

SINKHOLING BOTNETS

By: David Sancho and Rainer Link, Trend Micro Senior Threat Researchers

Botnets are a well-known security threat for businesses and end users alike. These are made up of many infected computers and are controlled by cybercriminals. The power of a botnet lies in the number of infected computers that make it up. The bigger a botnet is, the more it can do because of its members' compounded bandwidth and computing power. This allows cybercriminals to use botnets as spamming platforms, to instigate denial-of-service (DoS) attacks, or to simply spy on computer users' personal information, including their banking credentials as well as their email and social networking access data.

▶ **Botnets are a well-known security threat for businesses and end users alike. These are made up of many infected computers and are controlled by cybercriminals.**

From a researcher's perspective, botnets are very interesting albeit difficult to fully analyze. From an infection viewpoint, a bot's communication with the server occurs on a one-to-one basis. The victim provides information based on the commands the master server sends. In order to get a glimpse into the other side, we needed access to a malicious active server. We did this via sinkholing—one of several techniques by which one can learn about botnets from the server side.

Sinkholing is a technique that researchers use to redirect the identification of the malicious command-and-control (C&C) server to their own analysis server. This way, the malicious traffic that comes from each client goes straight to the research box, ready to be analyzed.

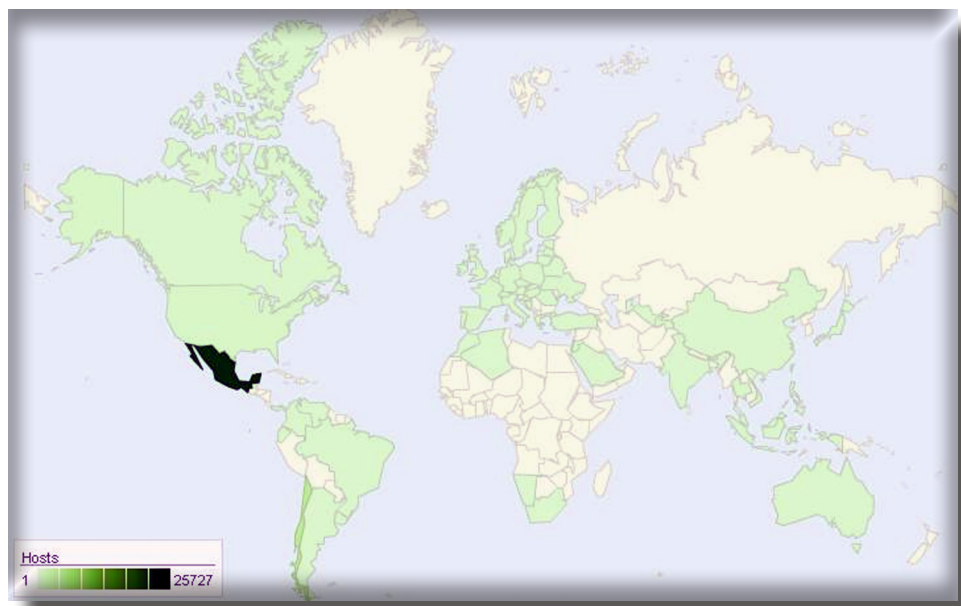
▶ **Sinkholing is a technique that researchers use to redirect the identification of the malicious C&C server to their own analysis server.**

Last month, we had the opportunity to do just that. We hijacked malicious traffic from a Zeus botnet's C&C server. We received a lot of data, which helped us get a clearer idea of the ways and methods that cybercriminals utilize to leverage current botnet technology in order to gather personal information for financial gain.

To impersonate the C&C server, we had to partner with CDMON, the registrar that the cybercriminals used, when they bought the domain name associated with the botnet. CDMON was kind enough to replace the server's original address with that of our own machine. This was enough to tell the bot clients that they should communicate with us instead of the cybercriminal. From the very moment the switch-over ensued, we received an onslaught of requests that we then stored for later analysis. We kept this going for three full weeks until we felt we had enough data then instructed CDMON to stop the redirection. Once done, the botnet remained entirely neutralized and stopped operating. The heavy analysis started from the moment we began to check the data we amassed during that time until we were in a position to draw conclusions on what we saw.

Botnet Statistics

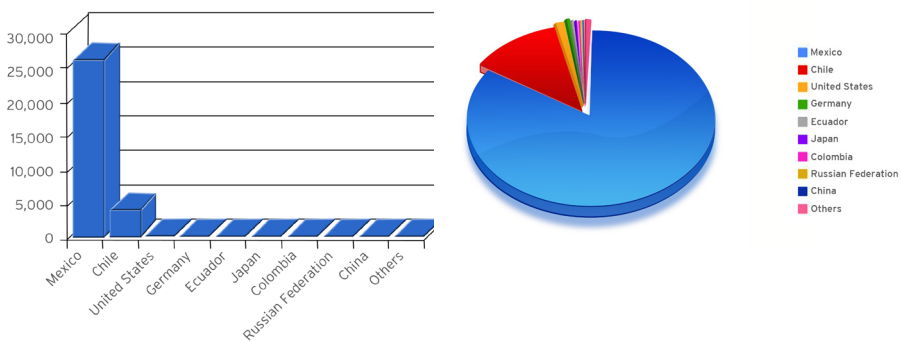
The data we gathered spoke volumes about the origin of the botnet we hijacked. Almost 97 percent of the requests we received came from South America, mostly from Mexico. The requests from the United States came at a distant third. This suggested that the bot either originally targeted Latin American users or proliferated via a Spanish language email or Web page.



It is worth noting that in Mexico, as in Chile, many banks still use single-factor authentication. This means that users may be more susceptible to compromise, as their online banking security remains limited.

We obtained 29,956,607 requests though these only came from 30,567 unique IP addresses. The disparity may have been due to the fact that our machine was configured to send empty replies in place of the malicious ones that the cybercriminals would have sent. As such, the bot clients or infected computers tried to communicate again and again, albeit unsuccessfully.

Split by Country

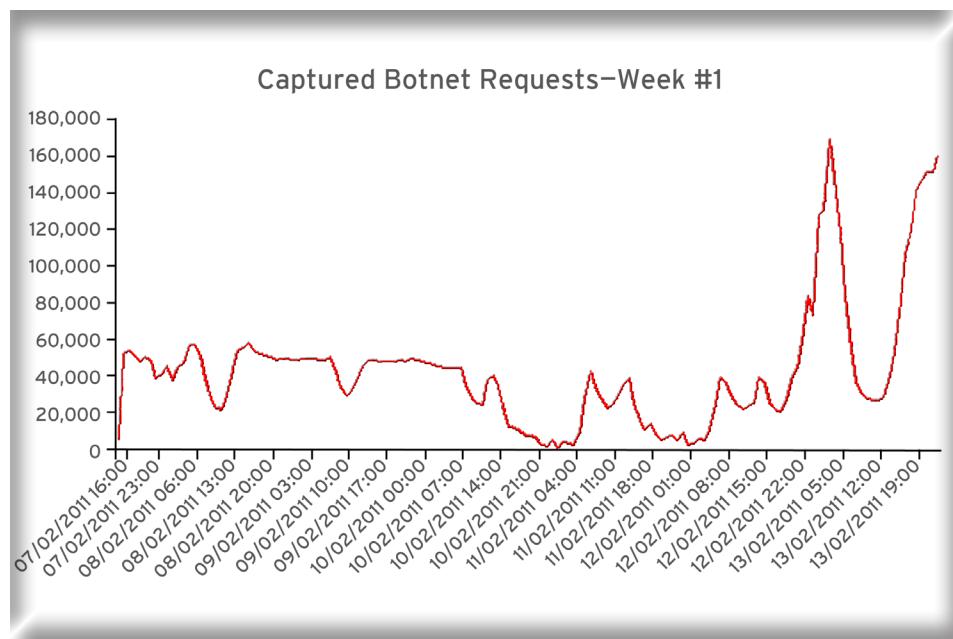


Sinkholing Botnets

A Trend Micro Technical Paper

The number of IP addresses we saw was also misleading because a lot of ISPs force each client to renew their IP addresses often and to acquire new ones. This led us to estimate that, in reality, the botnet was composed of between 3,000 and 10,000 bots.

The seasonality data in the following request graph (in UTC) for the first week is quite clear. The lows correspond to American nighttime hours. The big peaks, on the right side, on the other hand, refer to Saturday and Sunday in the region. As such, their corresponding nighttime in the middle resulted in a big low, as the infected computers were put to rest, which indicates that most of the infected computers were from South America.



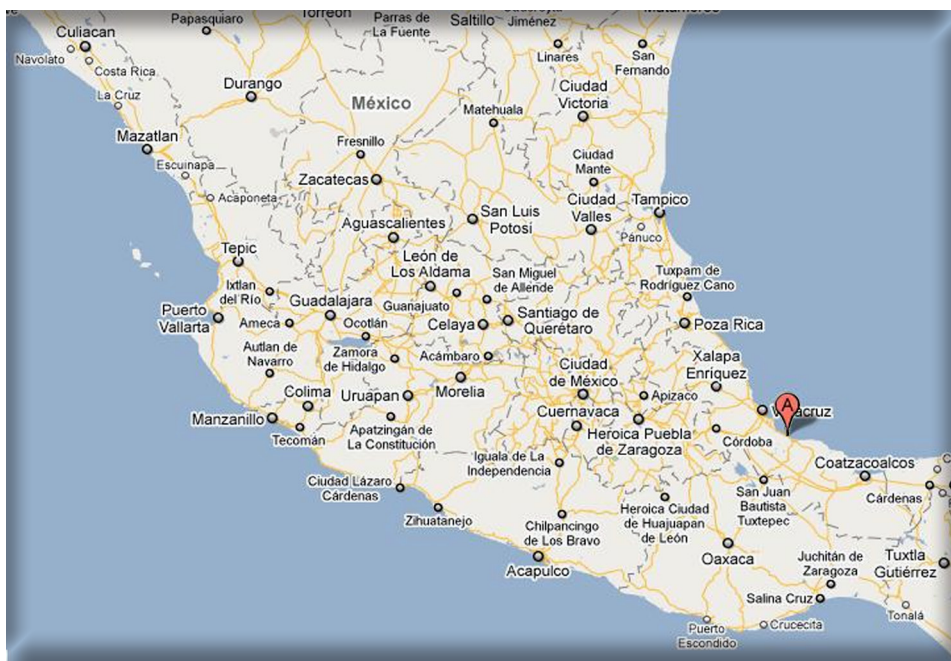
Sinkholing Botnets

A Trend Micro Technical Paper

Most of the connections in Mexico came from the country's capital, followed by Jalisco and Baja California. Our contact in Mexico also informed us that these were the most technologically advanced regions in the country.

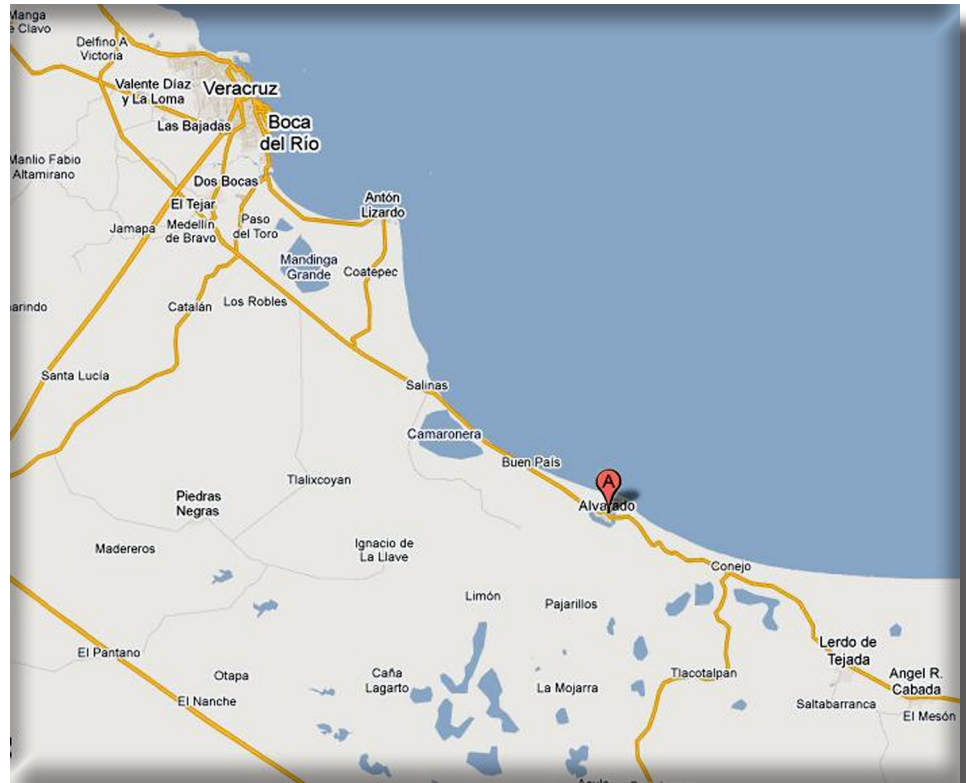


Our glimpse into this cybercriminal activity also yielded more interesting discoveries. We were expecting to see the botmaster connecting to the Web console at some point in order to manage the botnet or to reap stolen information. We checked for possible connections from outside pointing to a Web console and found a clear candidate from Veracruz, a province in Mexico, just a few minutes after the switch-over to our machine.



Sinkholing Botnets

A Trend Micro Technical Paper



The connection proved very suspicious because it had a referrer address that comprised the original domain name of the botnet. This indicates that it was accessed via a link from within the console, which was already open in the browser. The Web session looked open and the cybercriminal clicked a link but was instead directed to our machine, which allowed us to obtain the source IP address. We managed to map out the place where the connection was made and where the cybercriminal may have been at—Alvarado, a city within Veracruz. We also found that the cybercriminal used *Firefox 3.6.13* on *Windows 7* to access the botnet console. Of course, we gave this information to the relevant authorities and left it up to them to close in on the suspect.

From our little activity, we were able to more accurately estimate the size of the botnet and to obtain more information on its owner's geographical location. These gave us a very clear idea of what the botnet's infection targets were. Our undertaking also allowed us to access the botnet's original configuration file. Based on our findings, we saw that its targets included banks in Europe, South America, and the United States. The list of U.S. bank targets include HSBC, Wells Fargo, U.S. Bank, Canada Trust, Bank of America, and Citibank. The European bank targets included Halifax and Barclays (United Kingdom), Banesto and Santander (Spain), Banco Postal and IWBANK (Italy), Banque Populaire (France), AIB (Ireland), and Türkiye İS Bankası (Turkey), apart from well-known online service providers like PayPal, eBay, e-gold, Rupay, and Webmoney.ru. The lack of coherence regarding the targeted banks and the locations of the infected computers suggests that the botmaster just left a default configuration while spreading the Trojan around his own geographical area. This was a sign that he was still an amateur. As part of our investigation, we were able to pinpoint where the cybercriminal planned his operation. For us, the sinkholing project was successful and we look forward to continue using this method to neuter botnets and to gather as much intelligence as we can about their authors.

For us, the sinkholing project was successful and we look forward to continue using this method to neuter botnets and to gather as much intelligence as we can about their authors.

Not from Mexico? Why Should You Care?

Even though this botnet targets Mexico, regardless of where you live, botnets are a serious concern for Internet users. The *Zeus Tracker* website currently tracks over 500 C&C servers while the *SpyEyeTracker* tracks over 200 sites. In theory, each of these servers has a corresponding botnet. With approximately 200 countries around the world and taking into account that SpyEye and Zeus are only two of the multitudes of malware, it is unlikely that not a single botnet is targeting your country in some way. Of course, some countries are more likely to be targeted than others—population, Internet access, language, social trends, and other factors all have an effect. Keep in mind, however, that all that stands between a cybercriminal and a botnet targeting a country of his choice is a few hundred dollars worth of toolkits.

In this botnet's case, we were lucky to work with a registrar—CDMON—that was willing to work with us against the cybercriminals. In other situations, however, registrars and ISPs may not be as forthcoming.

Sinkholing gave us a unique view of a botnet normally only available to the cybercriminal behind it. Even though it was easy to see that the botnet in this case targeted Mexico, who the other 500+ Zeus servers' target is, unfortunately, still anyone's guess.

Sinkholing gave us a unique view of a botnet normally only available to the cybercriminal behind it.