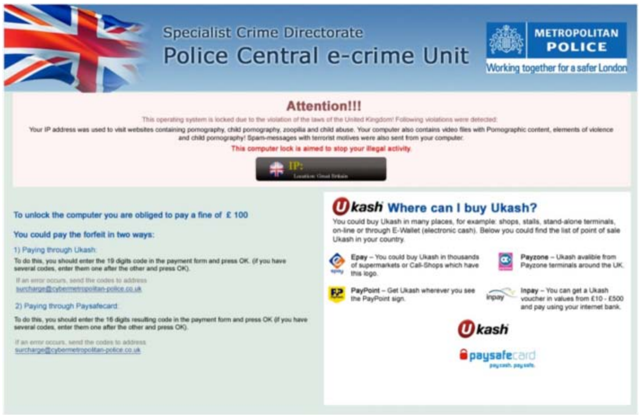
Acheter Ukash dans plus de 20.000 points de vente en France. Vous pouvez Obtenir Ukash dans des centaines de milliers d'endroits du monde entier, sur Internet, des portefeuilles, kiosques GAB, y compris les bureaux de tabac, Presse et stations service.

Tabac presse – Ukash est disponible dans des milliers Bureaux de tabac.

Toneo – Ukash est maintenant disponible avec la Carte Toneo.

Becharge – Utilisez Ukash en lign 24/7 avec Visa/ MasterCard ou Carte Bancaire.

Figure 5: Image users from France see



Specialist Crime Directorate
Police Central e-crime Unit

Attention!!!

This operating system is locked due to the violation of the laws of the United Kingdom! Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoopilia and child abuse. Your computer also contains video files with Pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

IP:
Location: Great Britain

To unlock the computer you are obliged to pay a fine of £ 100

You could pay the forfeit in two ways:

1) Paying through Ukash:

To do this, you should enter the 19 digits code in the payment form and press OK. (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address surcharge@cybermetropolitan-police.co.uk

2) Paying through Paysafecard:

To do this, you should enter the 16 digits resulting code in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address surcharge@cybermetropolitan-police.co.uk

Ukash Where can I buy Ukash?

You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.

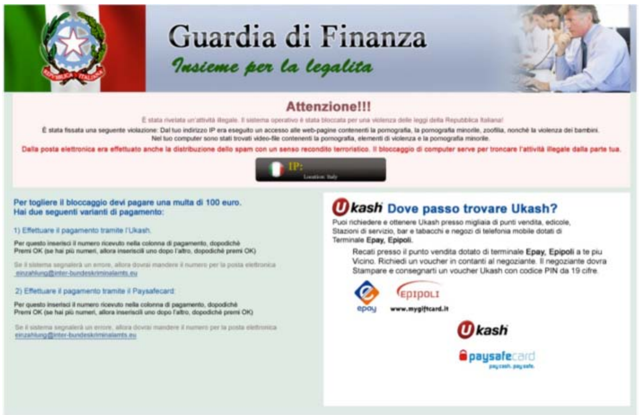
Epay – You could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.

Payzone – Ukash avalible from Payzone terminals around the UK.

PayPoint – Get Ukash wherever you see the PayPoint sign.

Inpay – You can get a Ukash voucher in values from £10 - £500 and pay using your internet bank.

Figure 6: Image users from Great Britain see



Guardia di Finanza
Insieme per la legalita

Attenzione!!!

È stata rivelata un'attività illegale. Il sistema operativo è stata bloccata per una violenza delle leggi della Repubblica Italiana!
È stata fissata una seguente violazione: Dal tuo indirizzo IP era eseguito un accesso alle web-pagine contenenti la pornografia, la pornografia minorile, zoofilia, nonchè la violenza dei bambini.
Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile.
Dalla posta elettronica era effettuato anche la distribuzione dello spam con un senso recondito terroristico. Il bloccaggio di computer serve per troncare l'attività illegale dalla parte tua.

IP:
Location: Italy

Per togliere il bloccaggio devi pagare una multa di 100 euro.
Hai due seguenti varianti di pagamento:

1) Effettuare il pagamento tramite l'Ukash.

Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché Premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK)

Se il sistema segnalerà un errore, allora dovrai mandere il numero per la posta elettronica einzahlung@inter-bundeskriminalamts.eu

2) Effettuare il pagamento tramite il Paysafecard:

Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché Premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK)

Se il sistema segnalerà un errore, allora dovrai mandere il numero per la posta elettronica einzahlung@inter-bundeskriminalamts.eu

Ukash Dove passo trovare Ukash?

Puoi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, Stazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di Terminale **Epay, Epipoli**.

Recati presso il punto vendita dotato di terminale **Epay, Epipoli** a te piu Vicino. Richiedi un voucher in contanti al negoziante. Il negoziante dovra Stampare e consegnarti un voucher Ukash con codice PIN da 19 cifre.

Figure 7: Image users from Italy see

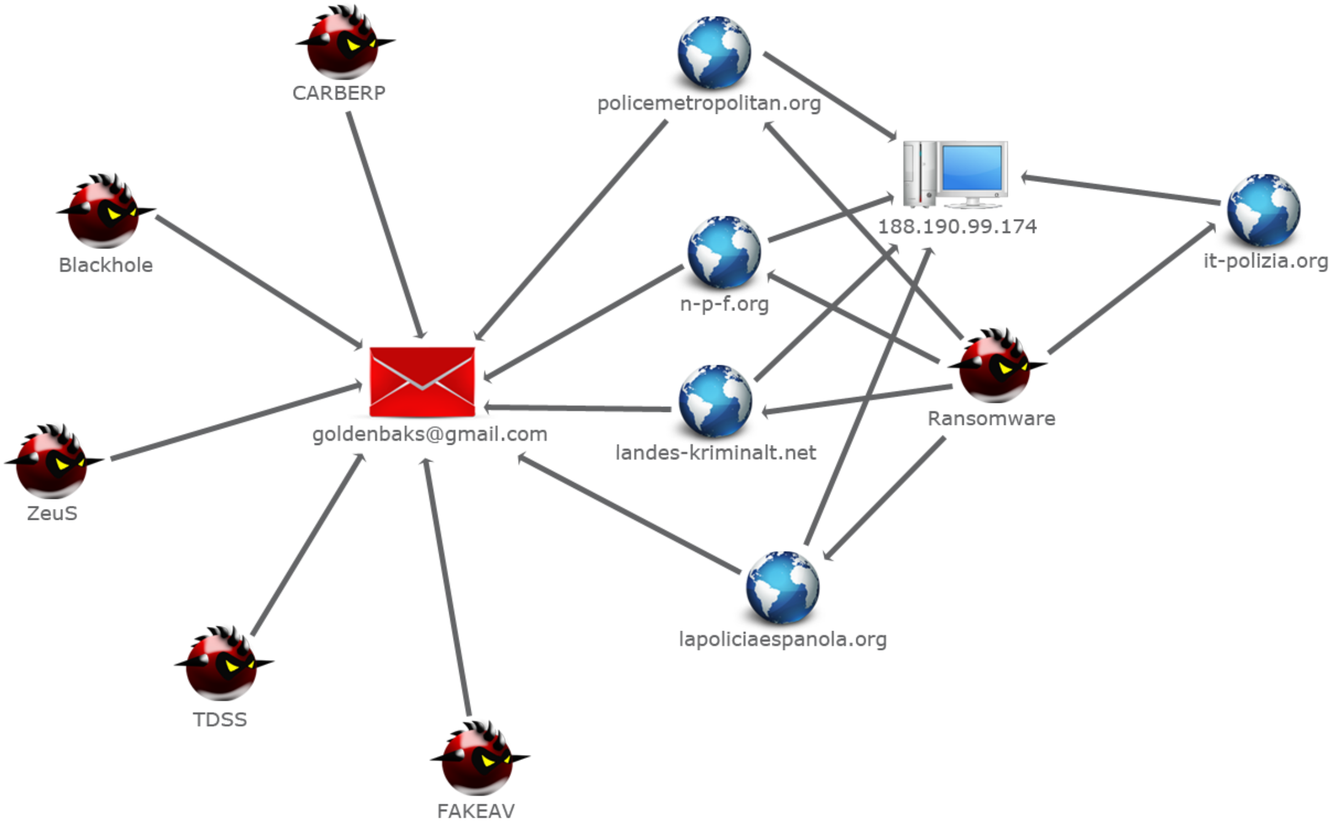
NETWORK ANALYSIS

The starting point of our network analysis was the IP address, *188.190.99.174,* which is located in the Ukraine. The address hosted a Police Trojan C&C server in February 2012 (see a sample analysis at http://www.abuse.ch/?p=3610).

A few domains were involved in the attack as well. These domains were also hosted on *188.190.99.174* and related to the European police force the Trojan impersonates. Looking at the email addresses of the registrants in *whois* revealed the following:

- *landes-kriminalt.net (goldenbaks@gmail.com)*
- *policemetropolitan.org (goldenbaks@gmail.com)*
- *n-p-f.org (goldenbaks@gmail.com)*
- *it-polizia.org (privacy protected registration)*
- *lapoliciaespanola.org (goldenbaks@gmail.com)*

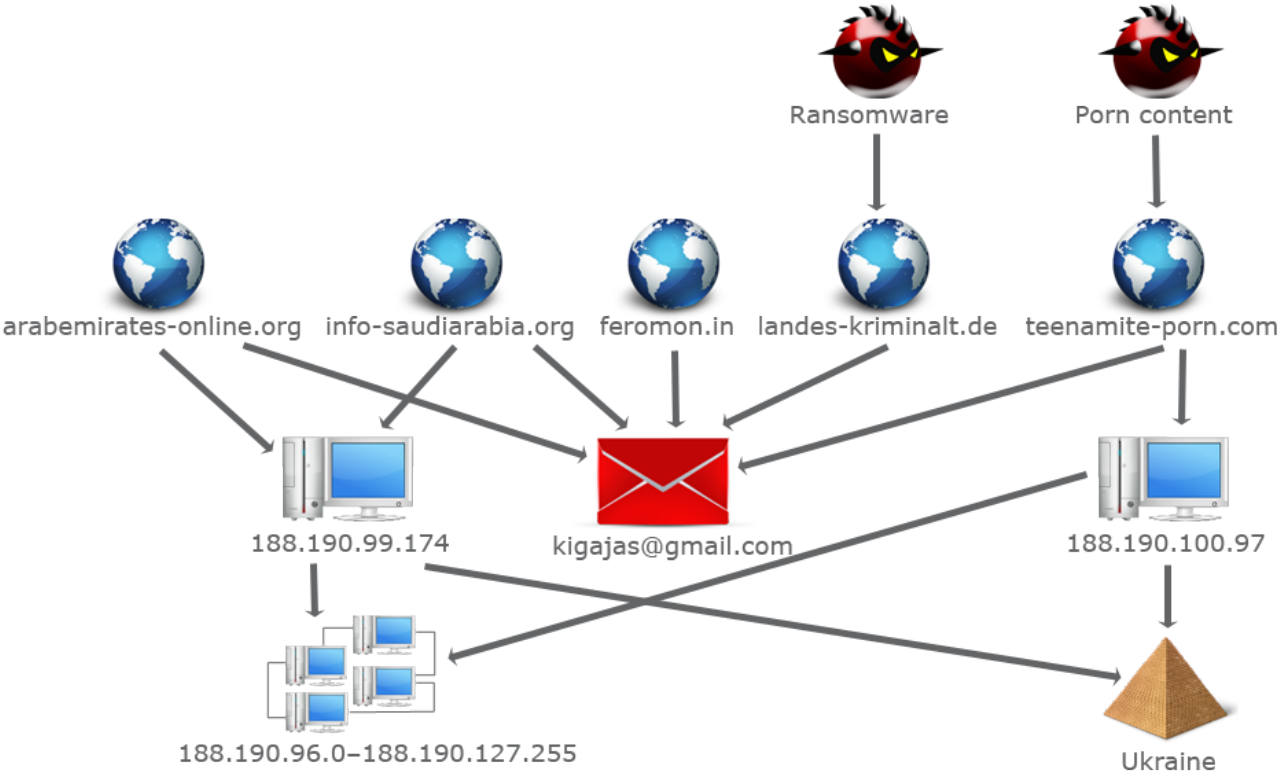
The registrant's email address—*goldenbaks@gmail.com*—has been in use for a couple of years now. It has been used to register several porn sites, among others. We were also able to connect the registrant's email address to domains that have been used in ZeuS, CARBERP, TDSS, and FAKEAV malware campaigns in 2010 and 2011. (A more detailed list of associated domain names is found in the *Appendix.)*



As of March this year, the ransomware C&C server hosted on IP address, *188.190.99.174,* is no longer active. It, however, appears that the IP address, *188.190.100.97,* hosted the same Police Trojan C&C server on March 6 of this year. Both servers—*188.190.99.174* and *188.190.100.97,* looked identical. As such, we suspect that both IP addresses belong to virtual servers hosted on the same physical server. Later on, a porn site—*teenamite-porn.com* (registered by *kigajas@gmail.com),* was temporarily hosted on the IP addresses. The email address, *kigajas@gmail.com,* was also used to register other domain names such as:

- *arabemirates-online.org (kigajas@gmail.com)*
- *info-saudiarabia.org (kigajas@gmail.com)*
- *teenamite-porn.com (kigajas@gmail.com)*
- *landes-kriminalt.de (kigajas@gmail.com)*
- *feromon.in (kigajas@gmail.com)*

Landes-kriminalt.de was used by a Police Trojan to impersonate the German National Police. We found that *arabemirates-online.org* and *info-saudiarabia.org* resolved to the same IP address—*188.190.99.174.* We began to see a relationship between the two sets of domains. Both sets shared IP addresses and hosted Police Trojan and porn domains.



In the latter part of March this year, new Police Trojans began pointing to two domains—*lertionk03.be* and *lertionk07.be.* These domains were registered by *thefirstweek@yandex.ru.* It appears that the domains *lertionk[1–20].be* all exist as well. These all have authoritative name servers, *ns1.nsserver.be* and *ns2.nsserver.be.* Looking deeper, we noticed that the name servers also had authority over the following domains:

- *lockcattrade.biz (zemcovolejjammdf@gmail.com)*
- *lertionk[01-020].be (thefirstweek@yandex.ru)*
- *zaletelly[01-020].be (thefirstweek@yandex.ru)*
- *robot[01-010].be (thefirstweek@yandex.ru)*
- *pornolabs.be (thefirstweek@yandex.ru)*
- *mekrosoft.in (alexudakovnah@gmx.de)*
- *mifkrosoft.in (alexudakovnah@gmx.de)*

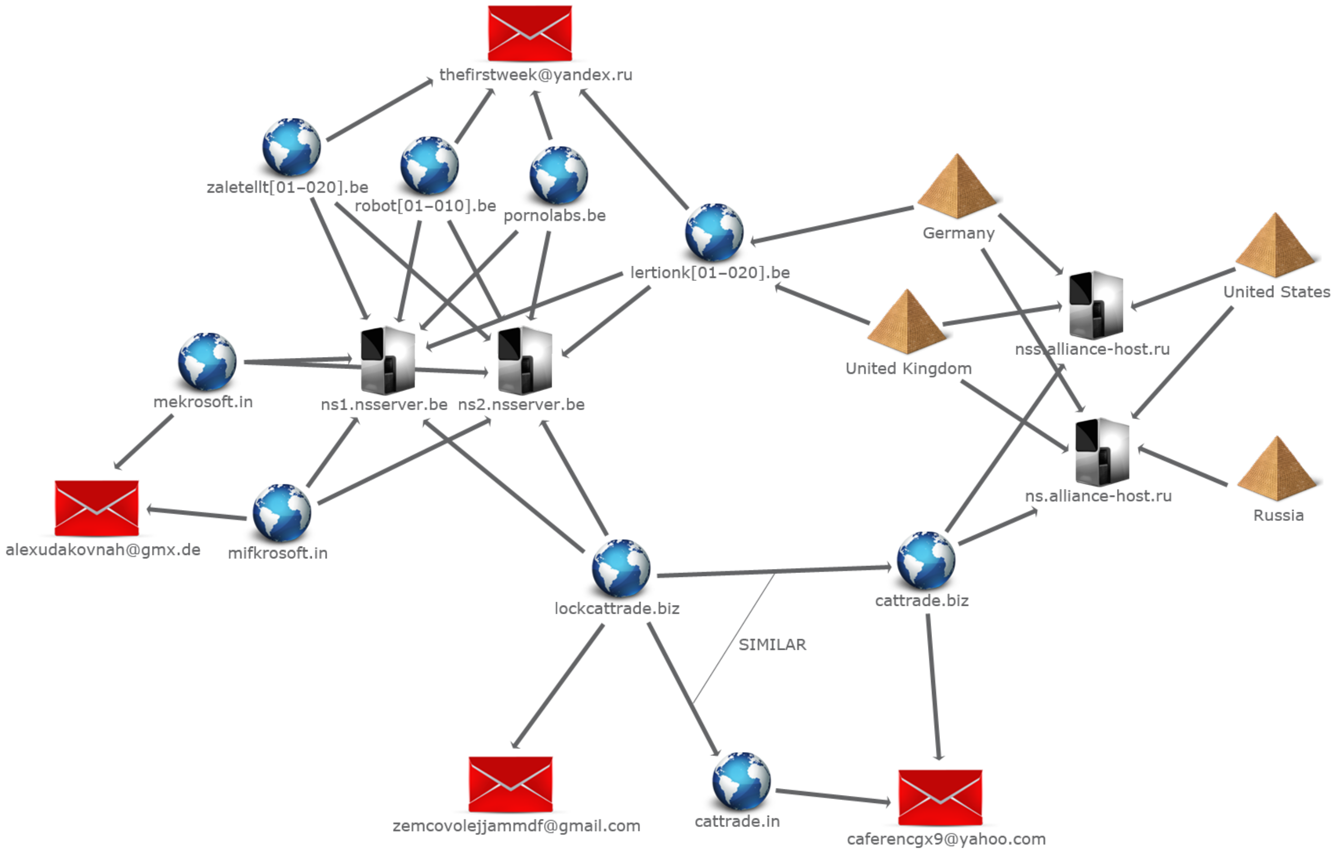
We also found that the *.be* C&C domain names moved from one IP address to another in Germany and the United Kingdom.

The domain name, *lockcattrade.biz,* can be a C&C or an affiliate domain. A similar domain—*cattrade.biz,* held the affiliate program of a ransomware Trojan just a month before.[1] This made us think that the Trojan we recently found and the one we were analyzing were related even though the affiliate program hosted on *cattrade.biz* was no longer there. After taking a look at the registration details of *cattrade.biz,* we discovered one more domain registered by the same email address— *cattrade.in (caferencgx9@yahoo.com).*

Cattrade.biz had authoritative name servers—*nss.alliance-host.ru* and *ns.alliance-host.ru. Lockcattrade.biz* can be an administrative or an affiliate program domain but this is only a wild guess based on its name. It is related to the other domains in *name server ns{1, 2}.nssserver.be.*

Alliance-host.ru turned out to be a shady bulletproof web-hosting reseller in Russia. According to its website, it is “a guaranteed bulletproof hosting provider.” Alliance Bulletproof Hosting claims that it has servers in the United States, the United Kingdom, Germany, and the Ukraine. It just so happened that the C&C servers we looked at sat in Germany, the United Kingdom, the Ukraine, and the United States. Was it a coincidence? We do not think so. The company does not have an address, a phone number, or any regular kind of business data as well. All it had was an *ICQ* or *Jabber* address for contact details. It was very likely the provider in charge of the Police Trojan’s network infrastructure and moving the C&C servers around.

[1] http://xylibox.blogspot.com/2012/02/cattrade-ransomware-affiliate.html


thefirstweek@yandex.ru
zaletellt[01–020].be
robot[01–010].be
pornolabs.be
lertionk[01–020].be
Germany
United States
United Kingdom
nss.alliance-host.ru
mekrosoft.in
ns1.nsserver.be
ns2.nsserver.be
ns.alliance-host.ru
Russia
alexudakovnah@gmx.de
mifkrosoft.in
lockcattrade.biz
cattrade.biz
SIMILAR
zemcovolejjammdf@gmail.com
cattrade.in
caferencgx9@yahoo.com

CONNECTIONS TO OTHER MALWARE CAMPAIGNS

The gang spreading the ransomware discussed in this research paper does not seem to be a novice in committing cybercrime. In fact, we can relate the ransomware Trojan to several data-stealing campaigns involving ZeuS and CARBERP Trojans, TDSS rootkits, and FAKEAV malware dating back to 2010 and 2011. We can also relate the Police Trojan gang to a ZeuS Trojan campaign launched in mid-March of this year and a Gamarue worm.

Earlier, we showed the registrant, *goldenbaks@gmail.com,* register several Police Trojan domain names. This registrant has been active since 2010 and owns domain names that have been used for ZeuS, CARBERP, TDSS, and FAKEAV campaigns.

Domain	Campaign
fastsearchportal.org	CARBERP
traffogon.net	CARBERP
kukushata.com	ZeuS
fastprosearch.com	FAKEAV
kigatropol.com	Blackhole Exploit
dscodec.com	TDSS

Table 1. Domains used in various malware campaigns in 2010 and 2011

MD5 Hash	Campaign
e7cf4d8e210cafcb5b45c92f9e0a547f	CARBERP
35b622c56a6958ec552f78f1e11e1aa9	CARBERP
3dd1b084a3994a6269a99427d1bca796	ZeuS
ce4fddb8d2cabd90e8f6871d392b7aae	FAKEAV
4bcb8136ba416358ff3e01d607594de7	FAKEAV
3ec7361806c77126e432f35459a11e6f	TDSS
6dd5fdcfed4af796e07e18bef163c7e2	TDSS
b0d5ef00e7aebdb67b22718b2ce418a3	TDSS
cad50f33fc6e375e003cf7ba50d0b3b9	TDSS
dae428ab8b10da86cfb231d2cc4de76c	TDSS
ce4fddb8d2cabd90e8f6871d392b7aae	FAKEAV
be07e8f685e6303837d48c54c16ed760	Chyup
f41dff5982f29a44c3ad234c7a483b4d	TDSS

Table 2: MD5 hashes of some malware samples that had ties to the Police Trojan gang

Closer analysis of the TDSS samples showed that these were the same samples from Estonian cybercrime gang—Rove Digital's Nelicash affiliate program. Rove Digital was taken down on November 8, 2011 by the Federal Bureau of Investigation (FBI), the National Aeronautics and Space Administration (NASA)'s Office of the Inspector General, and the Estonian Police Force in collaboration with Trend Micro and other security industry partners.[2] Rove Digital was responsible for spreading Domain Name System (DNS) changer Trojans on a large scale.

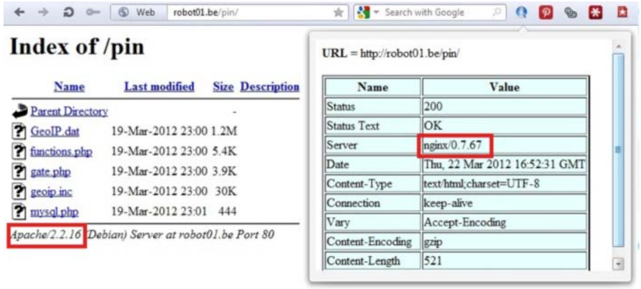
The TDSS samples we have seen in Police Trojan attacks were also the DNS changers Rove Digital's affiliate program used. As such, we believe that one or some of the gang members spreading the Police Trojans may also have been members of Rove Digital's affiliate program in the past. This shows that the gang is certainly not new to cybercrime.

At present, the gang also actively spreads variants of the Gamarue worm, some of which drop Police Trojans. Also, just this March, we saw a ZeuS Trojan connect to a Police Trojan C&C server, *blackbluerose.com,* which has ties to authoritative name servers, *ns{3,4}.nsserver.be. Nsserver.be* was also registered by *thefirstweek@yandex.ru,* the same registrant of several *.be* Police Trojan and Gamarue worm C&C domains.

[2] http://blog.trendmicro.com/esthost-taken-down-biggest-cybercriminal-takedown-in-history/

POSSIBLE INFECTION STARTING POINT

Looking at one of the Police Trojan C&C servers, we noticed that the attackers always used the *nginx* HTTP server. When we probed a little deeper though, we saw that the content server that actually serves the files was not the *nginx* but an *Apache* server. Actually, the C&C boxes have *nginx* listening on port 80 and the *Apache* server on port 81. Redirection seems to be taking place from one port to the other for an unknown purpose though a valid theory is that the front-end *nginx* server may be proxying the incoming client requests to the real back-end server located somewhere else.



```
Index of /pin

      Name              Last modified      Size  Description
-------------------------------------------------------------
   Parent Directory                          -
   GeoIP.dat          19-Mar-2012 23:00  1.2M
   functions.php      19-Mar-2012 23:00  5.4K
   gate.php           19-Mar-2012 23:00  3.9K
   geoip.inc          19-Mar-2012 23:00   30K
   mysql.php          19-Mar-2012 23:01   444
-------------------------------------------------------------
Apache/2.2.16 (Debian) Server at robot01.be Port 80
```

URL = http://robot01.be/pin/

Name	Value
Status	200
Status Text	OK
Server	nginx/0.7.67
Date	Thu, 22 Mar 2012 16:52:31 GMT
Content-Type	text/html;charset=UTF-8
Connection	keep-alive
Vary	Accept-Encoding
Content-Encoding	gzip
Content-Length	521

We have not found a definite infection chain for the Police Trojan yet. One remarkable link to a proxy network of Blackhole exploits—domain name, *kigatropol.com,* however, has the same registrant email address, *lapoliciaespanola.org (goldenbaks@gmail.com).* This was hosted on *199.15.236.24* (now clean) at the end of January. At that time, *199.15.236.24* was part of a proxy network that hosted a *Blackhole Exploit* pack. This network had IP addresses that looked nearly identical. These may all be related to the same backend server or were spawned by the same base virtual image.

We suspect that this is one of the affiliate networks the ransomware Trojan directed potential victims to.

CONCLUSION

We suspect that we are facing a Russian-speaking gang (possibly from Russia or the Ukraine) that operates the whole ransomware campaign. They seem to be using Alliance Bulletproof Hosting via a network of separate C&C servers in the United States, the United Kingdom, Germany, and the Ukraine. These could alternatively be C&C nodes that proxy requests to a central C&C server.

The Russian-speaking cybercriminals responsible for the ransomware Trojan seem to have been involved in several malware campaigns in the past. They used CARBERP, ZeuS, and FAKEAV Trojans as well as dangerous TDSS rootkits so they are not new to the malware scene. The TDSS Trojans appeared to be part of Rove Digital's affiliate program, Nelicash. As such, we suspect that the bad actors were previous Rove Digital affiliates.

The bad actors also owned numerous porn domains that may have been used to infect victims' systems. They used to run an affiliate *partnërka* site—*cattrade.biz,* that, at some point, made the jump to distributing ransomware. The affiliates that spread this ransomware seem to be primarily in the porn business.

Users' systems were infected after visiting an affiliate's porn page. The Trojan suggests that they have been watching objectionable content (which was probably true) and so are being required by the police to pay a fine. The porn site's webmaster gets a cut from the amount the victim pays. Based on this, porn sites are the most likely candidates as affiliates.

Even though porn seems to be the main link in this campaign, we saw other kinds of sites spread the Trojan as well. As such, the affiliates of this partnërka also utilize different ways to infect users' systems. The recent infection of the site, *laduree.fr,* shows how the attackers also compromise sites to peddle the Police Trojan.[3]

[3] http://blog.trendmicro.com/compromised-website-for-luxury-cakes-and-pastries-spreads-ransomware/

In sum, we are looking at a Russian-speaking cybercriminal gang with a dynamic network infrastructure that probably uses an affiliate network to help spread the ransomware Trojan and infect as many people's systems as possible.

APPENDIX

Associated Email Addresses

- *alexudakovnah@gmx.de*
- *caferencgx9@yahoo.com*
- *goldenbaks@gmail.com*
- *kigajas@gmail.com*
- *thefirstweek@yandex.ru.*
- *zemcovolejjammdf@gmail.com*

C&C Servers

- As of March 8, 2012:
  - *46.37.180.92*
  - *176.9.137.119*
  - *188.190.100.97*
- As of March 15, 2012:
  - *176.9.139.166*

Other IP Addresses

- *31.193.14.220* (name server)
- *31.193.14.221* (name server)
- *31.193.14.222* (name server)
- *31.193.14.223* (name server)
- *64.120.190.166 (lockcattrade.biz)*
- *78.47.116.212 (lockcattrade.biz)*
- *124.109.1.165 (blackbluerose.com - lotentake.net)*

Possibly Associated Domains

The following domains were also registered using the email address, *alexudakovnah@gmx.de:*

- *krobodoping.in*
- *poletaem001.in*
- *poletaem002.in*
- *poletaem003.in*
- *poletaem004.in*
- *poletaem005.in*
- *mekrosoft.in*
- *micolosoft.in*
- *microlsoft.in*
- *mifkrosoft.in*
- *mikosoft.in*
- *minkosoft.in*

The following domains were also registered using the email address, *caferencgx9@yahoo.com:*

- *cattrade.biz*
- *cattrade.in*

The following domains were also registered using the email address, *goldenbaks@gmail.com:*

- *apopeshko-kakashek.com*
- *besplatnoporno.org*
- *bundeskriminalamtes.org*
- *bundes-kriminalamt.net*
- *dscodec.com*
- *exchangeofchecks.com*
- *fastglobosearch.com*
- *fastprosearch.com*
- *fastsearchportal.org*
- *forbiddenexplicit.net*
- *gibridpk.com*
- *goldsexmovies.com*
- *grandporno.org*
- *gwb-cash.com*
- *inc0gnit02.com*
- *inc0gnit0.com*
- *kigatropol.com*
- *kukushata.com*
- *landes-kriminalt.net*
- *landeskriminalt.net*
- *landes-kriminalt.org*
- *lapoliciaespanola.org*
- *mega-porn0.net*
- *mpmasterporn.com*
- *myxxxhot.org*
- *nadrochi.net*
- *nitrosearch.info*
- *n-p-f.org*
- *policemetropolitan.org*
- *porno-day.net*
- *pornofromallworld.net*
- *pornopinto.com*
- *porno-pir.org*
- *pornoproriv.net*
- *privatetechnology.biz*
- *sexysheep.org*
- *sexzavod.net*
- *spacecodecpack.net*
- *speedsearch4you.com*
- *speedsearch4you.in*
- *systemcodec.net*
- *systemscodec.com*
- *theworldsearch.com*
- *tourboportal.com*
- *traffcash.biz*
- *traffogon.net*
- *tubechube.org*
- *turb-o-search.com*
- *vaginagold.net*
- *vtraxe.net*
- *winhomesecurity.net*
- *nanosearchpro.net*

The following domains were also registered using the email address, *kigajas@gmail.com:*

- *arabemirates-online.org*
- *feromon.in*
- *info-saudiarabia.org*
- *landes-kriminalt.de*
- *teenamite-porn.com*

The following domain was also registered using the email address, *zemcovolejjammdf@gmail.com:*

- *lockcattrade.biz*

The following domains were also registered using the email address, *thefirstweek@yandex.ru:*

- *nsserver.be*
- *lertionk[01-020].be*
- *zaletelly[01-020].be*
- *robot[01-010].be*
- *pornolabs.be*

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014
U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

TREND MICRO™ Securing Your Journey to the Cloud