

## Botnet Example Video

We have been installing and maintaining firewalls for 10 years now, long before they were popular. In doing security research at that time we came upon a new startup called WatchGuard. We were immediately impressed with the ease of setup, reporting, and most importantly, protection provided.

At that point in time firewalls were very hard to configure correctly. A lot of them required you to create a set of rules while logged into a command prompt. Others had a very simple web interface, but still required you to create the rules, and then list them in the correct order. Some firewalls took days to setup, configure, and test.

WatchGuard had a different solution. It involved installing a "Control Center" application on a PC and using a pre-defined set of rules. You did not have to worry about implementating them in the correct order either. If needed you could add your own custom rules. One of the things that immediately impressed us though were the proxy filters for smtp and http. With these proxies we could eliminate most if not all viruses before they entered the network. You simply configure the filter to only allow certain safe types of file attachments through.

Shortly after we had installed the WatchGuard Firebox on several networks several viruses spread rapidly on the internet through email. The WatchGuard Firebox did exactly what we had expected. It filtered out the viruses before they entered the network and these networks went on as if nothing was happening. The clients we supported at the time that did not have a WatchGuard installed were immediately infected, even though they were running the latest anti-virus products and were updated daily.

What does this have to do with your network today? A Lot. As you know viruses are still spread through email and are a very real risk. An even greater problem has risen though, especially in the past year. This threat comes from trojans, spyware, and botnets. These infections are not out to damage files on your PC as viruses were in the past. They are after something more valuable - your resources and data. These new infections are also delivered through websites, and any website is capable of infecting your PC. Trojans are normally installed on your workstation to download other programs. These other programs are capable of anything, from installing unwanted games, to key stroke loggers which record usernames and passwords. Of all of these though the worst has to be botnets. They are programs that are installed and controlled remotely by someone. They are worse than your worst nightmare, capable of anything. Anti-virus is useless against most botnets. You can find

information on what to date is the worst of these, the Storm, here .

So, what can you do to keep your network and data safe? While nothing is 100% following these simple rules will greatly limit your exposure -

1) Educate your users.

2) Keep anti-virus and anti-spyware up to date.

3) Install a firewall that provides an smtp and http proxy.

To see how botnets are created and how they work WatchGuard has released 3 excellent videos. The first video, Botnets Part 1 , explains how botnets are created. Video 2, Malware Analysis: Botnets Part 2 , explains how botnets are used. The third video, Malware Analysis: Botnets Part 3 , explains how to protect your network.

For more information on how to protect your network please feel free to email us , or call us at (888) 740-9193.