

Demystifying Pobelka

A technical intelligence report on the Pobelka botnet operation. January 11, 2013

This technical report describes the Pobelka botnet and puts it in the context of global malware operations. Fox-IT's InTELL unit provides reports like this on a continuous basis to customers in the financial sector so they know who's targeting their online banking systems and can prepare countermeasures. This report is classified as public.

Key takeaways of the report are:

- The initial Dutch report on Pobelka by Surfright and Digital Investigation presents a good view on the Pobelka botnet. The report you are reading contains additional technical details on the botnet and answers some of the questions left by the original report.
- This report provides a broader context in the ecosystem of botnets, Trojans, exploit kits, and the markets where infected computers are traded.
- This report details the identity of the people running the Pobelka botnet as well as a description of the origin of the botnet and the common methods of communication used.
- The Pobelka botnet is one of many botnets active in the Netherlands. Unfortunately it's not an exceptionally large or influential botnet but rather an average sized one.
- The Pobelka botnet is just one of the many examples of how a single individual was able to attack Internet users for over a year without much resistance. This is a global issue.
- The ease at which cybercrime services are available to criminals, makes it trivial for anyone to start in this business. The potential gains for the criminals are large, with little to no chance of successful prosecution.

The author of the report is Michael Sandee, Principal Security Analyst at Fox-IT and the Fox-IT InTELL team.

The intended audience for this report is technically savvy and familiar with botnet analysis and online banking security.

for a more secure society



Introduction

Right before Christmas 2012 Surfright and Digital Investigation published their research on Pobelka¹, a Citadel Trojan powered operation which was uncovered to be active during a large period of 2012, targeting Dutch and German Internet users. It includes a detailed analysis on the composition of the Citadel backend server, such as the origin of the infected systems.

In the aforementioned report it is stated that the primary purpose of the Pobelka botnet was to harvest sensitive information. This information entails details of internal networks and login data. The results of these reconnaissance steps could then allegedly be sold off to actors involved in state sponsored espionage. We are pretty sure that the attackers actually have no direct interest in the type of information as suggested. It is however interesting to look at the amount and type of data stolen by Trojans such as Citadel.

We should note that this Pobelka botnet is by far not the biggest botnet in The Netherlands that is harvesting information. Unfortunately there are also many similarly sized botnets such as the one named Pobelka.

The reason why Citadel is called a banking Trojan is because of its main purpose, the manipulation of online banking sessions to assist in making fraudulent transactions. All activity we see from Citadel is typically geared towards financial fraud, either through manipulation of online bank accounts or stealing of creditcards. Pobelka was definitely not different in that from other campaigns.

An indication of the fraud focus of Citadel based attacks is the relation of changes in the attack code and infection campaigns, in case an attack is in a non-working state, the attacker will not invest in large infection campaigns, this relation makes it clear that the focus is only on the fraud part.

Nonetheless the stolen information is often used in other ways, such as the usage of scraped and grabbed email addresses for the purpose of spamming. Additionally the most common usage of stolen data is abusing the stolen account information such as FTP and SSH account data, which is used to login to the relevant systems and modify any web content found to redirect visitors of the related website to the exploit kit of the attacker.

Another way stolen data gets used is for scraping credit card track data. This is usually performed at the point-of-sale (POS) systems in retail stores. These systems run Windows and are thus susceptible to infection. Card readers of POS systems function as a regular keyboard. Thus the built-in keylogger of Citadel registers swiped credit cards just as well.

Citadel in this case is only a tool, and since the standardization of the ZeuS webinjects format it actually means that criminals can freely switch between Trojans that support the webinjects format. Apart from the variants of ZeuS such as Ice-IX and Citadel, also for example Carberp, SpyEye, Hermes, Gozi and Bugat are alternatives attackers can utilize. In the case of Pobelka, the Trojan of choice prior to Citadel was SpyEye, which was ran by the same attacker in the second half of 2011 till February 2012, partially overlapping the start of the Citadel Pobelka setup. In this article we will dive deeper into the attack codes used and the relation to the attacker.

¹ <http://www.surfright.nl/en/hitmanpro/pobelka>



Bentpanel

While the aforementioned SpyEye and Citadel instances also used different attack codes against banks, the majority of the attacks used an attack we named “Bentpanel”. This was purely named based on the path used by the first related attack detected in The Netherlands in August 2011. There were however other botnets over time which used the same attack with paths such as “/panel/”, “/duespanel/” and “/controlpanel/”. Additionally the same attack infrastructure also was used to host attacks against banks in other countries and appeared to have attacked numerous US banks in the beginning of 2011 and also a series of online banks in Europe in the 2nd half of 2011 and during the course of 2012. The domains used to communicate to the Bentpanel fraud backend over time, related to this specific Pobelka attack, are listed below, including which Trojan configuration they were part of.

```
hxxp://www.touchproofserv.com/bentpanel/ (August, September 2011) (SpyEye)
hxxp://www.securetechanalytics.com/bentpanel/ (September, October, November 2011) (SpyEye)
hxxp://www.securetechicsatcontrol.com/bentpanel/ (November, December 2011) (SpyEye)
hxxp://www.givecheckanon-control.net/bentpanel/ (January 2012) (SpyEye)
hxxp://www.booltingproffilinside.net/bentpanel/ (January, February, March 2012) (SpyEye, Citadel)
hxxp://www.booltithighoffilinside.net/bentpanel/ (March 2012) (Citadel)
hxxp://www.deepdarkwaters.biz/bentpanel/ (April, May 2012) (Citadel)
hxxp://waitawhile.net/bentpanel/ (May, June 2012) (Citadel)
hxxp://taleyzermi.info/bentpanel/ (June, July, August 2012) (Citadel)
hxxp://trikolorhostonliner.net/bentpanel/ (August 2012) (Citadel)
```

Note that on another vhost there was an additional path “/bentpanel/” homing to the same backend server, however it was using a different vhost and database backend and also originated from a different botnet.

The actual Bentpanel attack was offered both as a service on a hosted infrastructure, but also was separately sold as a kit which an attacker could install on his own server. The purpose of the attack is to allow account hijacking, a technique which is far from new and was used to attack banks using two factor transaction signing as far back as 2007. These attacks are also being sold as token grabbers which have additional social engineering functionality to request the two-factor transaction signing codes. While the fully automated attacks, also often named ATS, were gaining tremendous popularity in the past years, the attackers have mostly switched to utilizing the manual attacks, this is an inexpensive method for attackers to hijack accounts and allow for a lot of flexibility to insert transactions, for example executing both domestic payments and also SEPA and SWIFT international transactions without the need of updating the webinject code. Additionally in many countries banks are starting to offer services to directly purchase goods from online shops with guarantee of payment, by purchasing vouchers such as Ukash and Paysafecard the criminals are able to directly sell off the stolen goods, typically under face value. The same vouchers are also used by ransomware which has become immensely popular since the end of 2011.

Note that Bentpanel was indeed largely used to execute the manual attack as described above, but it also had ATS capabilities, the usage in the wild of this capability was however very limited according to our findings. The amount of money mules (also named drops) configured over time was very low, and we suspect only during 2 short periods it was used in The Netherlands.

Coming back to the actual Bentpanel attack, the attacker is named “Finist”, who ran both the SpyEye C&C server and also the Pobelka Citadel server. In the Bentpanel administration interface, called “Bent Admin”, we can see the jabber address of “Finist” being defined, finist-bnt (at) jabber.cz, which is a specific address he used for receiving notifications from Bentpanel. These notifications for example include the stolen login credentials the attacker can use to get access to a victim bank account.



Current time :: 04:20:45 Bank ::

[Options](#) || [User Agent](#) || [Help](#)

BotAdmin

[Netherlands](#)

[Sweden](#)

[USA](#)

DropAdmin

[Netherlands](#)

| Bot Admin | | | | |
|----------------------|---------------------------------|----------------------|---|-------------------------------------|
| Sender Pass | Sender Jid | Reciever Jid | Reciever Jid 2 | Default status |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="finist-bnt@jabber.cz"/> | <input type="text" value="0"/> |
| Drop Admin | | | | |
| Sender Pass | Sender Jid | Reciever Jid | Reciever Jid 2 | Send percent |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="90"/> |
| Common options | | | | |
| BentAdmin Pass | Display Bot Limit | | | |
| <input type="text"/> | <input type="text" value="50"/> | | | |
| SuperAdmin | | | | |
| BotAdmin | On | DropAdmin | On | <input type="button" value="save"/> |

This instance of Bentpanel also had a help page which explains the various controls and how to use the administration interface and various settings. In contrary to the administration page, the help page is mainly in Cyrillic, hinting towards the origin of the author and users of this attack code.



Statuses

0 - при логине в окне отображается процесс ожидания в течении 5ти минут
1 - запрашивается токен
2 - запрашивается токен
5 - при логине в окне отображается процесс ожидания в течении 15ти секунд
999 - блокировка доступа

если статус 0 не менять (к примеру вы не за компом) то прождав 5ть минут, бот сможет залогиниться и у него выставится статус 5

при смене со статуса с 0 на 1 запрашивается токен моментально,

если статус с 1 ни на какой не менять через 5ть минут запрашивается токен повторно

при получении токена, сменив статус с 1 на 2 моментально запрашивается токен моментально (так же при смене с 2 на 1)

если статус с 2 ни на какой не менять через 5ть минут запрашивается токен повторно

при смене статуса на 999 блокируется вход.

статус 5 ставится тем пользователям, у которых стоял статус 0 и они прождав 5 минут попали на сайт.

Options

Sender Pass - пароль жабы отправителя
Sender Jid - жаба отправителя (её нужно зарегать где угодно)
BentAdmin Pass - пароль от админки
Reciever Jid - твой жабер (жабер который будет принимать сообщения с жабера
Display Bot Limit - количество ботов отображаемых в списке ботов к каждому банку
Deafault status - статус по умолчанию (если уехал на долго лучше поставить статус 5)

Bot List

Bot Ip - IP бота
Time - Время/дата последнего захода
Status - статус бота
Query - запрос (что запрашивать у бота при статусах 1, 2)
Min value - минимальное кол-во символов запроса
Max Value - максимальное кол-во символов запроса
Reserve1 - резерв (не используется)
Reserve2 - резерв (не используется)
Comment - дополнительный комментарий (сообщение которое **будет видно боту** при статусе 999, например : "телефон суппорта +555 55555")
Color - цвет (используется для себя, чтоб проще было ориентироваться в ботах)
Own Comment - свой комментарий (используется для себя как пометки, к примеру: записывать баланс)
Action - сохранить изменения для конкретного бота

Show actions

Search Bot by Ip - поиск по спуску ботов с нужным IP
Status - поиск по спуску ботов с нужным статусом
Own Comment - поиск по спуску ботов с определённой пометкой для себя (по полю Own Comment)
кнопка Search - осуществляет поиск
Logs for bank.. - лог дублируется что было отослано в жабуер получателя

кнопка Delete Text Log - очистить текстовые логи данного банка
кнопка Delete User Agent Log - очистить лог Юзер Агента
кнопка Delete SQL Logs - очистить список ботов
кнопка Delete All Logs - очистить текстовые логи данного банка, лог Юзер Агента и список ботов.

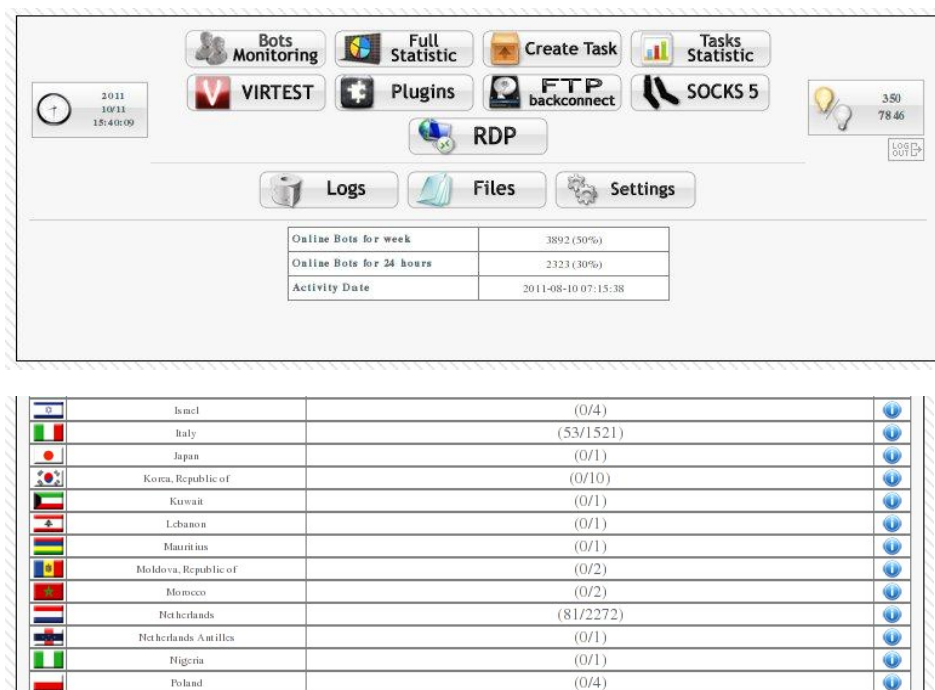
кнопка Delete Bot By Status - удалить из списка ботов тех ботов, у которых определённый статус
кнопка Delete Bot By Comment - удалить из списка ботов тех ботов, у которых определённый свой комментарий (Own Comment)

кнопка Enable/Disable Jabber - включает и выключает отсылку данного банка в жабер, при положении Off у новых ботов данного банка автоматически ставится статус 5



SpyEye

The first attacks using Bentpanel in The Netherlands originate from a SpyEye Trojan ran by the identity “Finist” as found earlier. The main SpyEye server was located at “dongdog .ru”, which had many infections from The Netherlands at the time. Note that it had numerous backup domains and new instances over time. Until October 2011 the amount of infections was relatively modest, with a little over 2000 infected systems from the Netherlands. As can be seen from the full statistic tab in the SpyEye C&C server, the first bot checked in on the 10th of August 2011, during 2 months the total amount of bots is 7846, with around 30% of the systems originating from The Netherlands.



The question as to how infections are targeted specifically at countries is easy to answer, by using the various underground services it is possible to buy infections or traffic (visitors) for a specific country or set of countries. In this specific case a traffic shop named lframeshop was used, which served as a traffic exchange platform where members could buy and sell off surplus traffic. This traffic was generated by placing a specifically crafted script which pointed to the lframeshop traffic distribution system on a website. This could be a compromised site, but also a site setup with malicious intent and pushed into high search engine ranking by the use of black SEO tricks.

During 2011 the prices of traffic originating from The Netherlands were quite high due to high demand, the cost of operating and specifically infecting systems in The Netherlands were quite high. This however did not stop Finist from continuously buying traffic.



alfa

NEWS BALANCE BUY TRAFFIC SELL TRAFFIC STATISTICS MY PROFILE EXIT

Баланс: 58.79\$

Средняя цена 1k: 6.04\$ Трафика сегодня: 262517 Трафика вчера: 442138 Доходы/Расходы

Если какого-то трафа, который Вам нужен - мало, стукните в саппорт.
Постараемся найти.

Заказать трафик +

Заказать пакет стран +

Статистика покупки трафика

| Name | URL | URL ? | Страна | Всего заказано | Цена \$/k | Всего доставлено | На сумму | Play/Pause | Delete |
|--------|-----------------------------------|-------|-------------|----------------|-----------|------------------|-----------|------------|--------|
| SE20 | http://peaceofcake.in/mai... per. | | Sweden | 20000 | 8\$ | 12701 | 101.608\$ | Pause | Delete |
| NL10 | http://peaceofcake.in/mai... per. | | Netherlands | 10000 | 18\$ | 8118 | 146.124\$ | Pause | Delete |
| Total: | | | | 30000 | | 20819 | 247.732\$ | | |

Статистика в реальном времени

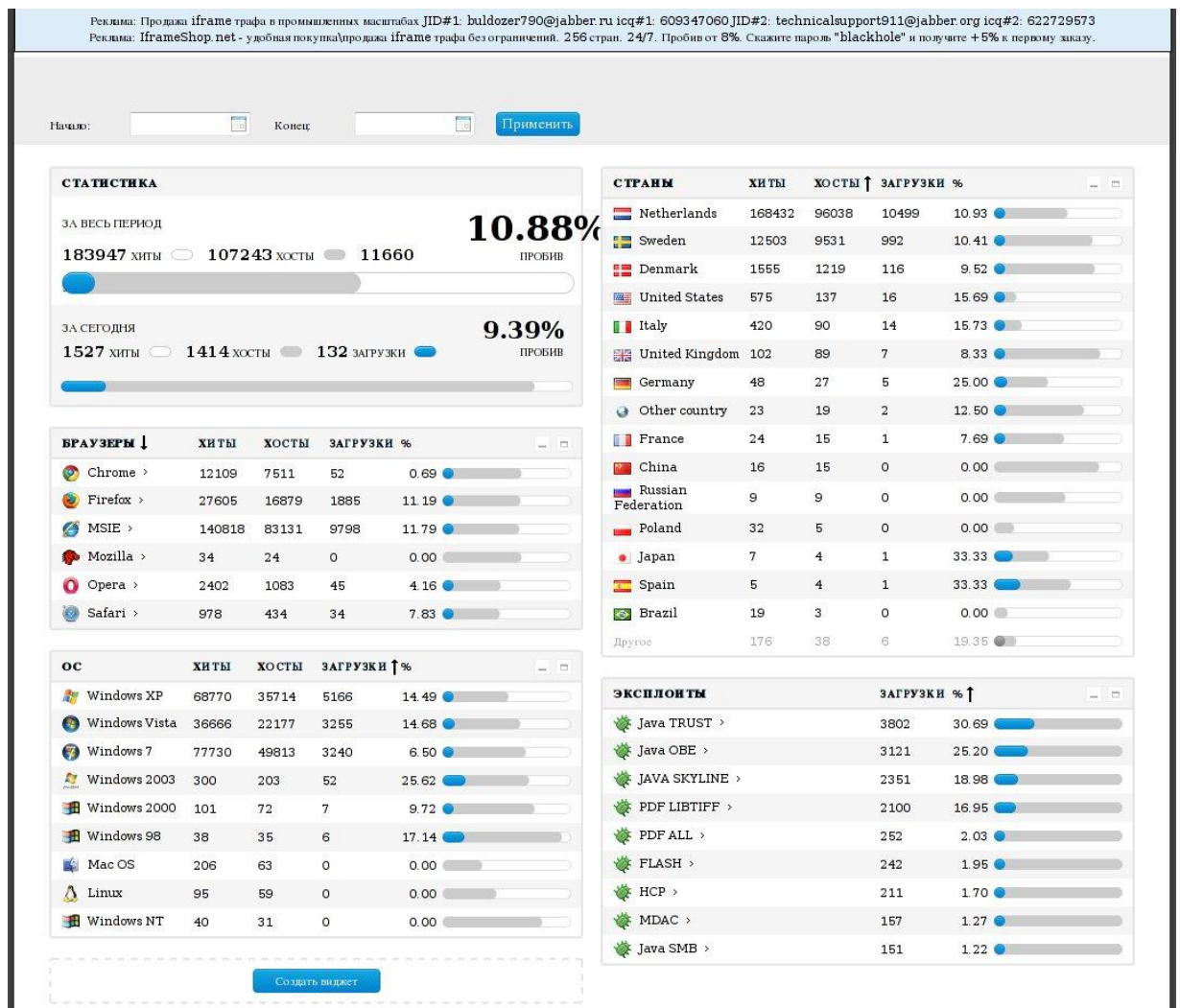
Посещения

UNDER CONSTRUCTION

Copyright © 2011 iframeshop.net
All rights reserved

Основной: 640873648 Тел.суппорт: 601822945
Jabber: iframeshop@darkdnz.net

Finist at this point bought both traffic for The Netherlands at 18USD per 1000 visitors, and Sweden at 8USD per 1000 visitors. The URL to the Blackhole exploit kit is also shown, both the Dutch and Swedish traffic was pushed to the same exploit kit. In the screenshot below you can also see that the blackhole exploit kit was actively advertising for the iframeshop service.



The exploit kit received a continuous stream of traffic and was continuously infecting systems with SpyEye. Almost 11% of all visiting systems, total based on unique IP, actually retrieved the payload executable, which amounted to well over 10.000 systems during the period shown. The SpyEye binary was also regularly updated with a recrypted version to evade detection and removal by popular anti-virus products. Finist also used the most popular service for anti-virus detection verification in the underground, scan4you, to verify both the malware executables as well as the urls and domains to exploit kits and the C&C servers he used.



**Dedicated, VPS/VDS, Shared Hosting
Domains, SSL Certificates**

**Надежные решения
от профессионалов**

**SOON FULLS, LOGINS
SMTPS, FTPS, and much more**

www.AutoCrypt.net

**DAILY PAYMENTS!
ВЫПЛАТЫ ПО ЗАПРОСУ**

LAMPEDUZA.NET

Цены вас порадуют!

**Выкупля USA TRAFF по выгодным ценам
jab: vip.person@exploit.im**

[Profile](#) [Check](#) [History of Checking](#) [Pereodica](#) [Upload funds](#) [Links](#) [Contact Us](#) [Advertisement](#) [Logout](#)

Language: RUSSIAN

Your Profile

Your Profile ID : 7579

Your Token from API : cb415fc18d72a436735c

Name : finist

Amount : 0.10\$ (add)

Contract : Per month (change)

Password : (change)

Profile info:

Your ID : 7579

Name : finist

Amount : 0.10\$ (add)

Contract : Per month (change)

Save file on server: (used for recheck)

☒ for 0 day

☐ for 1 day

☐ for 5 day

☐ for 15 day

☐ for 30 day

Clear history automatically after (after history clean you still can to see result by direct url):

☐ for 0 day

☐ for 7 day

☐ for 30 day

☒ for 3 month

☐ for 1 year

Tarificaion:

Per Month - 25\$.

Per Check - 0.15\$.

Referral - 10%

More...

Save

Disable File checking Engine

☐ adware - Ad-Aware

☐ arca - ArcaVir

☐ avast5 - Avast 5

☐ avg - AVG Free

☐ avira - AntiVir (Avira)

☐ bit - BitDefender

☐ bull - BullGuard

☐ huster - VirusBuster Internet Security

☐ clam - Clam Antivirus

☐ comodo - COMODO Internet Security

☐ drweb - Dr.Web

☐ etrust - eTrust-Vet

Disable IP/Dmain checking Engine

☐ abuseat - abuseat.org

☐ avast5 - Avast 5

☐ avg - AVG Free

☐ block - DNS Blocked Domain

☐ comodo - Comodo

☐ drweb - Dr.Web

☐ ff - Firefox Phishing and Malware

Protection

☐ google - Google Safe Browsing

☐ avant - hpHosts

☐ ie8 - IE8 Security Filter

☒ k7 - K7 Ultimate

Adult traffic USA EU

traffsa@jabbim.pl

Новое слово в КРИПТОВАНИИ

SOLLHOST ABUSE'IMMUNITY HOSTING SERVICE



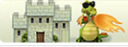
On Scan4you it is also interesting that they advertise for a large amount of underground crime services, including SollHost, which was one of the bulletproof hosting services used by Finist regularly for servers related to both malware components and the financial fraud. The financial fraud part are for example the systems used for phishing creditcards and storing stolen online banking credentials and the associated control panels to manage the money mules, typically these are systems linked to from within the Trojan configuration.

Switch to Citadel

As since October 2011 no updates were released for SpyEye and also no official support was available for the Trojan, most of the users of SpyEye started to look for alternative Trojans, which were at the time Zeus variants, but also the Trojan named Hermes became suddenly very popular. Finist however chose the Citadel Trojan which appeared in the underground in December 2011, and they had setup the Citadel C&C server in January 2012. However the SpyEye installation was still being used until February 2012. The Citadel C&C server backend, to which the domain pobelka .com pointed, was actually located in The Netherlands at the hoster named NetRouting.

Regarding the Citadel variations there were a number of campaigns, in the earlier published analysis these are described by their name: "Mandarinas", "Lime", "Mango" and "Pepper". Additionally there is one more campaign which was active in early 2012, that was "Oranges". In the Citadel control panel in the beginning of 2012, the bots originating country was actually misinterpreted, as the X-Originating-IP used to represent the bot's original IP address by the proxy, was not set correctly. The source country was thus misrepresented by the location of the proxy, which were mainly located in Eastern Europe.



**Citadel II**
Universal Spyware System

CP :: Summary statistics

Information:
Current user: [REDACTED]
GMT date: 10.02.2012
GMT time: [REDACTED]

Statistics:
Summary
OS
Botnet
Bots
Scripts

Reports:
Search in database
Search in files
Jabber notifier

System:
Information
Options
User
Users
Logout

Information
Total reports in database: 16 986 923
Time of first activity: 02.02.2012 18:48:16
Total bots: 16 862
Total active bots in 24 hours: 72.12% - 12 161
Minimal version of bot: 1.2.4.0
Maximal version of bot: 1.2.4.0

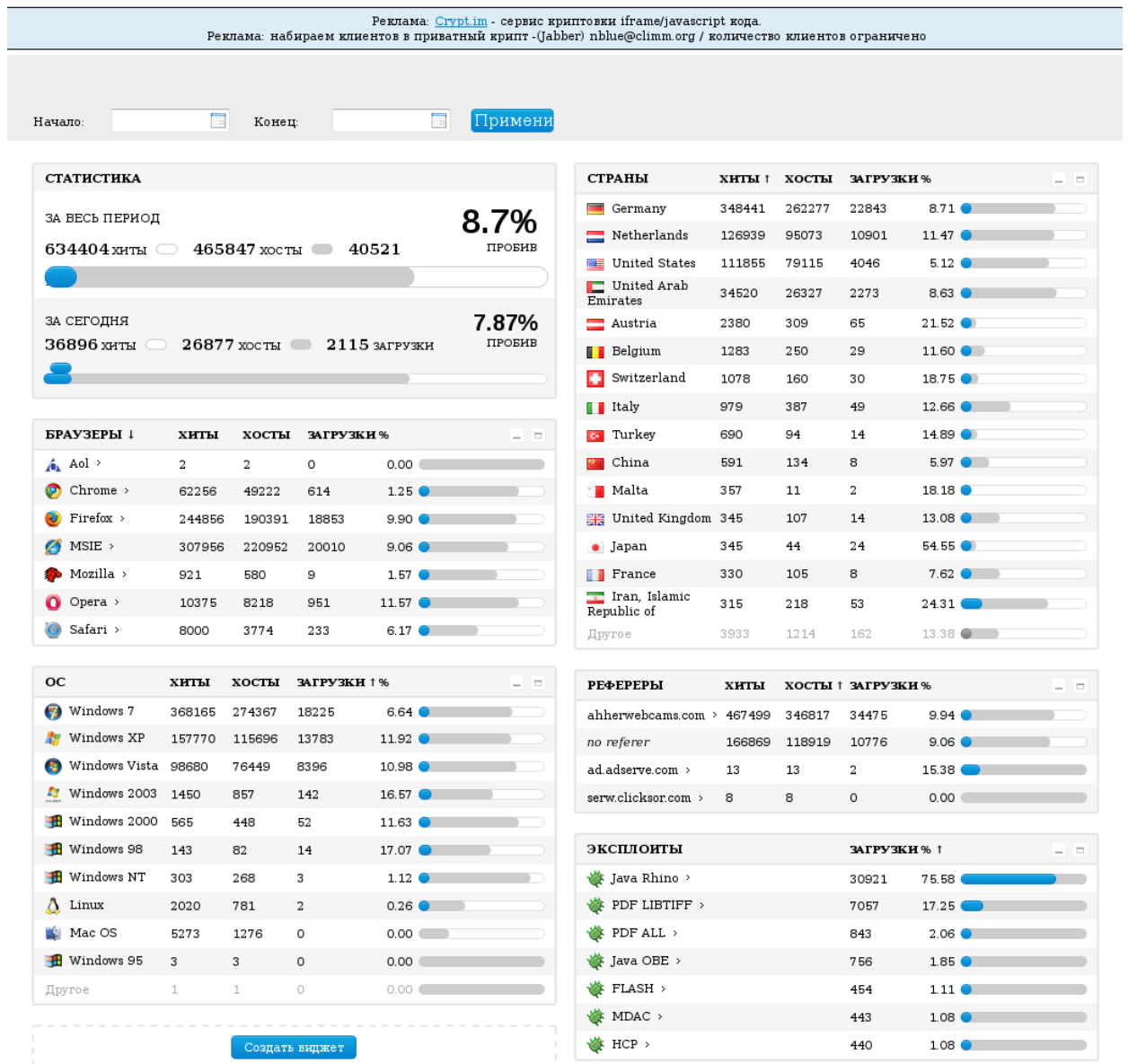
Current botnet: [All] >>
Actions: **Reset "New bots"**

New bots (16 787)

| | |
|----|-------|
| PL | 5 281 |
| .. | 2 571 |
| RU | 1 782 |
| RO | 1 551 |
| UA | 1 239 |
| IT | 869 |
| US | 768 |
| BG | 726 |
| UZ | 479 |
| GE | 437 |
| AZ | 306 |
| NL | 179 |
| LT | 171 |
| KZ | 119 |
| HU | 92 |
| DE | 56 |
| CZ | 43 |
| BA | 28 |
| MD | 22 |
| EU | 13 |
| TR | 13 |
| BY | 10 |
| MK | 10 |
| FR | 9 |
| ES | 7 |
| GB | 2 |
| LV | 2 |
| GR | 1 |
| PT | 1 |

Online bots (0)
-- Empty --

On the 10th of February the “mango” Citadel was spread via the Blackhole exploit kit using the domain “bestviagra .in”. The amount of systems during the period covered that retrieved the Citadel Trojan and was thus successfully exploited is over 40.000, of which over half originated from Germany and over a quarter originated from The Netherlands.



It is interesting to see the source of infections, apart from the typical targets Germany and The Netherlands, there is also the US (United States) and AE (United Arab Emirates), which are unusual targets for this campaign. However since this attacker or group of attackers also specialized in voucher fraud, such as the Paysafecard and Ukash vouchers, it is possible that the attacks launched against users in AE were also related to vouchers. One voucher type named CashU seems to be popular in that region. The underground shops which specialize in cashing out Paysafecard and Ukash also allow cashing out CashU vouchers, an example of such a shop is Prepaidex. Prepaidex and other similar exchange sites sell vouchers below face value, which could be used to purchase various services including for example servers and domains that could be used to host exploit kits, which are typically short lived. The vouchers

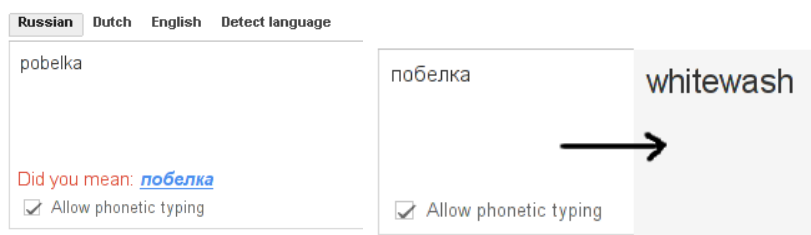


that are being sold are typically obtained using fraudulent activity such as banking malware, but also ransomware. As seen in below advertisement Prepaidex allowed selling of various vouchers in exchange for Liberty Reserve or Webmoney as online currency.



The name Pobelka

There is a little controversy regarding the name Pobelka and its meaning. The Russian word “Pobelka” actually has no meaning in Russian, both in the official language or in underground slang, regarding financial fraud. The author of the original Pobelka article appears has made creative use of Google Translate by using the phonetic typing function and choosing the suggested word in Russian language, it will be translated into the word “Whitewash” in English.



While “Whitewash” does not mean anything related to money laundering in English, literally translating it to Dutch, “Witwassen”, it does mean money laundering, however this is assumed only by accident and has no relation to the original meaning of the word Pobelka in Russian as suggested.

Infection campaigns

In the original Pobelka article a number of infection campaigns are mentioned, the campaigns are listed with the explicit note that the author does not know if they are actually related, but seemingly that the timing coincides with a peak in the number of bots checking into the Citadel C&C server. We made an analysis of the list and show which malware the various infection campaigns are related to:



The large news site Nu.nl was compromised and in the afternoon of the 14th of March 2012 it sent visitors to an exploit kit which attempted to infect the systems with smoke loader, the smoke loader in turn attempted to install Sinowal/Torpig (banking malware) on the system, we have blogged about this incident here: <http://blog.fox-it.com/2012/03/16/post-mortem-report-on-the-sinowallnu-nl-incident/>. The infection campaign involving the site deparade.nl was actually on the 18th of June 2012 and also infected systems with Sinowal/Torpig.

Visiting the site beslist.nl in the second half of August 2012 led to a Citadel malware infection which was the variant described here: <http://securityblog.s21sec.com/2012/10/sopelka-botnet-three-banking-trojans.html>.

Additionally visiting the site of Omroep West on the 16th of August 2012 led to an infection with the Hermes banking malware, the same variant which was spread by Dorifel a week earlier. In contrary to what the Pobelka article suggests, the Dorifel trojan was not spread by the Pobelka Citadel, but by a different Citadel. More on that later in this article.

The infection campaigns which did spread variants of the Pobelka Citadel were Omroep Zeeland on the 29th of March 2012, with the Lime Citadel variant with Citadel version 1.3.3.3, Weeronline.nl in the first half of June 2012 with the Lime Citadel variant with Citadel version 1.3.4.0. Additionally the Telegraaf.nl campaign was spreading several Citadel variants over time and also other not direct financial fraud related malware. The exploit kit appeared to be Redkit which skims a percentage of the infections from its members and installs pay per install malware on those, however we cannot explain why two different Citadels were spread in the same campaign, the only reasonable explanation was that it was an outsourced infection campaign.

The following C&C domains and paths are examples of actual active C&C paths in 2012 of the Pobelka Citadel.

```
hxxp://kvaskirogas .ru/lime/tuktuk.php
hxxp://lokaltriper .ru/lime/tuktuk.php
hxxp://krugvkube .ru/pepper/disney.php
hxxp://electricityrobot .ru/mango/tuktuk.php
hxxp://securenetsolutions .ru/mango/tuktuk.php
hxxp://securenetsolutions .ru/oranges/tuktuk.php
hxxp://secureserfingnet .ru/mandarinas/vrata.php
```

Dorifel connection

Based on the sudden drop in systems connecting to the C&C server of Pobelka in the days before the 9th of August 2012 and the number of systems connecting on the 9th of August 2012 as compared to the number of systems which were connecting to the Dorifel C&C server, the assumption is made that they are related. We actually wrote a blog about Dorifel here, <http://blog.fox-it.com/2012/08/09/xdccryptdorifel-document-encrypting-and-network-spreading-virus/>, on the 9th of August 2012, but Dorifel itself was spread on the 8th of August 2012 at which time the Pobelka Citadel was down according to the report, which makes it very unlikely they had any relationship. Additionally during our analysis of Dorifel we received information that the Citadel spreading Dorifel was using the following Citadel C&C:

```
hxxp://windows-update-server .com/ver/ajax.php
```

This Citadel was different from Pobelka and actually was using a backend server in Ukraine rather than The Netherlands.



Creditcard phishing

The attack using the domain `securehomserv .com` described in the original Pobelka article, is attempting to phish creditcard details using the websites Ebay, Amazon, Facebook and Paypal. The analysis mentions the domain was locked on the 17th of February 2012, however this was the day the domain was created and was actually online for a long time. This creditcard phishing attack code was active during the summer of 2012, and by the end of July 2012 it had logged 108 records with full creditcard details which could be used for CNP payments, such as renting servers or registering domains. Finist was also active on various creditcard dump sites where he used to purchase card details from other criminals to use for fraudulent purchases.

The inject code and corresponding server side panel of this creditcard phishing attack was created by someone named Symlink.

The domain `securehomserv .com` was also used on an attack on German banks in the first half of 2012 using an automated attack which listed mostly Greek SEPA mules.

| Accounts Drops Add Drop | | | | | | | |
|---|-------------------|-----|-------------------|------------------|--------------------|-------|--|
| METHOD | IBAN/accNum, NAME | | blz / SWIFT / BIC | COMMENT | LIMITS | MARKS | STATUS |
| SEPA | GR | EV | EFGBGRAA | Mieten bis 05.12 | from 4000 to 6500 | | Deactive [E] [X] |
| SEPA | GR | KYB | ABGRGRAA | Mieten bis 06.12 | from 4000 to 6500 | | Deactive [E] [X] |
| SEPA | GR | IOS | ETHNGRAA | Mieten bis 06.12 | from 4000 to 6500 | | Deactive [E] [X] |
| SEPA | HL | ZA | OTPPVHJHB | Mieten bis 06.12 | from 5000 to 10000 | | Active [E] [X] |
| Inside | 00 | Ark | 22151730 | Mieten bis 07.12 | from 5000 to 6500 | | Active [E] [X] |
| SEPA | GR | DIN | CRBAGRAA | Mieten bis 06.12 | from 4000 to 6500 | | Active [E] [X] |
| SEPA | GR | FO | ETHNGRAA | Mieten bis 06.12 | from 3000 to 6500 | | Active [E] [X] |



Finist requesting money mules

During our underground research we found references to Finist requesting money mules for usage with Dutch and German bank accounts, he requested both Dutch mules and also mules in other countries which he could transfer to from Dutch accounts. Another actor named Grom made a request on Finist behalf, because Finist was not yet a member of this forum.

10.02.2012, 20:50

Grom
Member
[Аватар для Grom](#)
Регистрация: 17.09.2010
Сообщений: 33

Выкупим ваш NL и DE траффик
" Выкупим ваш NL и DE траффик / загрузки
ICQ 900-545 ; Jabber: finist@jabber-br.org "
USA DROPS, ТАМОЖНЯ, ВАРИАНТЫ. - 174180549
! Выкупаем ваш стаф !

Later Finist himself was invited into the forum, which shows the people who vouched for Finist, and also his purpose to get into the forum, which is obtaining money mules, also known as drops, and buying traffic to redirect to his exploit kit.



| | |
|---|--|
| <p>31.05.2012, 11:47</p> <p>Support Администратор Регистрация: 21.02.2009 Сообщений: 282</p> | <p>Имя: Finist (Y)</p> <p>Регистрация проходит в соответствии с Уставом Форума и Порядком регистрации новых мемберов.</p> <p>Jabber/ICQ: finist@jabber-br.org</p> <p>1-ый поручитель: Grom (финансовое поручительство 1700) 2-ой поручитель: Marcus (финансовое поручительство 1700) 3-ий поручитель: Taleon (финансовое поручительство 1700)</p> <p>Вид деятельности: дроповодство - вещевой кардинг, скупка трафа, заливы</p> <p>Статусы на других форумах: Verified / Vendor of: drops buy traffic</p> <p>Профиль на мазе: Finist</p> |
| <p>31.05.2012, 12:30</p> <p>Marcus Banned Регистрация: 17.12.2011 Сообщений: 134</p> | <p>Подтверждаю поручительство и фин. ответственность. Знаю около 2х лет, плотно работаем год по разным темам (трафик, локер)</p> |
| <p>31.05.2012, 12:42</p> <p>Самая Крохотная Drops Service Аватар для Самая Крохотная Регистрация: 09.07.2009 Сообщений: 61</p> | <p>Finist отличается высоким профессионализмом и адекватностью, что очень ценно в наших рядах 😊 Настоятельно рекомендую к регистрации 😊</p> <p>I wanna be loved by you, just you, And nobody else but you, I wanna be loved by you, alone! Boop-boop-de-boop!</p> |
| <p>31.05.2012, 16:11</p> <p>risk25 Member Аватар для risk25 Регистрация: 13.07.2009 Сообщений: 162</p> | <p>нужный человек ЗА!</p> |
| <p>31.05.2012, 16:11</p> <p>S Модератор: Приватная информация  Регистрация: 04.07.2009 Сообщений: 105</p> | <p>Работал с ним, около 2 лет знаю, парень адекватный, всегда договаривались Голосую ЗА</p> |
| <p>31.05.2012, 21:28</p> <p>Grom Member Аватар для Grom Регистрация: 17.09.2010 Сообщений: 33</p> | <p>Да, фин ответственность, регистрируем. USA DROPS, ТАМОЖНЯ, ВАРИАНТЫ. - 174180549 ! Выкупаем ваш стаф !</p> |
| <p>02.06.2012, 15:14</p> <p>aska Banned Регистрация: 27.03.2010 Сообщений: 36</p> | <p>Адекватный, профессиональный.</p> |
| <p>04.06.2012, 23:40</p> <p>741 Member Регистрация: 06.07.2009 Сообщений: 70</p> | <p>адекватный чел, однозначно за.</p> |



Later he publicly asked for money mules several times:



Lately we have not observed any activity directly tied to Finist, however he is still active on Jabber so possibly he has found himself some new targets to attack. For well over a year however he has attacked Dutch Internet users, but with him are many others, and this problem not only exists in The Netherlands, but is active globally and is growing at an exponential rate. The ease at which cybercrime services are available to criminals, makes it trivial for anyone to start in this business, and the potential gains for the criminals are large, with little to no chance of successful prosecution. So without a doubt 2013 is going to be another year full of banking malware botnets and other nasty threats.