

# Citadel: a cyber-criminal's ultimate weapon?

---

[blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/](http://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/)

Jérôme Segura

November 5, 2012



In old times, a citadel was a fortress used as the last line of defense. For cyber criminals it is a powerful and state-of-the-art toolkit to both distribute malware and manage infected computers (bots). Citadel is an offspring of the (too) popular Zeus crimekit whose main goal is to steal banking credentials by capturing keystrokes and taking screenshots/videos of victims' computers. Citadel came out circa January 2012 in the online forums and quickly became a popular choice for criminals. A version of Citadel (1.3.4.5) was leaked in late October and although it is not the latest (1.3.5.1), it gives us a good insight into what tools the bad guys are using to make money.

In this post, I will show you how criminals operate a botnet. This is not meant as a tutorial and I do want to stress that running a botnet is illegal and could send you to jail.

## **A nice home**

In order to get into business the bad guys need a server that is hosted at a company that will turn a blind eye on their activities and also guarantee them some anonymity. Such companies are called Bulletproof hosting and can be found in most underground forums (Figure 1).

We're glad to offer you a reliable bulletproof hosting, dedicated servers and some other facilities!

We don't care about your business.  
We're specialized in providing top-quality and troubleproof service. Your success is our success as we

**Are you tired of 'worthless' services? Looking for stability and reliability to develop your business, welcome to our company.**  
You can find out turnkey solutions for spam, Zeus, SpyEye etc.

Range of our services:

**Bulletproof Hosting (Shared Hosting)**

- Control Panel – Direct Admin
- Direct data centers operation
- Your personal data anonymity
- Unlimited traffic

**Bulletproof Servers (Dedicated Servers, VPS/VDS)**

- Dedicated and virtual servers in CIS, Asia and Europe
- Personal stand lease holding in data center
- Turnkey solutions for spam, Zeus, SpyEye etc.
- Quick server setup

**Additional services**

- Stable domains
- Certificates (SSL)
- Administration facilities
- DDoS protection
- Technical issues guidance

**Forbidden content:**

- Child pornography

**Allowable content:**

- Botnets (Zeus, SpyEye, Citadel, Ice9, etc.)
- Exploits, loaders
- Drop projects
- Outcoming spam (via socks)
- Incoming spam
- Fakes
- Grey and white projects (torrents, adult, forums)

**Note: your nature of business must be accorded with support team!**

**Payments:**

- LibertyReserve
- WebMoney
- Western Union, MoneyGram (+10%)

**Contacts:**

**Server ordering, technical support:**

Figure 1: an ad for Bulletproof hosting

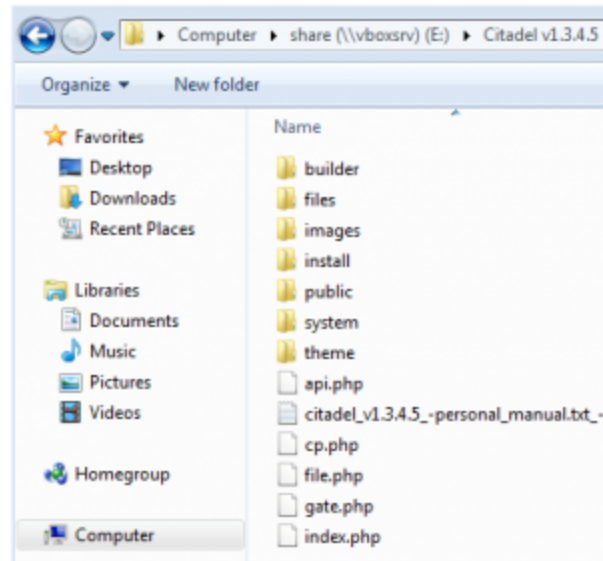
Those hosting firms are for the most part located in countries like China or Russia and therefore in their own jurisdiction where so long as you don't commit crimes against your own people not a whole lot can happen to you. To cover their tracks even more, the bad guys use proxy or VPN services that disguise their own IP address.

## A shiny new toy

Once set up with a server, it is time to install what will be the mastermind program to create and organize an entire array (botnet) of infected computers worldwide. A variety of crimekits exist but in this post we will concentrate on Citadel.

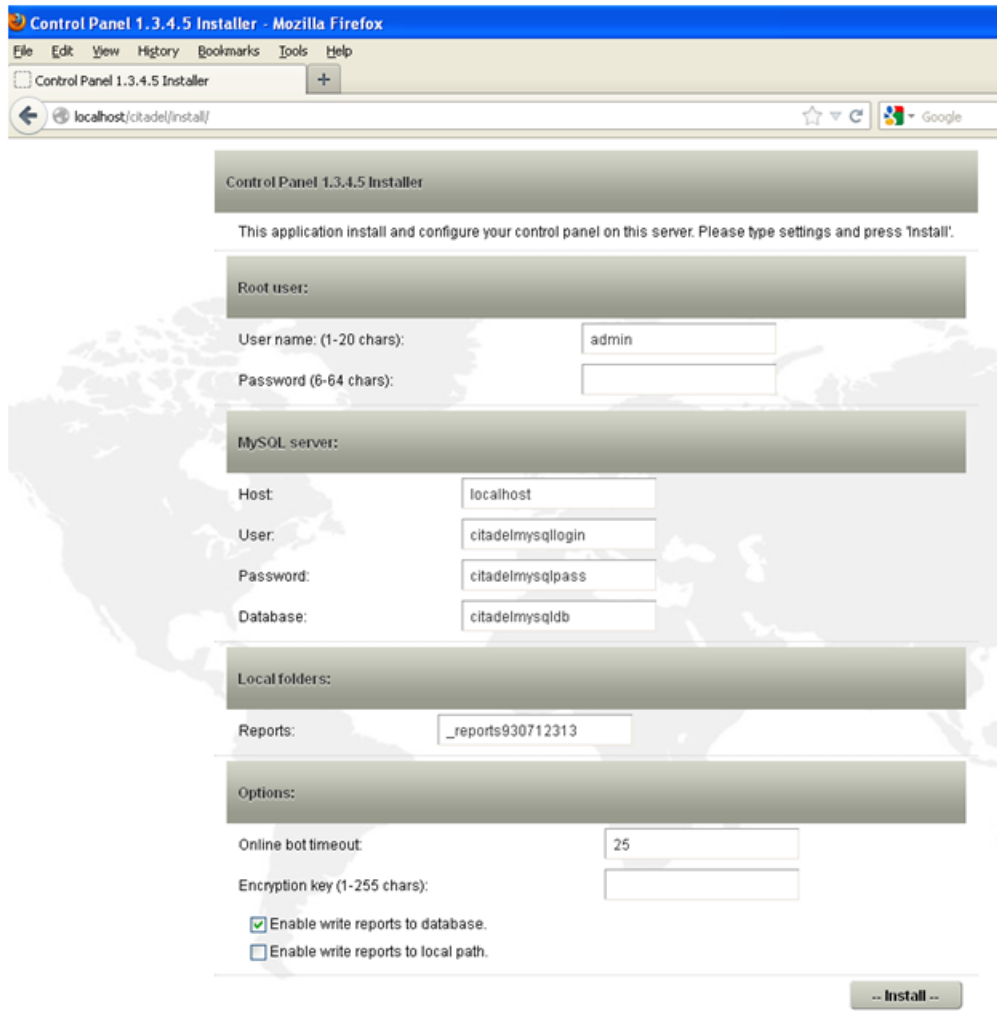
Once again, the core installation files can be found in the underground community or through your own connections. Recently, the Citadel kit was withdrawn from forums to prevent too much exposure and attention. It costs around \$3000 USD.

Figure 2 shows what the package looks like. An instruction manual in both Russian and English is provided. The kit requires server software such as Apache, and PHP with a MySQL database to work properly.



*Figure 2: the citadel package*

To install Citadel, you simply browse to the install folder with your browser (Figure 3) and set up the main access username and password as well as database information.



*Figure 3: Citadel's installation screen*

In this testing, the installer did not automatically create the database but you can do so by hand (Figure 4):

```
mysql> CREATE DATABASE citadelmysqldb;  
Query OK, 1 row affected (0.00 sec)
```

*Figure 4: creating a database for Citadel's exploit pack*

To finally access the login page, you need to browse to the cp.php file (Figure 5):

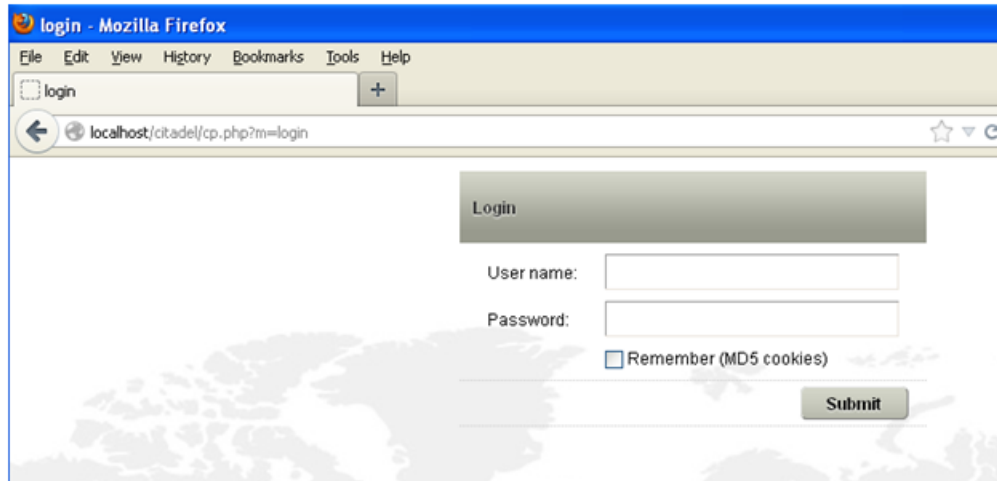


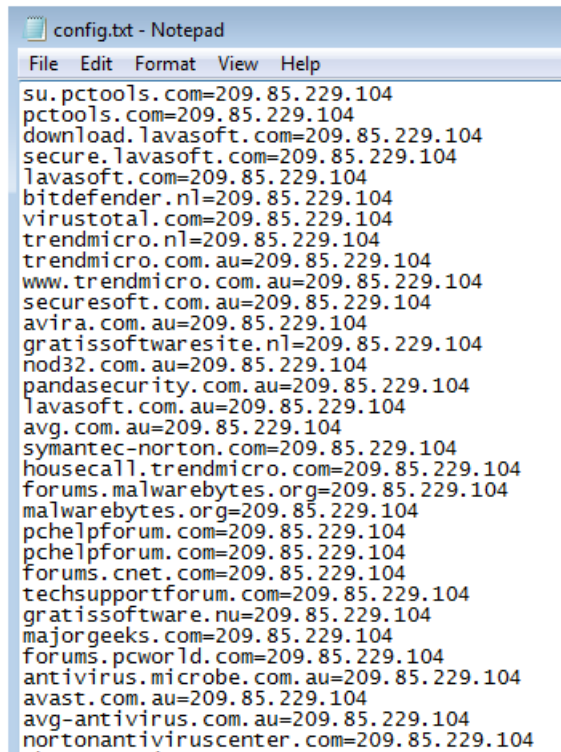
Figure 5: Citadel's login page

Before logging in, I want to show you the other component that makes this package complete. It is called the builder (Figure 6) and is essentially used to create the piece of malware that criminals will distribute (forced installs through infected websites) and that links to their crimekit.



Figure 6: creating the Citadel bot with the builder

The malware is built to avoid AV detection and is tested with online virus scanners like Scan4You, an equivalent to the popular VirusTotal except this one is totally anonymous and does not share uploaded samples with antivirus vendors. Speaking of which, once installed on the victim's machine, the malware will prevent access to security sites (Figure 7).



```
config.txt - Notepad
File Edit Format View Help
su.pctools.com=209.85.229.104
pctools.com=209.85.229.104
download.lavasoft.com=209.85.229.104
secure.lavasoft.com=209.85.229.104
lavasoft.com=209.85.229.104
bitdefender.nl=209.85.229.104
virustotal.com=209.85.229.104
trendmicro.nl=209.85.229.104
trendmicro.com.au=209.85.229.104
www.trendmicro.com.au=209.85.229.104
securesoft.com.au=209.85.229.104
avira.com.au=209.85.229.104
gratissoftwaresite.nl=209.85.229.104
nod32.com.au=209.85.229.104
pandasecurity.com.au=209.85.229.104
lavasoft.com.au=209.85.229.104
avg.com.au=209.85.229.104
symantec-norton.com=209.85.229.104
housecall.trendmicro.com=209.85.229.104
forums.malwarebytes.org=209.85.229.104
malwarebytes.org=209.85.229.104
pchelpforum.com=209.85.229.104
pchelpforum.com=209.85.229.104
forums.cnet.com=209.85.229.104
techsupportforum.com=209.85.229.104
gratissoftware.nu=209.85.229.104
majorgeeks.com=209.85.229.104
forums.pcoworld.com=209.85.229.104
antivirus.microbe.com.au=209.85.229.104
avast.com.au=209.85.229.104
avg-antivirus.com.au=209.85.229.104
nortonantiviruscenter.com=209.85.229.104
```

Figure 7: a list of antivirus vendors that are blocked by Citadel's malware

Here is an example of an infection from a Citadel Trojan.

Infected PCs all report to the mothership and wait for orders. This is where it gets interesting because making malware is one thing but actually managing your own campaigns is the key to success. The Citadel control panel is well designed and puts a lot of features at your fingertips (Figure 8).



Figure 8: Citadel's Control Panel

Each feature is actually a module written in PHP as seen on Figure 9. The control panel gives you an overview of the machines that have been infected. It's a sort of Malware Analytics with stats by country, Operating System, etc...

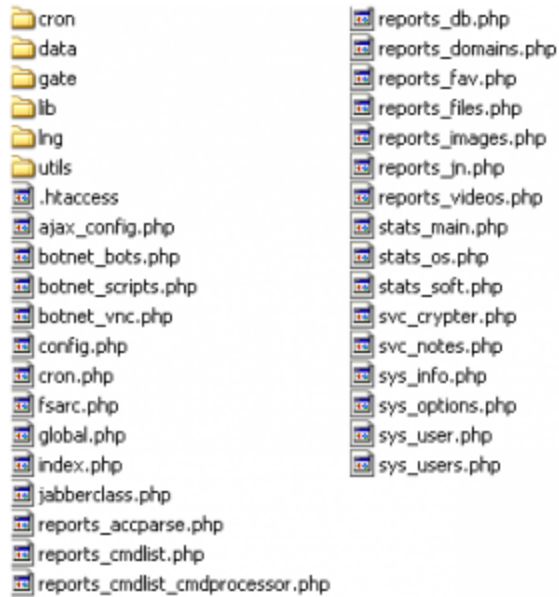


Figure 9: Citadel's modules

The main purpose of Citadel is to steal banking credentials and so it's no big surprise to see advanced search features to specifically look for financial institutions (Figure 10).

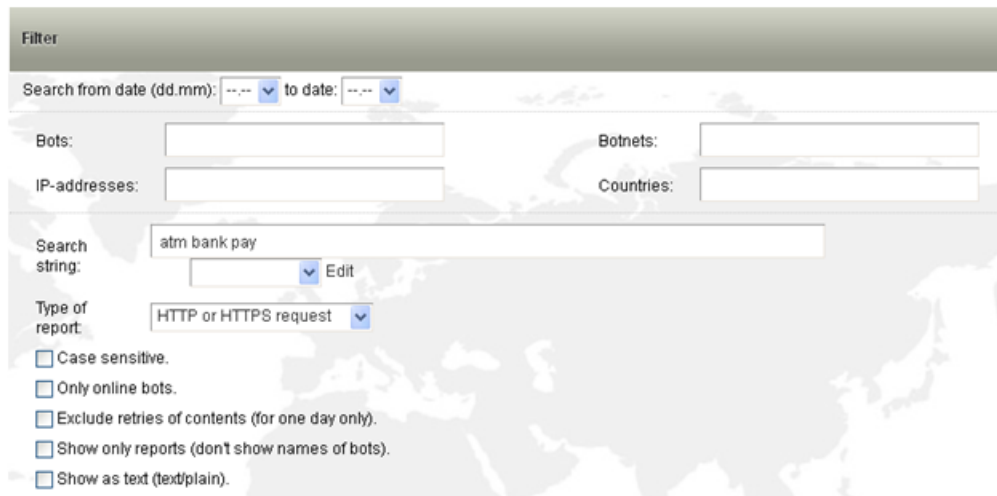


Figure 10: Citadel's advanced search features

A password is a password whether it'd be for a bank or something more common like a Facebook or Gmail account. In fact, you can customize any site that is of interest to you and capture the credentials. Notifications of successfully stolen passwords can be sent via Instant Message through the Jabber protocol (Figure 11).



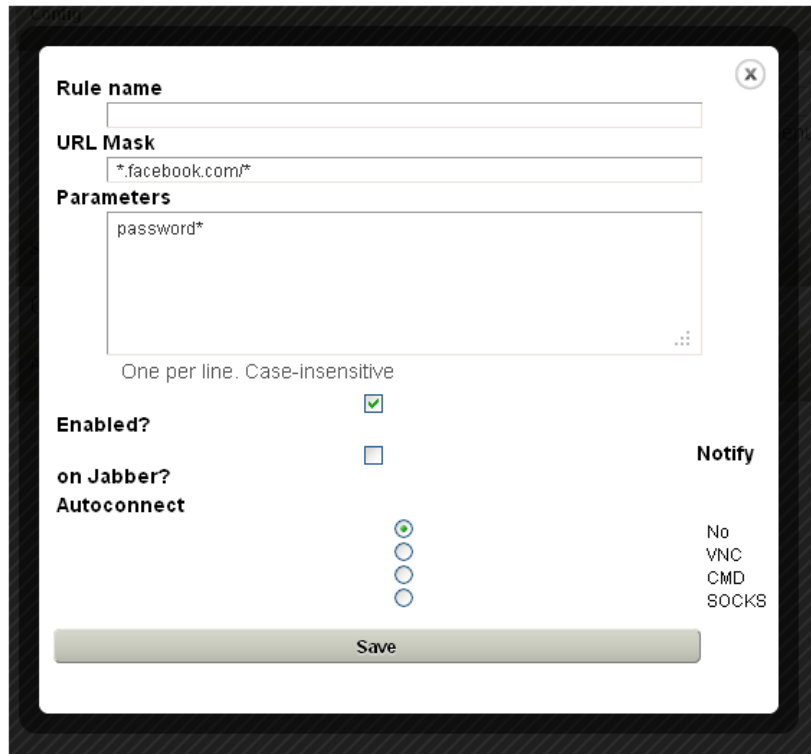


Figure 11: Citadel's custom rules and notifications

Stolen credentials are harvested by various means:

- Keystroke logging
- Screenshot capture
- Video capture

A powerful feature used to trick users into revealing confidential information is dubbed WebInject. It is powerful because it happens in real time and is completely seamless. A WebInject is a piece of code that contains HTML and JavaScript which creates a fake pop-up that asks the victim for personal information within the context of logging into a site. The bad guys can trigger it in two ways: either automatically when a site of interest is opened by the victim, or manually on the fly.

It is the ultimate phishing tool because it does not go against any known proper precautions a user would normally take. For instance, the site's URL is unchanged and shows the secure pad lock with the financial institution's SSL certificate (Figure 12). This type of hack is also called a man-in-the-middle attack.

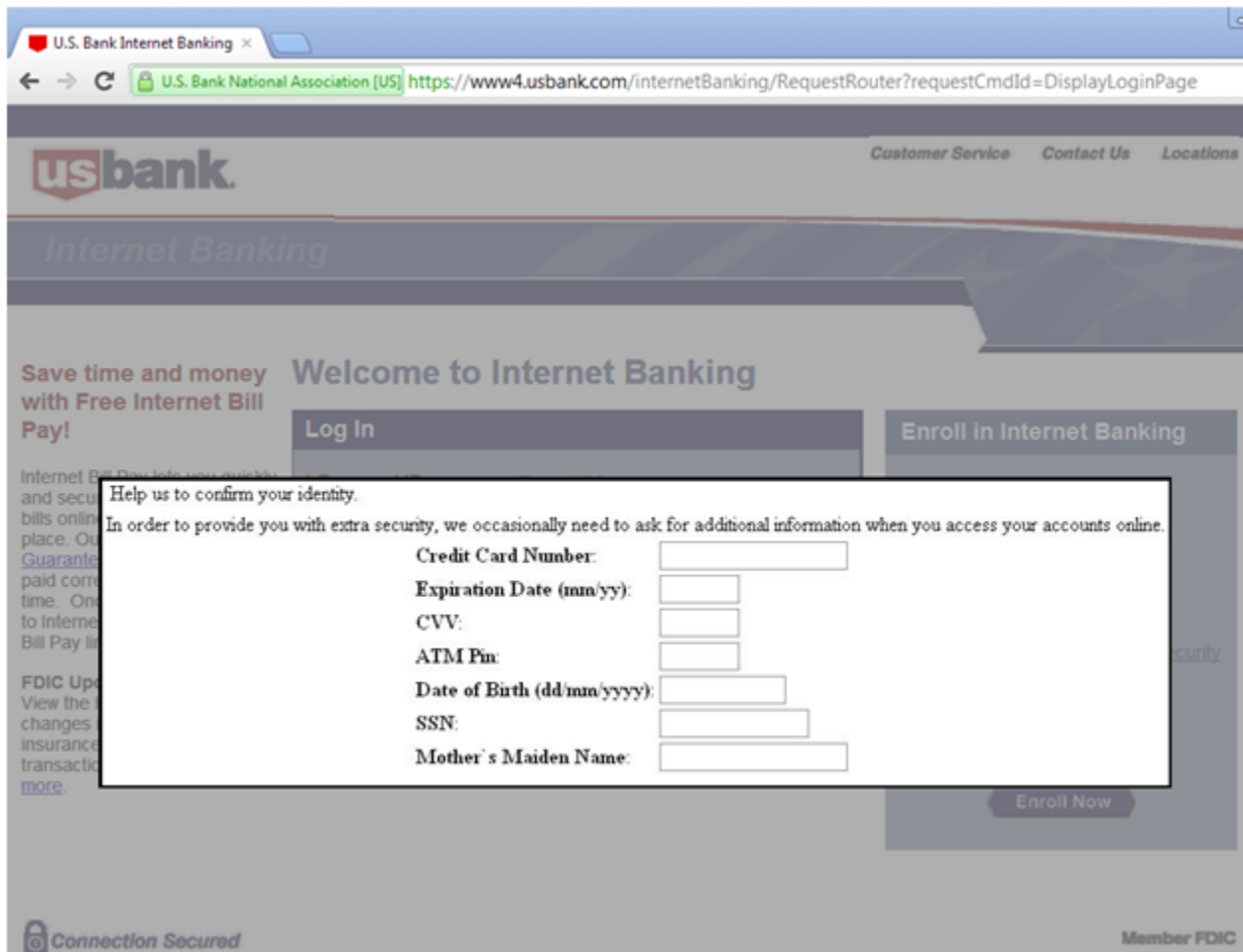


Figure 12: Man-in-the-middle attack through webinject

In case this method does not work (some people might get suspicious), the bad guys can always revert to a more direct approach with some ransomware. Citadel is also involved in the distribution of the FBI Moneypak (also known as Reveton) malware which locks the user out of his computer and demands \$200 (Figure 13). It is customized based on the victim's country of origin.

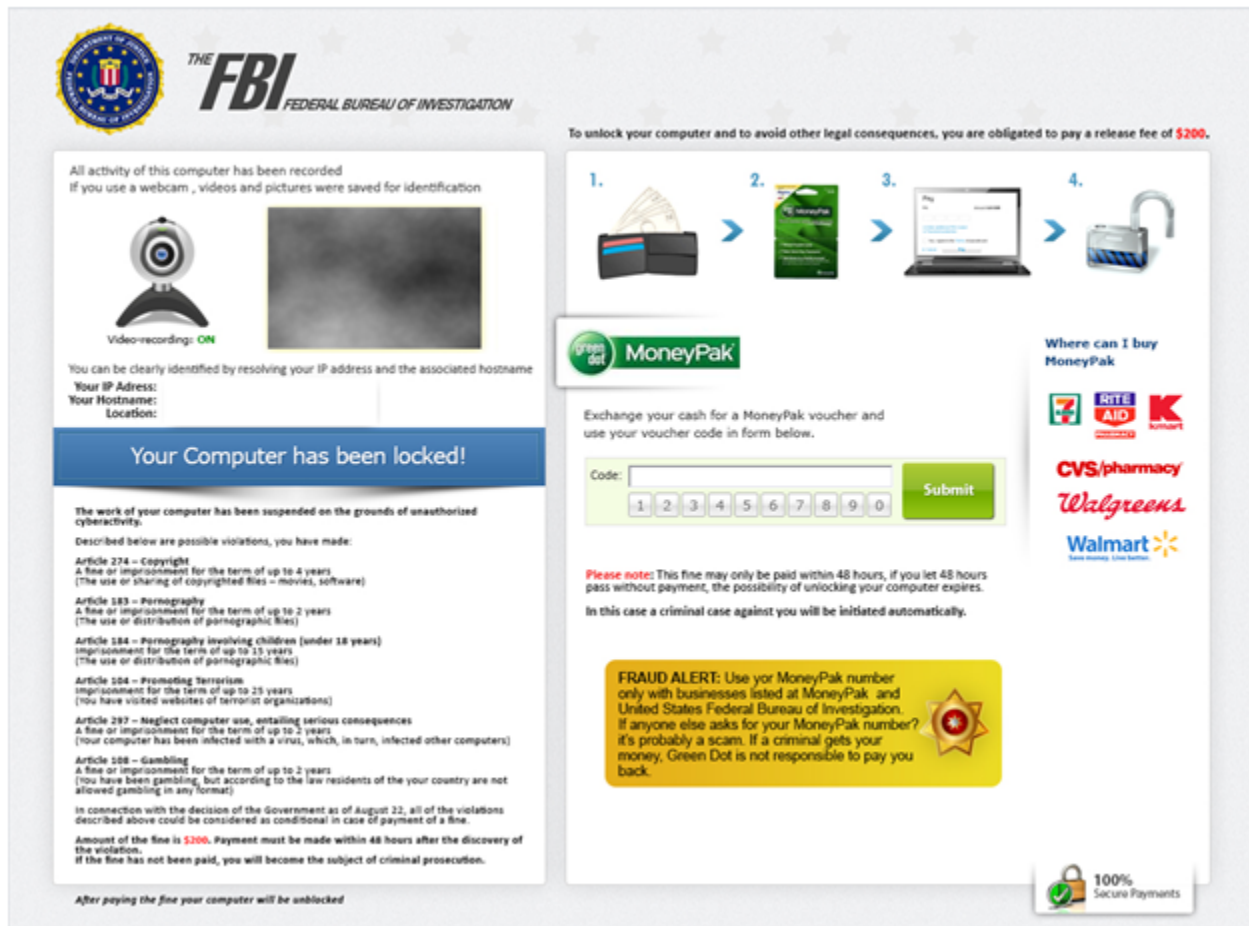


Figure 13: Reveton ransomware distributed by Citadel Trojan

Since a lot of people download music and movies from torrents or other shady sites, the message tricks them into thinking they have been caught by the local authorities. It's a very smart scare tactic which works quite well, unfortunately. To add to the drama, the malware will attempt to turn on the user's webcam as if they were already under surveillance.

The FBI has posted an article regarding this scam (<http://www.fbi.gov/news/stories/2012/august/new-internet-scam>) and urges people to not pay any money as it could get you into even more troubles.

Malwarebytes users are protected against the FBI MoneyPak malware. If you aren't one of them and are already infected you can remove this ransomware by following these 3 steps:

1. Reboot your computer into Safe Mode with Networking. (Instructions from Microsoft [here](#))
2. Download Malwarebytes Anti-Malware.
3. Run Malwarebytes Anti-Malware and remove all malware (Figure 14)

That's it!

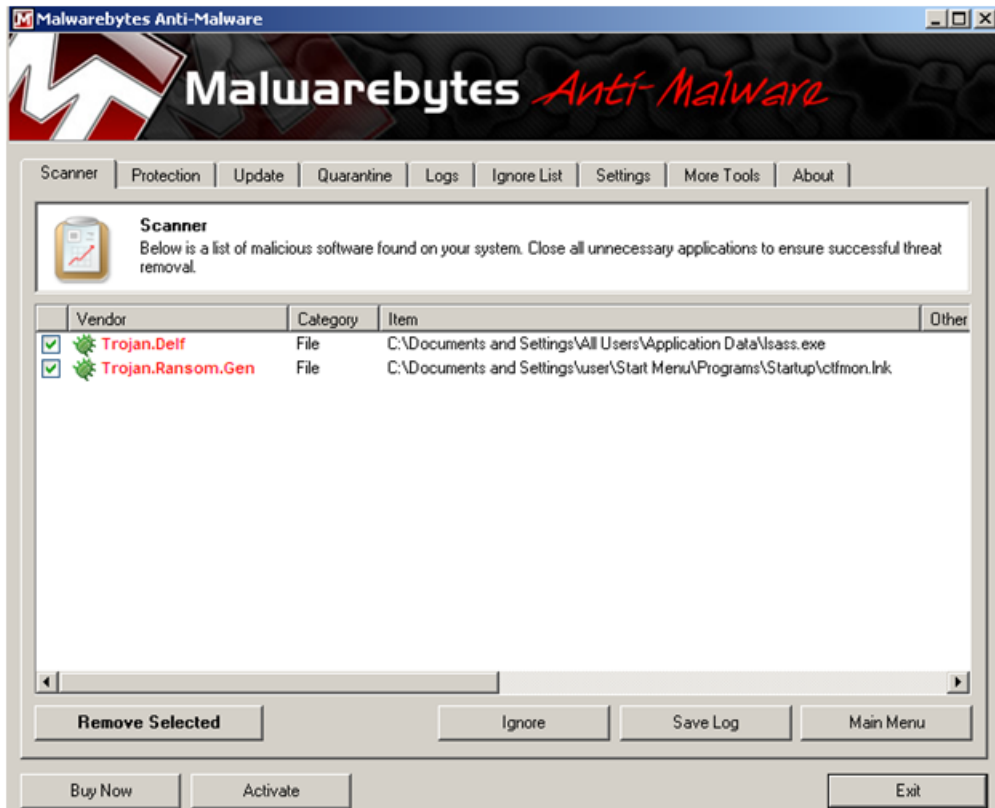


Figure 14: Reveton ransomware Trojan detected by Malwarebytes Anti-Malware.

### What's next for Citadel?

The latest version (1.3.5.1) whose code name is Rain Edition is getting pricey at \$3931 but it includes a lot of valuable features (advanced support for Chrome and Firefox, improved WebInjects, smarter 'on-the-fly' updates to the Trojan, etc...).

The makers of Citadel are trying to keep a low enough profile to avoid gathering too much attention which could result in efforts to go after them (as we have seen with Zeus). Getting your hands on Citadel is more difficult because of a stricter validation process within the Russian underground.

### How to protect yourself

When seeing such technically advanced crimekits it puts a lot of things into perspective. The methods used to steal personal information are so advanced and sneaky that even the most cautious user may get fooled. It is best to avoid infection in the first place by using a solution such as Malwarebytes Anti-Malware PRO that constantly protects your computer by blocking malicious sites and files. Using a combination of both safe online practices (if you ever feel uncomfortable disclosing personal information, give your bank a call or ask a friend) and a good anti malware solution will keep you safe(r).