A Call to Action

ISPs and Botnets

Service Providers and Botnet Security – A Call to Action

Introduction

For too long, service providers have been getting a free pass on addressing some of the most dangerous threats to the safety of the Internet. For the past few years, botnets and the criminals behind them have been actively reshaping the landscape of cyberspace for the worse. Endpoint security providers, the financial industry, consumers, and enterprises are, to one degree or another, scrambling to react to these new attacks on their businesses and bank accounts.

However, aside from involvement in a few high-profile botnet takedowns, most service providers have done little to stop these threats from the dark side of the Internet. While a few service providers are taking some effective measures to stop customers from suffering blows to their finances or privacy, most are not. This, despite the fact that ISPs are, arguably, ideally positioned to address this growing problem.

The Botnet Threat

Let's briefly recap the current situation.

On the technological front, we have seen the decline of the 'fire and forget' type of Internet threat in favor of a new approach – malware that includes a 'phone home for further instructions' capability. Botnets, as they have come to be called, have become invisible armies in the hands of increasingly organized cybercriminals.

The exact size of the botnet problem is difficult to determine. Estimates of the number of "zombies" or "bots" – systems infected with botnet malware – vary greatly depending on your source. Shadowserver's estimates of bot-infected PCs over the past 3 years have been as high as 7 million systems, and seldom dropped below 1 million. [1] Some academic research indicates bots could account for as many as 11% of the 650 million computers attached to the Internet, or 71.5 million computers.[2]

What are criminals using all these "bots" for? Predominately: spam, identity theft and other financial crimes. Conservative statistics indicate that between 80% and 95% of spam comes from botnets, and between 80% and 90% of e-mail is spam. Identity theft is also widespread. Amazingly, so many identities are available that a complete individual identity sells for $3 to $15 in wholesale cyber markets.[3]

Many experts agree that one of the key factors in the success of the botnets has been the lack of consistent security practices on the part of individuals and small businesses. This lack of security has given the botnets an open playing field from which to launch their attacks.

Why should service providers take a more active role in solving this problem? There are a variety of reasons, ranging from the selfless, to the practical, to the selfish.

Make the World a Better Place

First of all, ISPs should be looking to keep their customers safe. Some ISPs have begun to 'deal' with the security problem by negotiating with security software providers to give their customers free security software. While this is certainly a good first step, putting the burden on customers to find, install, and maintain security software is unrealistic, and places an unfair burden on the customer. Customers are just that, customers. Their interest is in their lives and businesses. History has shown us end users are not technology experts. If left with the responsibility to protect their PC, many will neglect to do so, making it all the more dangerous for everyone.

In addition to keeping customers safe, ISPs have a responsibility not to pass along malicious and worthless Internet traffic to their peers. Not only are botnets the major source of spam, but they also pump a ton of other worthless traffic onto the Internet. In 2008, Arbor Networks did a study that showed that up to 3% of all Internet traffic is composed of packets that are part of distributed denial of service attacks.[4] These DDoS attacks are another product of botnets.

Ideal Enforcement Point

From a practical standpoint, ISPs are simply in the best position to deal with these types of threats. First of all, endpoint solutions, even if users install them and keep them working, have not proven effective at combating botnets. The efficacy of these solutions can be demonstrated by looking at the rate of botnet infections over the past few years. A particularly telling example is the Zeus botnet, which is well known to collect banking information from infected computers. Although it was first discovered in July of 2007, even as of August of 2010, fewer than 50% of Antivirus clients were correctly detecting and removing this extremely dangerous threat.

A much more effective approach to the botnet problem involves breaking the connection between the bots and their Command and Control (C&C) servers at the network level. This prevents infected systems from sending stolen information back to the C&C, keeps systems from sending spam, and effectively stops the infection in its tracks.

The very best place to do this network-level filtering is the service provider network. The service provider network is similar to the Internet's Interstate Highway System or Autobahn – all traffic going anywhere on the Internet must pass through the ISP network. This makes them the most logical location to intercept botnet communications.

Additionally, ISPs already have all of the technology and resources needed to do this network filtering. At the most basic level, all that is needed are high-performance network routers. The modern infrastructures of nearly all ISPs are more than capable of doing this blocking, with virtually no impact on the overall performance of their network. More advanced blocking of more carefully hidden C&C servers requires looking deeper into the traffic, and making a more complicated decision. This requires advanced traffic shaping or filtering technology. Again, this technology is quickly becoming ubiquitous in ISP networks.

Save Money, Keep Customers

Of course, there are more than a few selfish financial reasons for ISPs to step up to the botnet problem.

Firstly, once customer computers become infected with a bot, they can become *very* slow. When they are active (sending spam, etc.) they also consume quite a bit of the inbound and outbound bandwidth. Bots also have the potential to interfere with other, uninfected systems in the home, or disrupt VOIP or IPTV streaming. This brings up an important motivation – increased customer satisfaction. Providing a safer product will reduce customer problems and increase customer satisfaction.

Secondly, proactively addressing security issues offers the opportunity for ISPs to differentiate themselves around a topic that has the potential to resonate with their customers. Providing 'cleaner pipes' provides a benefit to customers beyond price. Even if security plays only a small role in customer buying decisions, it will impact the bottom line. An ISP with 10 million subscribers who can increase their customer base by even 1% stands to increase revenue by as much as $24M per year.

ISPs may also want to consider taking a proactive stance in the fight against malware in order to avoid mandates from governments. In many ways, Internet connectivity is being viewed by consumers and governments as a public utility, and, therefore, something to be monitored and regulated. After all, consumers worldwide have the expectation that when they turn on the faucet or flip on the light switch, they will not be poisoned or electrocuted. With Internet becoming

the medium for traditional services like telephone and TV, the mission-critical nature of home broadband networks is constantly increasing.

Many watched the recent debate in Australia over censorship of child pornography with apprehension – not because of the issue at hand, but because of its implications for ISPs. If the technical problems associated with filtering traffic correctly can be overcome, it is easy to see how this type of an effort could be extended to include other forms of traffic with absolutely no accepted value. Malware could certainly fall safely inside this category.

By proactively taking meaningful steps to combat the threat, ISPs can legitimately make the case that "the market will take care of itself" and potentially avoid governmental mandates. This could save ISPs huge amounts of money and allow them to adopt the most effective and economical solutions.

Lower tech support costs are another potentially compelling reason for ISPs to become more involved in security. Botnets often give the customer the impression that there is some problem with the network, and triggers a call to tech support. Help desks are an expensive part of any consumer-facing business. Fielding botnet calls is even more difficult, because often times the help desk doesn't have the time or expertise to help the customer fix the problem beyond suggesting "you have a virus, please try installing antivirus software."

The main argument against ISPs blocking malware has been a technological one – much of the malware traffic on the Internet today resembles legitimate traffic. Internet Relay Chat, web, and secure web (HTTPS) are among the most popular protocols used by the cybercriminal. ISPs make the simple argument that blocking any of this traffic risks interrupting valid consumer communications. In the past, there may have been legitimacy to this argument, but technological advances in malware intelligence have begun to create highly actionable, accurate lists of botnet C&C servers that can be blocked without any collateral damage.

Conclusion

Therefore, the time has come for ISPs to step up to the plate and begin taking an active role in protecting the safety of their customers and the Internet community. They have a moral obligation to do so, because they are in the best position to combat the threat most effectively. Moreover, there are significant financial reasons for them to become involved, both in lowering their costs and increasing customer loyalty.

To learn more about the botnet threat, visit http://www.umbradata.com.

[1] http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotCount36-Months
[2] Brent Rowe, et al, The Role of Internet Service Providers in Cyber Security, June 2009, RTI
[3] Symantec Intelligence Quarterly January-March 2010, page 4
[4] http://news.techworld.com/security/11854/net-traffic-clogged-with-junk-packets/