

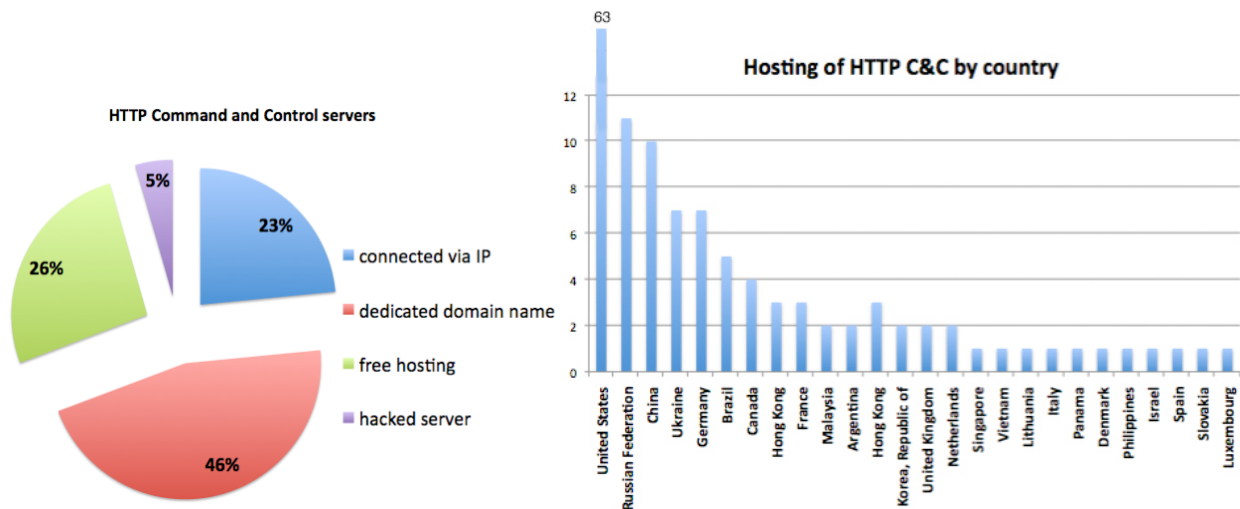
# A TASTE OF HTTP BOTNETS



Botnets come in many flavors. As one might expect, these flavors all taste different. A lot of Internet users have had their taste of IRC, P2P and HTTP based botnets as their computers were infected with malicious software. HTTP based botnets seem to be the flavor of the month, but what do we know about the recipe for HTTP based botnets? Who's actually cooking them? This paper takes a closer look at HTTP botnets and tries to give insight on who is behind the stove and what exactly is being served.

## The Locations

As HTTP botnets use HTML to communicate, naturally they try to blend into normal HTTP traffic, but are HTTP botnets also hosted on legitimate (hacked) websites or do they use specially registered domain names for their purpose? Looking at one day of identified HTTP C&Cs in June 2008, we see that 46% used a dedicated domain name. Indeed, it appears that most of those dedicated domain names were registered for only one purpose - they serve only the HTTP botnet. Perhaps here lies an interesting opportunity to take down some of these nets; flambé the domain name to bring some pain to the herder.



Figures 1 and 2 represent one day of HTTP C&C locations in June 2008.

We have also seen that 26% use *free hosting* at providers like 'freehostia.com' and 'funpic.de' to control the net. Others C&C's use a 'static' IP address that the infected users need to connect to.

When we look at the 131 unique IP addresses involved in the snapshot of one day in June 2008, we see that 63 of those IP addresses are located in the United States, followed by 11 hosted in Russia and 10 in China.

As we see in Figure 1, we also spotted hacked servers, which were misused for HTTP C&C purposes. A closer look at these hacked servers showed that a significant number of them were websites maintained from Brazil or used the Spanish language. Could it be that, culturally or for technical reasons, Brazilian hackers prefer hacked servers for their HTTP C&C's?

## The Menu

All HTTP botnet C&C servers have the same purpose; control the network. One major advantage of HTTP based botnets over traditional C&Cs, is the fact that more information can be easily presented to the herder. It's a bit like 'botnet 2.0' for the herders and more accessible for those who didn't grow up with IRC.



Figure 3, Firepack web interface

The figure on the left shows an example of the web interface of the FirePack Exploit kit. The webpage will give a nice overview of the type of infected machine and the country it is located in.

Firepack is said to be sold for \$3000 [1] although it is not as advanced as the IcePack and Mpack kit.

Visible in this particular Firepack version is the fact that it is in English and also contains Russian text:



Recently the Firepack kit has also been translated to Chinese as it is now available for the Chinese market [2].

# A TASTE OF HTTP BOTNETS



## Some Tasting

The exact usage of each of these botnets differs. We have seen several HTTP based botnets that were engaged in DDoS attacks, installation of adware, obtaining financial account login details and some botnet operators rented out the infected clients as proxies. As expected, HTTP C&Cs are used for several different criminal activities at the same time and do not seem to differ greatly in this regard from their IRC or P2P based relatives.

So what are the patterns of victims connecting to a HTTP botnet? In this example we look at a *machbot*. The infected clients connect to this host using a base64 [3] encoded string, containing information about the local IP, operating system and user id number. For example;

```
GET /cgi-bin/get.cgi?data=dmVyPTUmdWlkPTE4MDczMzM2NSZjb25uPSZvcz1YUCZzb2Nrcz0xNTczJmlwPTE5Mi4xNjguMTk3
```

The server involved would answer with a base64-encoded string which could contain a DDoS target or a command to download a additional piece of malware. As this particular type of botnet uses base64 to encode the request and answer, it is fairly easy to track activities from the C&C server. Some of the other HTTP based botnets do not even use any form of obfuscation and commands can be read directly.

Looking closer at the host involved, we saw that infected computers were also connecting to the host and reporting information on socks ports. For example;

```
GET /cgi-bin/stat.cgi?25896;25874;21458;SOCKS4;SOCKS5;
```

Therefore it seemed that the infected computers weren't only used in DDoS attacks, but could also be rented out as proxies [4]. Looking at one day of victims connecting to this botnet we see 3929 distinct IP addresses. These victims connected with one-minute intervals to the host reporting their socks information. Plotting these 3929 IP addresses on a world map, we can see the following infection locations:

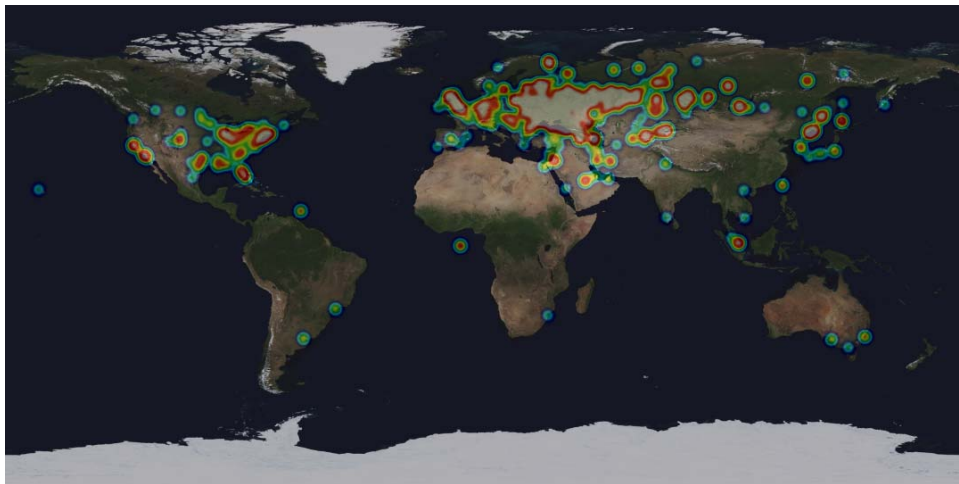


Figure 4, heatmap representation of infected users of a machbot

Selling these proxies isn't just limited to the 'underground scene'. Some of them actually have highly developed websites, in different languages with login function for their customers.

## PROFESSIONAL SOCKS SERVERS

### Socks 4/5 Service

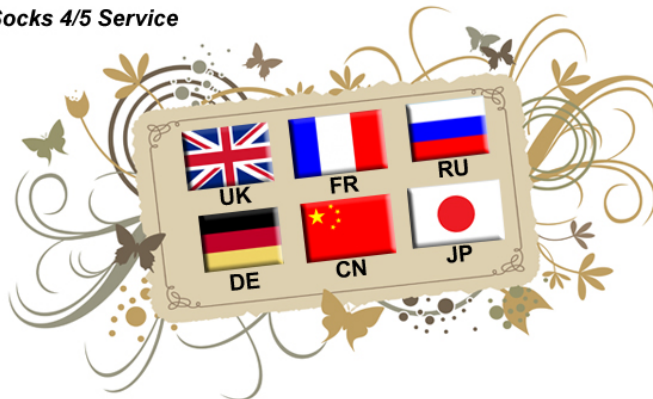


Figure 5, professional website for socks proxy renting

# A TASTE OF HTTP BOTNETS



A closer look on the website reveals a sales pitch: "A unique feature of this services is that ALL proxy servers are checked up every 5 minutes! This means that 99% of all proxy servers, which you can see, are working" Another interesting phrase that speaks to the criminal activity involved is the fact that the websites states: "the average lifetime of a particular proxy server is 24 hours."

## Tariff Rates

Daily plans ***						Per Use plans				
1 Proxy Price	Daily Limit **	Monthly Price	Tariff Name	Quantity Per Month	Proxy Helper	1 Proxy Price	Monthly Price	Tariff Name	Quantity Per Month	Proxy Helper
0.13€	5	\$20	Daily 5	150	\$10	0.50€	\$9.95	PerUse 1	20	\$10
0.11€	10	\$35	Daily 10	300	\$10	0.30€	\$15	PerUse 2	50	\$10
0.08€	20	\$50	Daily 20	600	\$10	0.25€	\$20	PerUse 3	80	\$10
0.07€	30	\$65	Daily 30	900	free !	0.15€	\$29.95	PerUse 4	200	\$10
0.06€	50	\$95	Daily 50	1500	free !	0.10€	\$50	PerUse 5	500	free !
0.05€	75	\$125	Daily 75	2250	free !	0.07€	\$69.95	PerUse 6	1000	free !

\* Quantity of proxies, involved in monthly payment.  
 \*\* Quantity restriction on proxies which you can use for a day  
 \*\*\* Tariffs have a refund system implied to a proxy that goes dead while work

Figure 6. Proxy Rates

Renting 600 proxies will cost around \$50 per month, with a limited usage of 20 proxies per day. So a botnet with an average of 4000 bots online per day could easily make \$10,000 per month, providing that there are enough customers.

Not only does the website provide a login functionality, the also provide a special support program, that will update itself with the latest available proxies for the account purchased. This level of investment on the part of the developers would certainly suggest that business is good.

As can be seen in figure 7, with the click of a button a miscreant can change from a proxy in Saint-Laurent-du-Var, France to a proxy in Venezuela.

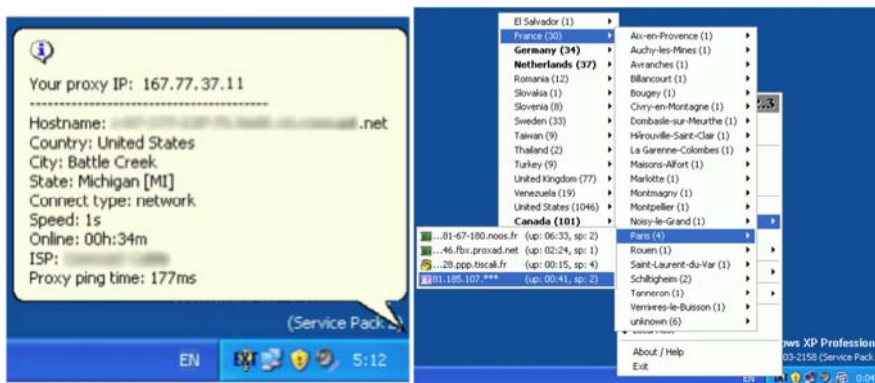


Figure 7. Support program

Not only do the proxies show the global activity of these miscreants but the different languages on the website suggest the depth of international cooperation between these miscreants on the Internet. Below, for example, you can see the Japanese version of the website:

全部の SOCKS 4/5 と言うプロキシは最大の活動の時期が 24 時間です。すべてのプロキシのセルヴェル()は 可や 国 や 州や 網に加入するタイプやスピードや オンラインの 時間やドメインやいかなる要点で 探すことも出来ます。もし、貴方が何かちょっと 遠くないと 思ったら、サービスを使い始める日から 二日間に亘って、二日間の 価格を引くことを含んで、お金を返すことが保証します。貴方に "http" と言うプロキシが必要だったら、 局地的なプロキシサーバーを創立する "sockschain" と言うプログラムを使っていいです。同じの時に、このプログラムは自分で "socks" プロキシを通して、働きます。サービスは 毎月に 最小の料金を与えます。すなわち、もし貴方は月に亘って一か月の(7)を 消費しなかったら、残った税率の部分が すぐ無くなります。"Support" で "account" を作った後、コントロールボードから 自動的に料金を払うようになります。いくらかの将来の月に関する料金を払う可能性もあります。



Figure 8. Japanese language on the website

# A TASTE OF HTTP BOTNETS



## The Ingredients

When we take a closer look at the location of infected users per country for another particular HTTP botnet we have been tracking, we can see that 75% of the infected users on one particular day are from Russia.

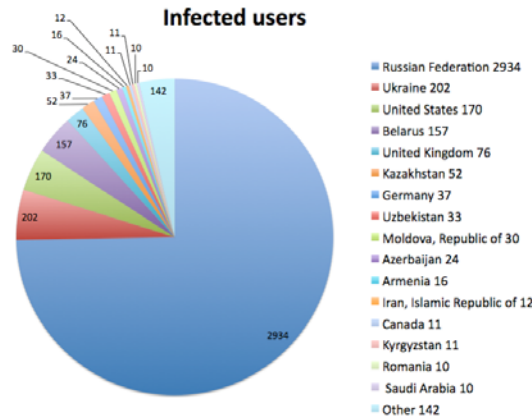


Figure 9, Worldwide infection distribution Machbot

Looking at the other countries involved, we can see that it isn't just Russians that are infected. It could be that the large infection rate in Russia happened due to a spam run with the malware written in the Russian Language or perhaps due to infected websites in the Russian language containing malicious iframes [5].

## To Whom Is It Served?

As we take a closer look at two other active HTTP based botnets involved in DDoS attacks, we see some interesting things. These two botnets are operated by Eastern European suspects. One botnet is located in the US and the other in Europe. The first one shows that this particular net has a history of attacking escort and pornographic websites. We see that 14% of the attacks are targeted at escort agency websites and 15% target pornographic websites:

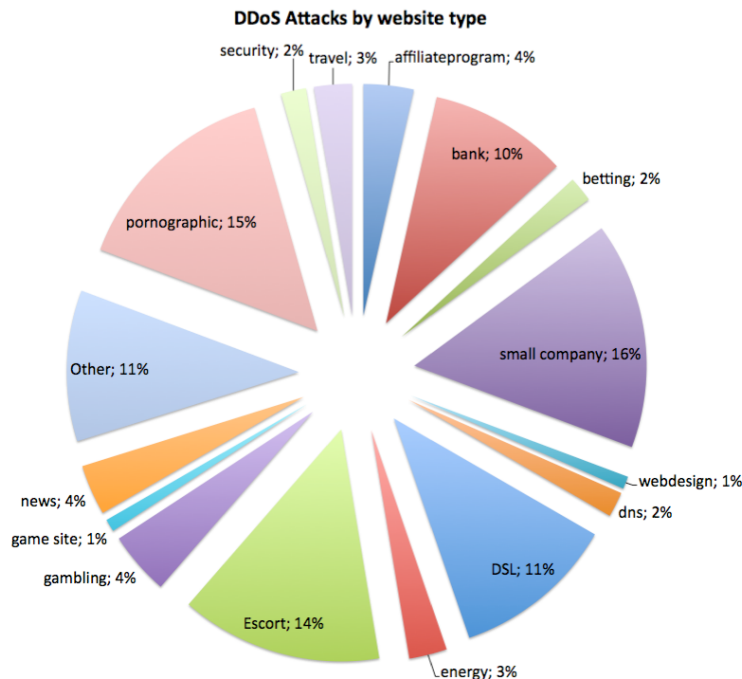


Figure 10, DDoS attack victims HTTP botnet 1

# A TASTE OF HTTP BOTNETS



When we take a look at the second botnet, we can see that this botnet is more interested in attacking advertising and investment programs (HYIP) as well as websites selling ICQ [6] numbers:

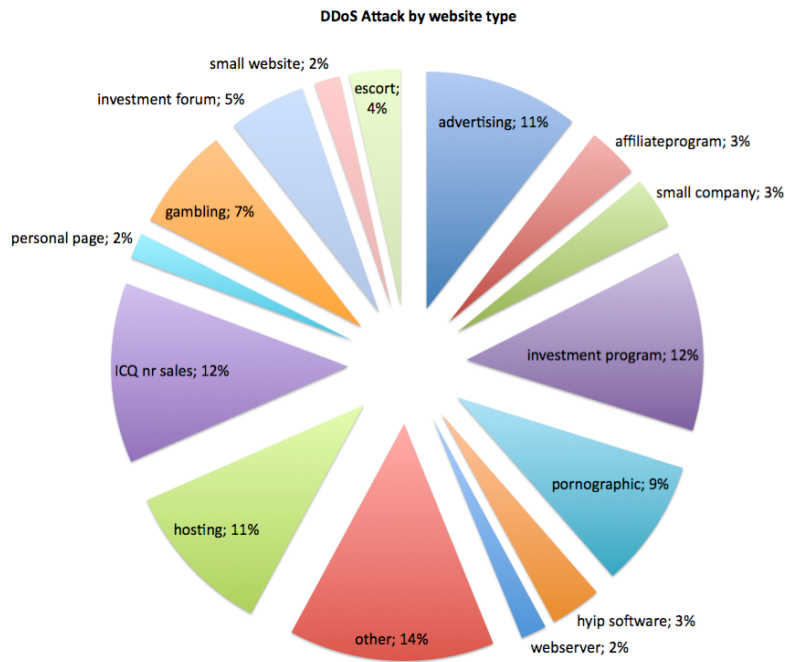


Figure 11, DDoS attack victims HTTP botnet 2

## The Language Mousse

Besides the type of website being attacked, we can also look at the language of the website under attack to get a better idea of who the victims of these attacks really are. In both example botnets, we see that most victims are Russian speaking. As some attacks are targeted at IP addresses that could not be linked to a website, no language could be discerned. These were for the most part attacks against DSL based Internet connections.

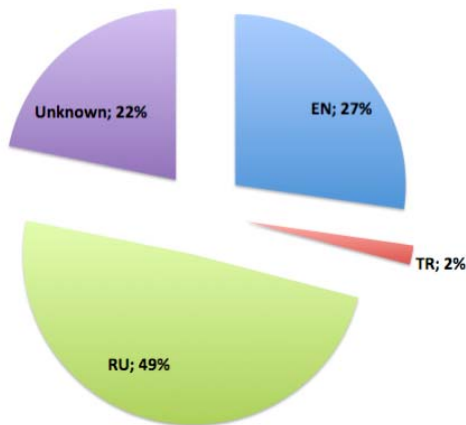


Figure 12, Website Language victims HTTP botnet 1

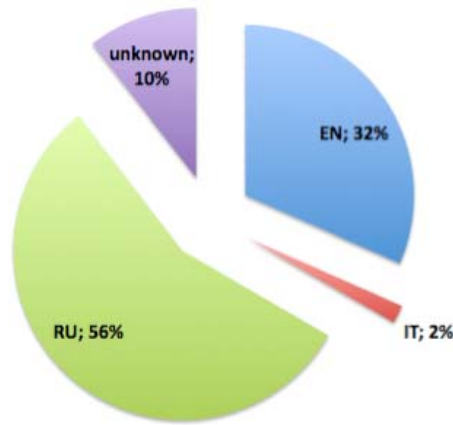


Figure 13, Website language victims HTTP botnet 2

# A TASTE OF HTTP BOTNETS



## Advertising

How do these criminals find targets? One of the ways is to advertise on forums or use an already established contact list of clients asking for DDoS attacks. Below is the advertisement of one of the HTTP botnets mentioned. It is translated from Russian into English and redacted.

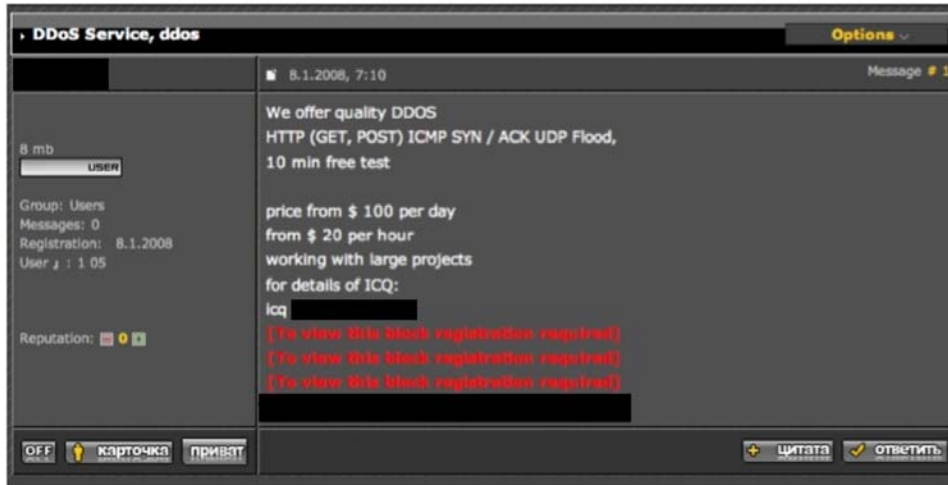


Figure 14, miscreants' advertisements

You can see, in this advertisement, the use of ICQ IM program to contact the poster. In Russian based miscreant activity we see that ICQ is the most popular way of communicating between criminals.

## The Chinese Kitchen

When we have a look at the Chinese HTTP botnets we see that a lot of these nets target mostly websites in China. Looking closer at two of the most active Chinese based HTTP botnets, we see that almost all of the attacks are indeed targeted towards Chinese IP space.

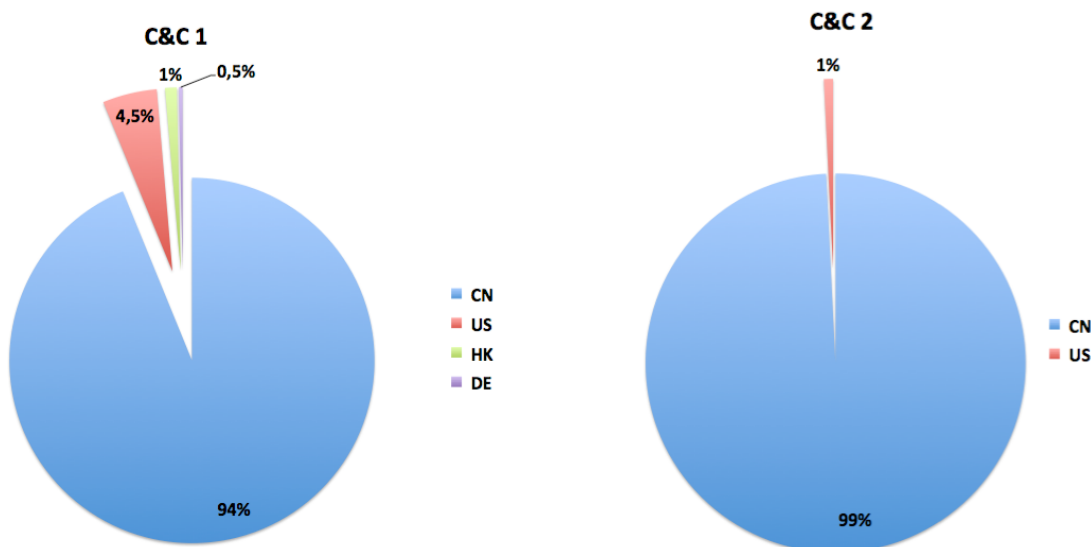


Figure 15, DDoS target countries Chinese HTTP based botnets

A closer look at the DDoS targets from the botnets reveals that games sites are popular targets for some of the Chinese HTTP botnets.

# A TASTE OF HTTP BOTNETS



When we take a look at the infection distribution for one particular Chinese HTTP botnet we see they have a high infection rate in Asia, but there are also infections across the world. Further investigation into this host showed that it was also engaged in installing (English) adware, which would explain that worldwide infections are important for the financial reward driving the use of this C&C.

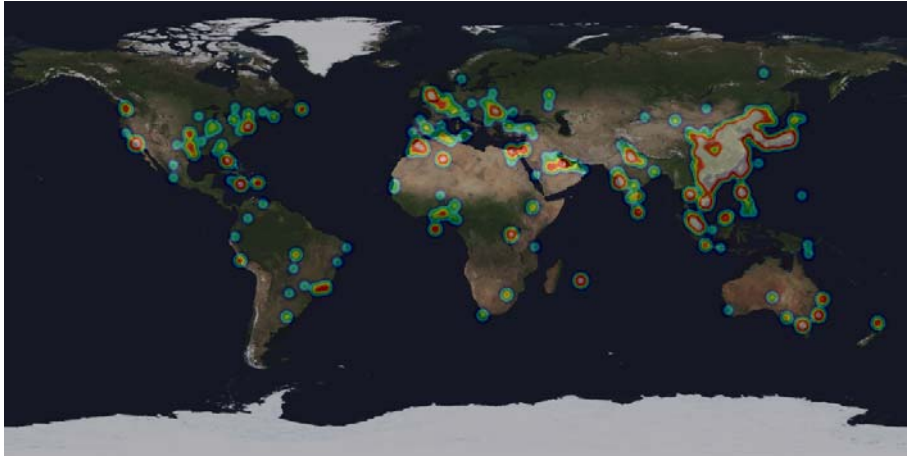


Figure 16, Worldwide infection distribution of a Chinese HTTP botnet.

## The Conclusion

In recent years law enforcement and industry have partnered much more effectively in addressing the issue of traditional IRC based botnets. This has meant the miscreants that rely on botnets for their livelihoods have been forced to develop new techniques to try to stay one step ahead. Web based botnets are a natural evolution of the original IRC based botnets. Our research shows that there are some significant differences in their use compared to other types of botnets; geographically as well as culturally and technically.

The US remains the most popular hosting location for the C&Cs but there is a marked preference for dedicated and free hosts as opposed to hacked machines. Victims of many of the newer HTTP botnets we have examined are located in countries traditionally accused of harboring those behind botnets, such as China and Russia. Could it be that these markets have themselves evolved to the point where they are ripe for extortion or competitive attack through DDoS?

We have also seen a marked increase in the level of sophistication and variety of money making criminal schemes involving botnets: not only has the engineering developed but the application and use of these tools has also matured from the last generation.

What is clear is that the game has changed again. Botnets remain the foundation of so much cyber crime and they are cheap to deploy and capable of enough revenue generation to justify someone paying an army of criminals to maintain and develop these tools. Law enforcement and industry must redouble their efforts to communicate and share intelligence in partnership. Team Cymru remains committed to being at the forefront of the fight to combat the march of this newer generation of botnets, wherever the miscreants behind them turn out to be. For more information on what you can do to help please visit [www.team-cymru.org](http://www.team-cymru.org).



# A TASTE OF HTTP BOTNETS



## References:

- [1] Firepack - <http://pandalabs.pandasecurity.com/archive/FirePack-for-the-winter.aspx>
- [2] Firepack exploit kit - <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>
- [3] Base64 encoding - <http://en.wikipedia.org/wiki/Base64>
- [4] Socks Proxies - <http://en.wikipedia.org/wiki/SOCKS>
- [5] Iframe html tag - [http://www.w3schools.com/TAGS/tag\\_iframe.asp](http://www.w3schools.com/TAGS/tag_iframe.asp)
- [6] ICQ Instant Messenger Program - <http://www.icq.com/>

## Note:

Some of the pictures and quotations in this paper were redacted.