TREND MICRO | Securing Your Web World

Police RansomWare

Loucif Kharouni

Background info

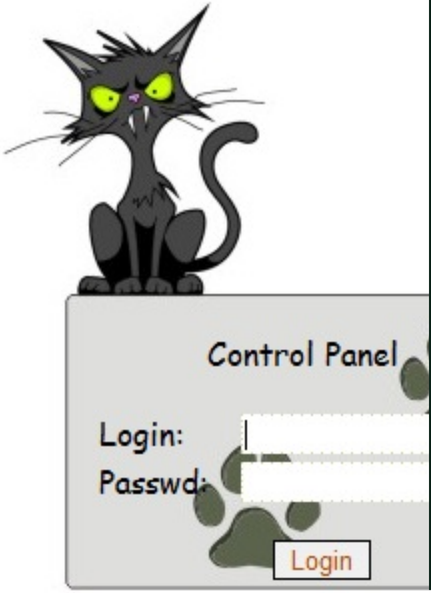
- Keep the victim’s computer hostage against ransom
- First attacks were in Russia (2005-2006)
- Check for victim’s geo-location
- Fake country police forces
- Social engineering
- Malware creators well organized
- Difficult to clean

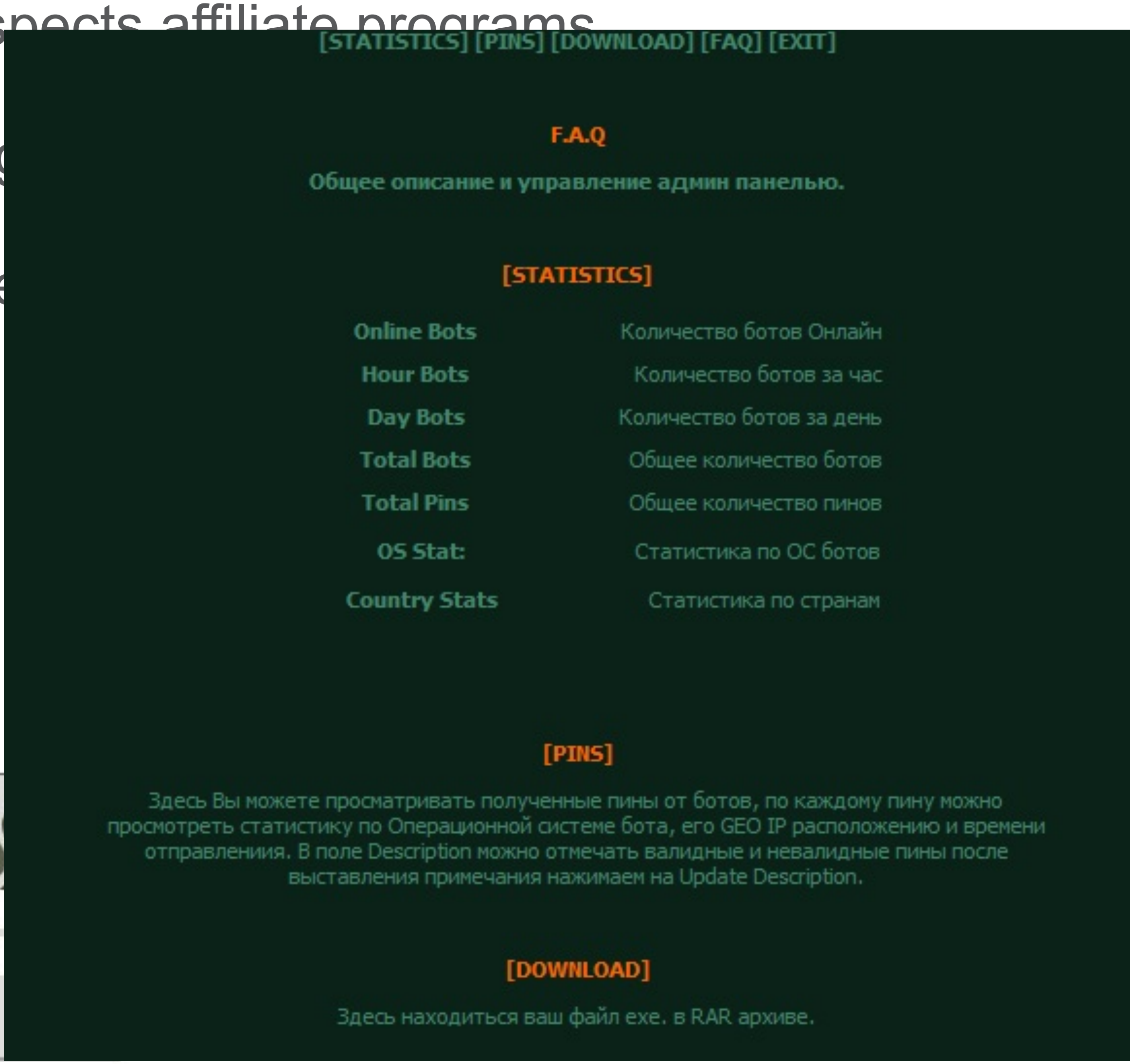
Police Trojan – What is it?

- Several groups creating their own Trojan
- Very persuasive at extracting money from victims
- New versions popping up
- Use of affiliate programs
- Drive-by-download, porn websites

Different group, same beast

- At least found 2 suspects affiliate programs
- Different groups targ
- Showing local police





F.A.Q

Общее описание и управление админ панелью.

[STATISTICS]

Online Bots	Количество ботов Онлайн
Hour Bots	Количество ботов за час
Day Bots	Количество ботов за день
Total Bots	Общее количество ботов
Total Pins	Общее количество пинов
OS Stat:	Статистика по ОС ботов
Country Stats	Статистика по странам

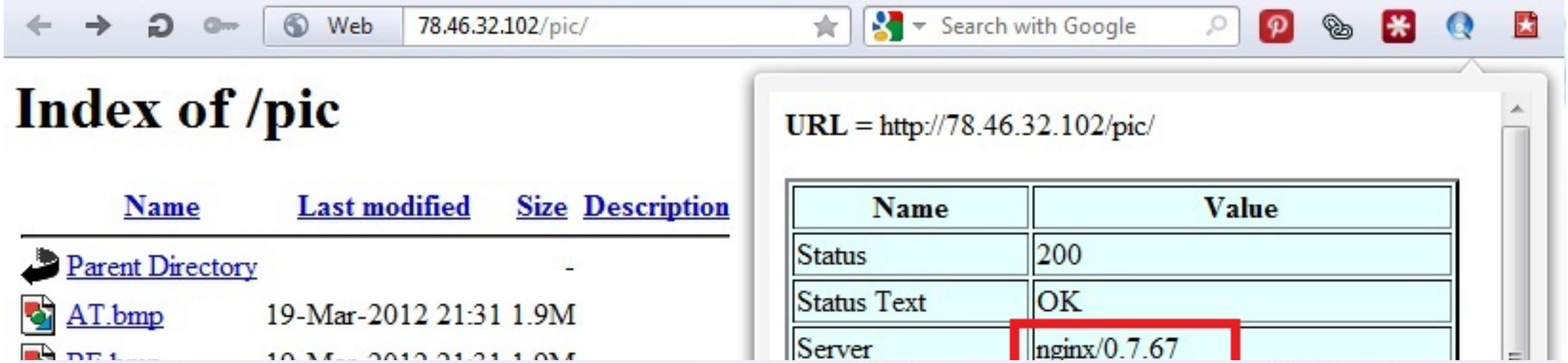
[PINS]

Здесь Вы можете просматривать полученные пины от ботов, по каждому пину можно просмотреть статистику по Операционной системе бота, его GEO IP расположению и времени отправлениия. В поле Description можно отмечать валидные и невалидные пины после выставления примечания нажимаем на Update Description.

[DOWNLOAD]

Здесь находиться ваш файл exe. в RAR архиве.

1st Group

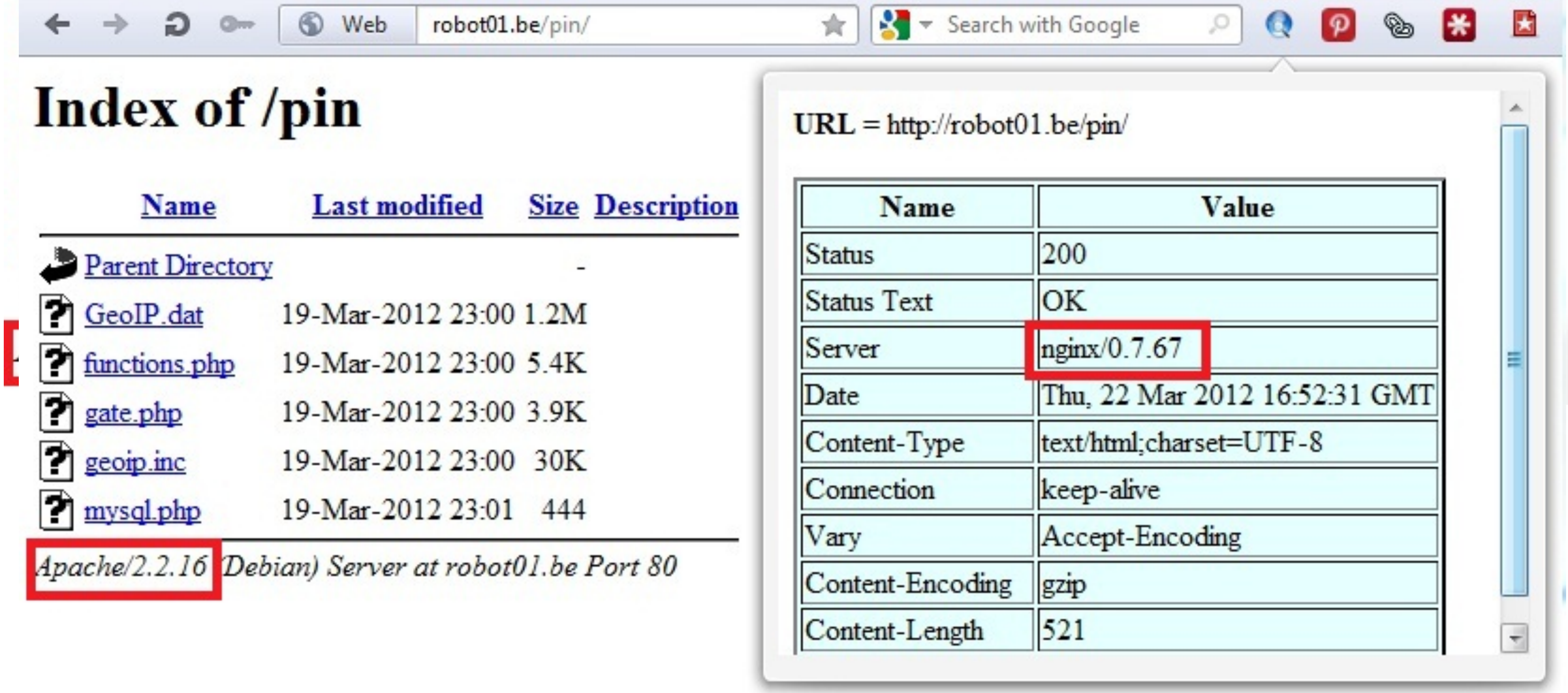


Index of /pic

Name	Last modified	Size	Description
Parent Directory		-	
AT.bmp	19-Mar-2012 21:31	1.9M	

URL = http://78.46.32.102/pic/

Name	Value
Status	200
Status Text	OK
Server	nginx/0.7.67



Index of /pin

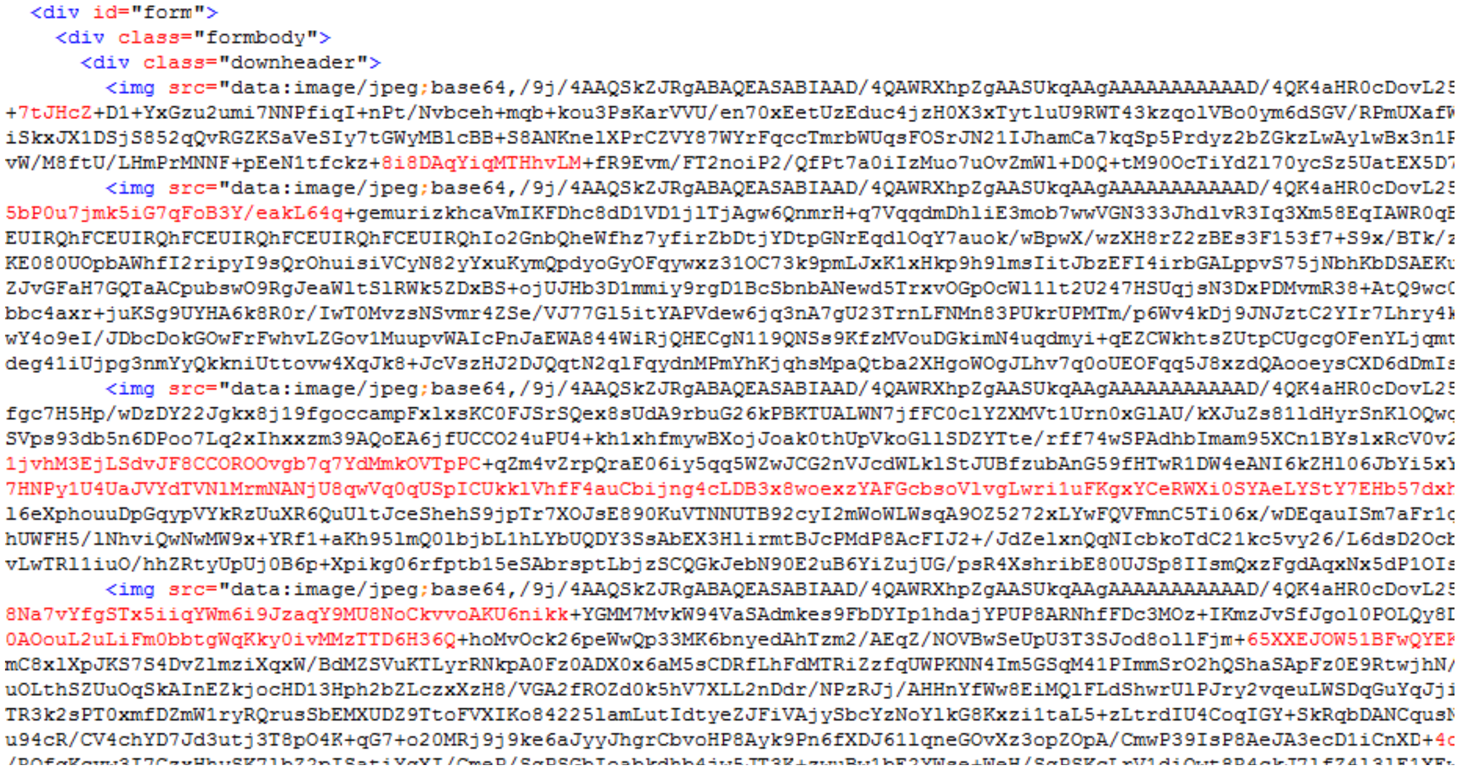
Name	Last modified	Size	Description
Parent Directory		-	
GeoIP.dat	19-Mar-2012 23:00	1.2M	
functions.php	19-Mar-2012 23:00	5.4K	
gate.php	19-Mar-2012 23:00	3.9K	
geoip.inc	19-Mar-2012 23:00	30K	
mysql.php	19-Mar-2012 23:01	444	

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

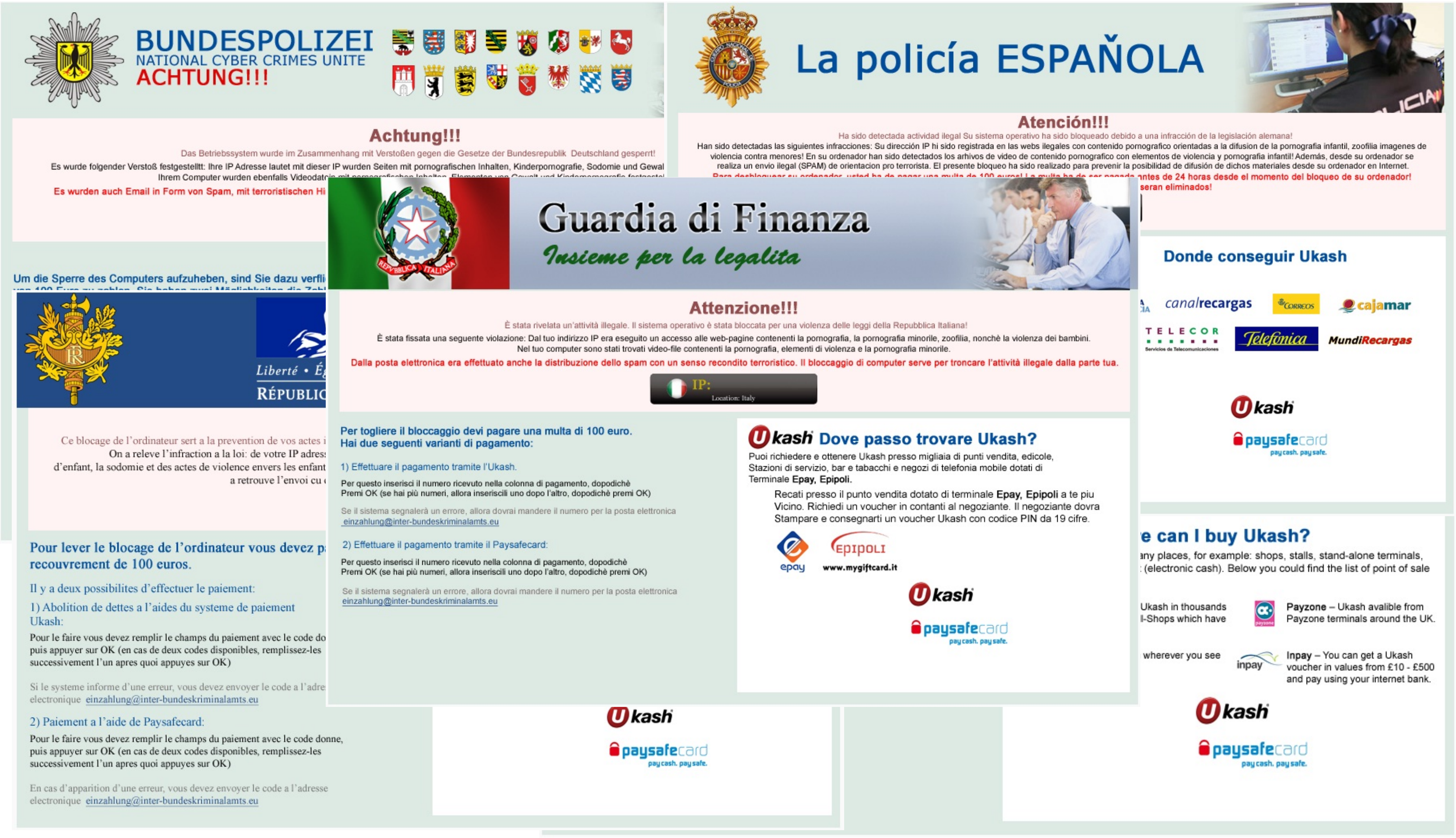
2nd group



```
    <div id="form">
      <div class="formbody">
        <div class="downheader">
          <img src="data:image/jpeg;base64,/9j/4AAQSkZJRgABAQEASABIAAD/4QAWRXhpZgAASUkqAAgAAAAAAAAAAAD/4QK4aHR0cDovL25
+7tJHcZ+D1+YxGzu2umi7NNPfiqI+nPt/Nvbceh+mqb+kou3PsKarVVU/en70xEetUzEduc4jzH0X3xTytluU9RWT43kzqolVBo0ym6dSGV/RPmUXafW
iSkxJX1DSjS852qQvRGZKSaVeSIy7tGWyMBlcBB+S8ANKnelXPrCZVY87WYrFqccTmrbWUqsFOSrJN21IJhamCa7kqSp5Prdyz2bZGkzLwAylwBx3n1F
vW/M8ftU/LHmPrMNNF+pEeN1tfckz+8i8DAqYiqMTHhvLM+fR9Evm/FT2noiP2/QfPt7a0iIzMuo7uOvZmWl+D0Q+tM90OcTiYdZl70ycSz5UatEX5D7
          <img src="data:image/jpeg;base64,/9j/4AAQSkZJRgABAQEASABIAAD/4QAWRXhpZgAASUkqAAgAAAAAAAAAAAD/4QK4aHR0cDovL25
5bP0u7jmk5iG7qFoB3Y/eakL64q+gemurizkhcaVmIKFDhc8dD1VD1jlTjAgw6QnmrH+q7VqqdmDhliE3mob7wwVGN333JhdlvR3Iq3Xm58EqIAWR0qE
EUIRQhFCEUIRQhFCEUIRQhFCEUIRQhIo2GnbQheWfhz7yfirZbDtjYDtpGNrEqdlOqY7auok/wBpwX/wzXH8rZ2zBEs3F153f7+S9x/BTk/z
KE080UOpbAWhfI2ripyI9sQrOhuisiVCyN82yYxuKymQpdyoGyOFqywxz31OC73k9pmLJxK1xHkp9h9lmsIitJbzEFI4irbGALppvS75jNbhKbDSAEKu
ZJvGFaH7GQTaACpubswO9RgJeaWltSlRWk5ZDxBS+ojUJHb3D1mmiy9rgD1BcSbnbANewd5TrxvOGpOcWl1lt2U247HSUqjsN3DxPDMvmR38+AtQ9wcC
bbc4axr+juKSg9UYHA6k8R0r/IwT0MvzsNSvmr4ZSe/VJ77Gl5itYAPVdew6jq3nA7gU23TrnLFNMn83PUkrUPMTm/p6Wv4kDj9JNJztC2YIr7Lhry4k
wY4o9eI/JDbcDokGOwFrFwhvLZGov1MuupvWAIcPnJaEWA844WiRjQHECgN119QNSs9KfzMVouDGkimN4uqdmyi+qEZCWkhtsZUtpCUgcgOFenYLjqmt
deg41iUjpg3nmYyQkkniUttovw4XqJk8+JcVszHJ2DJQqtN2qlFqydnMPmYhKjqhsMpaQtba2XHgoWOgJLhv7q0oUEOFqq5J8xzdQAooeysCXD6dDmIs
          <img src="data:image/jpeg;base64,/9j/4AAQSkZJRgABAQEASABIAAD/4QAWRXhpZgAASUkqAAgAAAAAAAAAAAD/4QK4aHR0cDovL25
fgc7H5Hp/wDzDY22Jgkx8j19fgoccampFxlxsKC0FJSrSQex8sUdA9rbuG26kPBKTUALWN7jfFC0clYZXMVt1Urn0xGlAU/kXJuZs81ldHyrSnKlOQwq
SVps93db5n6DPoo7Lq2xIhxxzm39AQoEA6jfUCCO24uPU4+kh1xhfmywBXojJoak0thUpVkoGllSDZYTte/rff74wSPAdhbImam95XCn1BYslxRcV0v2
1jvhM3EjLSdvJF8CCOROOvgb7q7YdMmkOVTpPC+qZm4vZrpQraE06iy5qq5WZwJCG2nVJcdWLklStJUBfzubAnG59fHTwR1DW4eANI6kZHl06JbYi5xY
7HNPy1U4UaJVYdTVNlMrmNANjU8qwVq0qUSpICUkklVhfF4auCbijng4cLDB3x8woexzYAFGcbsoVlvgLwri1uFKgxYCeRWXi0SYAeLYStY7EHb57dxh
l6eXphouuDpGqypVYkRzUuXR6QuUltJceShehS9jpTr7XOJsE890KuVTNNUTB92cyI2mWoWLWsqA9OZ5272xLYwFQVFmnC5Ti06x/wDEqauISm7aFr1q
hUWFH5/lNhviQwNwMW9x+YRf1+aKh95lmQ0lbjbL1hLYbUQDY3SsAbEX3HlirmtBJcPMdP8AcFIJ2+/JdZelxnQqNIcbkoTdC21kc5vy26/L6dsD2Ock
vLwTRl1iuO/hhZRtyUpUj0B6p+Xpikg06rfptb15eSAbrsptLbjzSCQGkJebN90E2uB6YiZujUG/psR4XshribE80UJSp8IIsmQxzFgdAqxNx5dP1OIs
          <img src="data:image/jpeg;base64,/9j/4AAQSkZJRgABAQEASABIAAD/4QAWRXhpZgAASUkqAAgAAAAAAAAAAAD/4QK4aHR0cDovL25
8Na7vYfgSTx5iiqYWm6i9JzaqY9MU8NoCkvvoAKU6nikk+YGMM7MvkW94VaSAdmkes9FbDYIp1hdajYPUP8ARNhfFDc3MOz+IKmzJvSfJgol0POLQy8D
0AOouL2uLiFm0bbtgWqKky0ivMMzTTD6H36Q+hoMvOck26peWwQp33MK6bnyedAhTzm2/AEqZ/NOVBwSeUpU3T3SJod8ollFjm+65XXEJOW51BFwQYEK
mC8xlXpJKS7S4DvZlmziXqxW/BdMZSVuKTLyrRNkpA0Fz0ADX0x6aM5sCDRfLhFdMTRiZzfqUWPKNN4Im5GSqM41PImmSrO2hQShaSApFz0E9RtwjhN/
uOLthSZUuOqSkAInEZkjocHD13Hph2bZLczxXzH8/VGA2fROZd0k5hV7XLL2nDdr/NPzRJj/AHHnYfWw8EiMQlFLdShwrUlPJry2vqeuLWSDqGuYqJji
TR3k2sPT0xmfDZmW1ryRQrusSbEMXUDZ9TtoFVXIKo84225lamLutIdtyeZJFiVAjySbcYzNoYlkG8Kxzi1taL5+zLtrdIU4CoqIGY+SkRqbDANCqusN
u94cR/CV4chYD7Jd3utj3T8pO4K+qG7+o20MRj9j9ke6aJyyJhgrCbvoHP8Ayk9Pn6fXDJ61lqneGOvXz3opZOpA/CmwP39IsP8AeJA3ecD1iCnXD+4c
```

Government of Canada
Gouvernement du Canada
Canada
Canadian Security Intelligence Service
Service canadien du renseignement de sécurité
Canadian Security Intelligence Service
www.csis.gc.ca

Other examples



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 festgestelltt: Ihre IP Adresse lautet mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornografie, Sodomie und Gewal

Ihrem Computer wurden ebenfalls Videodate

Es wurden auch Email in Form von Spam, mit terroristischen Hi

Um die Sperre des Computers aufzuheben, sind Sie dazu verfli

La policía ESPAÑOLA

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.

antes de 24 horas desde el momento del bloqueo de su ordenador!

seran eliminados!

Donde conseguir Ukash

Liberté • É

RÉPUBLIC

Ce blocage de l'ordinateur sert a la prevention de vos actes i

On a releve l'infraction a la loi: de votre IP adres

d'enfant, la sodomie et des actes de violence envers les enfant

a retrouve l'envoi cu

Pour lever le blocage de l'ordinateur vous devez p 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 do 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'adre 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

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, dopodichè
Premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodichè 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, dopodichè
Premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodichè 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.

e can I buy Ukash?

any places, for example: shops, stalls, stand-alone terminals, (electronic cash). Below you could find the list of point of sale

Ukash in thousands l-Shops which have

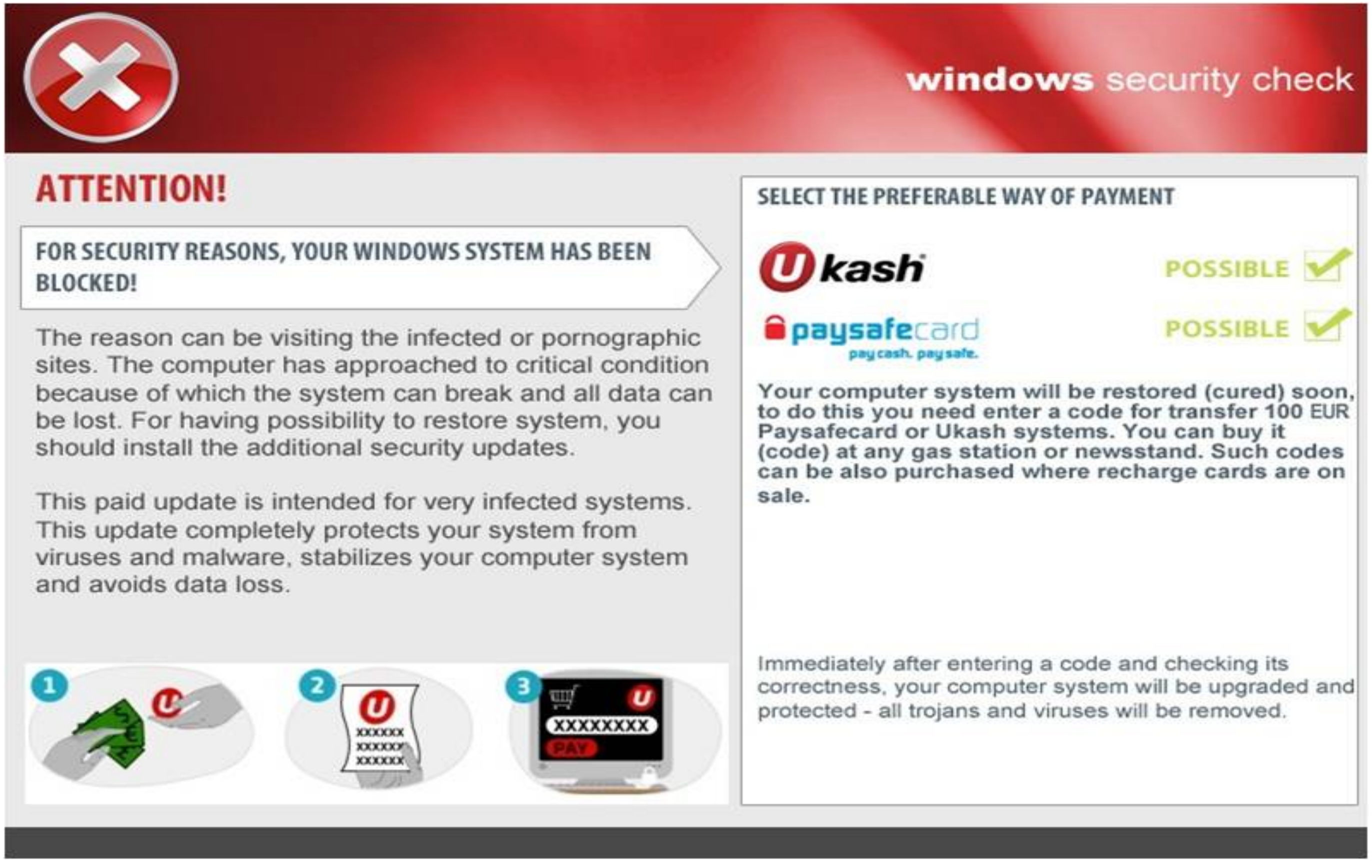
wherever you see

Payzone – Ukash avalible from Payzone terminals around the UK.

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

FAKEAV?

- Security Tool notifications, if country can’t be determined
- Similar to standard FAKEAV attacks



windows security check

ATTENTION!

FOR SECURITY REASONS, YOUR WINDOWS SYSTEM HAS BEEN BLOCKED!

The reason can be visiting the infected or pornographic sites. The computer has approached to critical condition because of which the system can break and all data can be lost. For having possibility to restore system, you should install the additional security updates.

This paid update is intended for very infected systems. This update completely protects your system from viruses and malware, stabilizes your computer system and avoids data loss.

SELECT THE PREFERABLE WAY OF PAYMENT

Ukash POSSIBLE ✓

paysafecard pay cash. pay safe. POSSIBLE ✓

Your computer system will be restored (cured) soon, to do this you need enter a code for transfer 100 EUR Paysafecard or Ukash systems. You can buy it (code) at any gas station or newsstand. Such codes can be also purchased where recharge cards are on sale.

Immediately after entering a code and checking its correctness, your computer system will be upgraded and protected - all trojans and viruses will be removed.

How do they retrieve the money

- New payment method
- Used vouchers instead of credit card payments
- 2 kind of vouchers accepted, PaySafeCard/Ukash
- Online, gas station, kiosks, pharmacy through Europe
- Available in the US and Canada
- No record if voucher change hands
- It can be sold and re-sold, until someone spend it

Underground Voucher Exchange

- Use of v

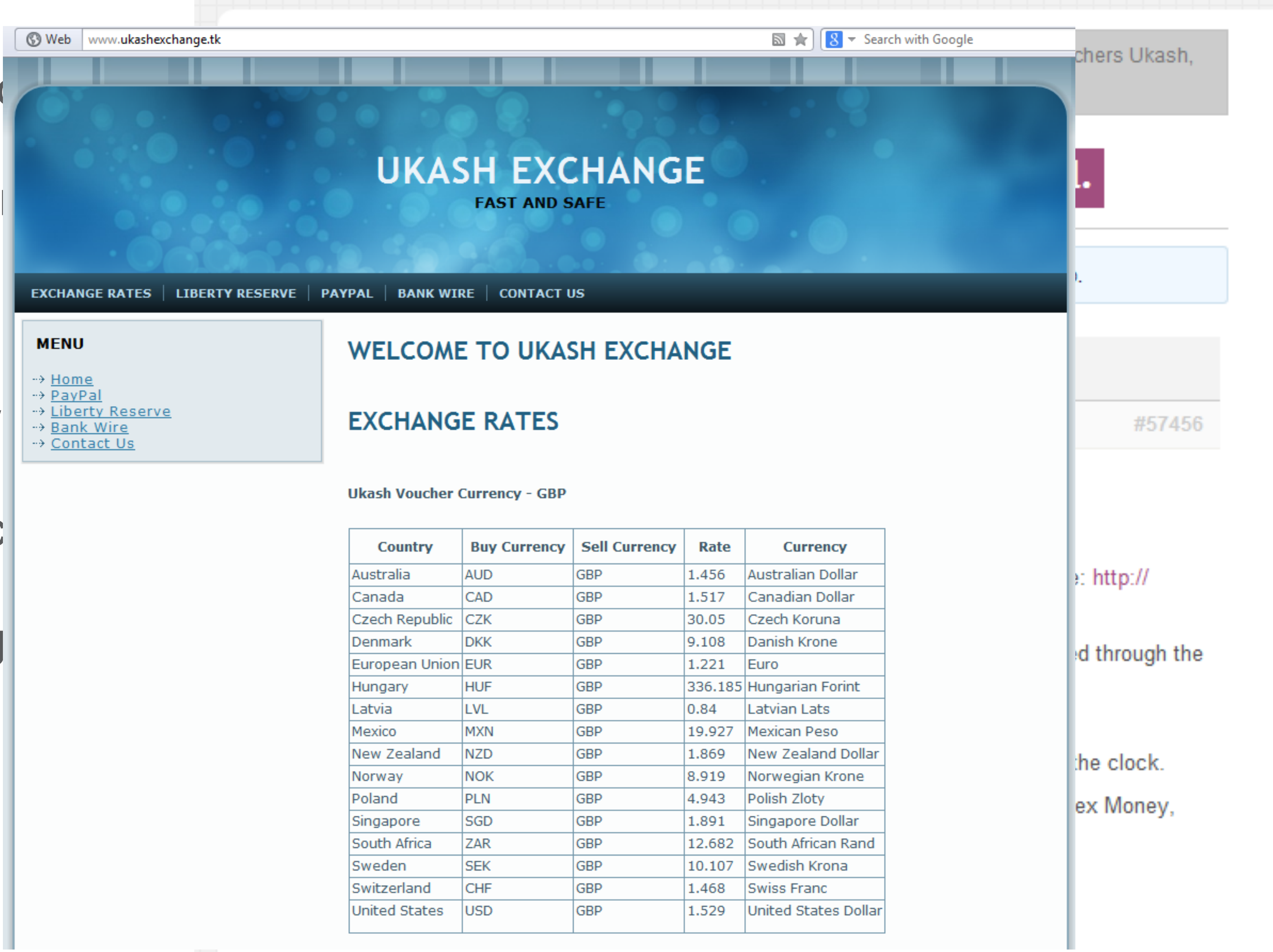
- Cybercri

  its value

- These w

  an end c

- Exchang



UKASH EXCHANGE

FAST AND SAFE

EXCHANGE RATES | LIBERTY RESERVE | PAYPAL | BANK WIRE | CONTACT US
MENU
Home
PayPal
Liberty Reserve
Bank Wire
Contact Us

WELCOME TO UKASH EXCHANGE

EXCHANGE RATES

Ukash Voucher Currency - GBP

Country	Buy Currency	Sell Currency	Rate	Currency
Australia	AUD	GBP	1.456	Australian Dollar
Canada	CAD	GBP	1.517	Canadian Dollar
Czech Republic	CZK	GBP	30.05	Czech Koruna
Denmark	DKK	GBP	9.108	Danish Krone
European Union	EUR	GBP	1.221	Euro
Hungary	HUF	GBP	336.185	Hungarian Forint
Latvia	LVL	GBP	0.84	Latvian Lats
Mexico	MXN	GBP	19.927	Mexican Peso
New Zealand	NZD	GBP	1.869	New Zealand Dollar
Norway	NOK	GBP	8.919	Norwegian Krone
Poland	PLN	GBP	4.943	Polish Zloty
Singapore	SGD	GBP	1.891	Singapore Dollar
South Africa	ZAR	GBP	12.682	South African Rand
Sweden	SEK	GBP	10.107	Swedish Krona
Switzerland	CHF	GBP	1.468	Swiss Franc
United States	USD	GBP	1.529	United States Dollar

Summary

- Threat landscape change
- Several cybercriminal groups
- Business model improved
- Vouchers are now used