

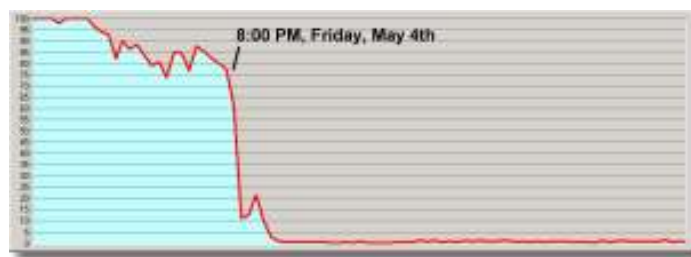
The GRC.com Attacks

by *Simon Salomon*

The Internet is a virtual community that consists of people from all walks of life. It is occupied by different age groups, races, and is used for countless purposes. Although the Internet is a virtual place it is still vulnerable to evil people who wish to terrorize other Internet users. The reasons for such terrorist acts committed by criminals are numerous and each one is in itself a crime or at least a breach of ethics. However, as is with most criminals, ethics is far from their mind.

Unlike the physical world where we have police officers who are employed and dedicated to enforcing the law, the Internet is without such protection. There is really no one central office where we can call and report an incident. There is no phone number that you can call to report a security breach. Imagine calling 911 and reporting a stolen file from your hard drive. You will certainly be denied any serious police services because most people still don't understand the magnitude of the damage that can occur in the virtual world. One great example of this is the events that took place during the grc.com attacks. I shall go through this amazing and exciting publicized story to discuss the problems, difficulties, and the outcome that resulted from these destructive events.

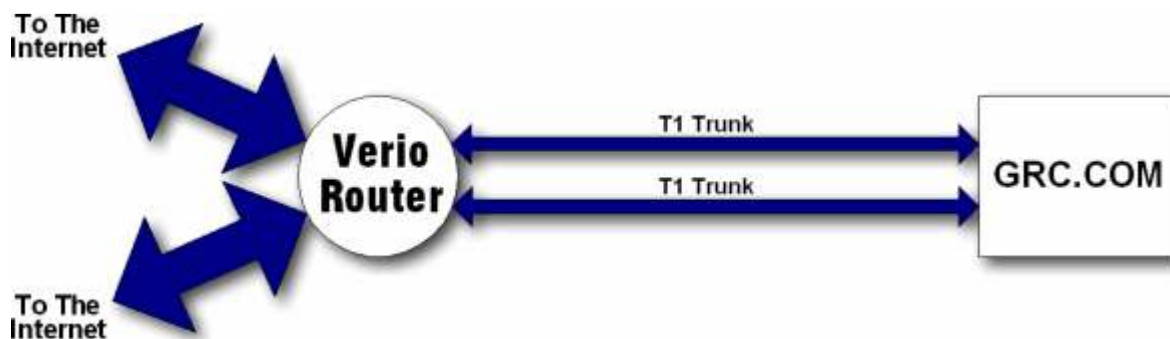
On May 4th 2001, around 8:00 PM, the grc.com website went down. Here is a diagram showing the affect.



The reason for this was not random and it was not for something we would consider to be an illegal act, like for example extortion. The reason grc.com was being attacked was out of anger. Provoked by an article written by Mr. Gibson, a thirteen year old boy who went by the name of Wicked began flooding the grc.com website with large UDP packets and ICMP debris from the large-packet ping commands. Right away the web site's services were rendered unavailable to valid users.

The method of attack was a non strategically made move to consume all the bandwidth that grc.com had available for it's users. The following diagram

shows a high level view of the GRC (Gibson Research Corporation) corporation's connection to their Internet Service Provider (ISP) via two T1 trunks.



As you can see from the diagram above the ISP is connected to the Internet via two huge 100 megabit connections. Once the malicious packets make their way to the ISP they are tunneled to GRC via two 1.54 MB T1 trunks. This means that no matter what they do on the GRC side of the connection there is no way to stop all those packets from consuming all the available bandwidth that GRC is allocated. The only way to stop these attacks or at least diminish their effect on the corporation was to filter them from the ISP's end of the connection.

I felt aghast when I read that the ISP failed to help their customer, GRC, in a timely manner. The corporation's website was down for seventeen hours before Mr. Gibson was able to get someone who would be able to help him. To my amazement it only took two minutes for Verio (the ISP) to remedy the problem. They applied a brute force filter to the Verio router to filter all UDP and ICMP traffic that was headed toward GRC.com. Although this brought the website back up, it was certainly no cure. This was because the blocking of UDP and ICMP traffic not only disabled malicious packets from reaching the site, but it always prevented legitimate UDP and ICMP traffic from going through. However, because TCP was not blocked, the Web/FTP/News services were still available.

Once the website was up again it was time to review the logs. The logged traffic showed that the grc.com website had been attacked by 474 Windows PC's. This meant that the grc.com website had fallen victim to a Distributed Denial of Service (DDoS) attack. Who were all these computers that were used to attack the grc.com website? Fortunately, all the machines that were exploited to produce this attack were logged in the log file. The log showed that there were all kinds of network domains and a cast of Internet Service Providers.

Armed with this information Gibson went to the ISPs of the enslaved hosts and notified them that they had infected machines on their network. At this the ISP just ignored the report and gave Gibson the run around. This is a huge problem, and I never thought this type of thing would occur. How would a network administrator protect his network if ISPs are unwilling to assist with closing down infected computers? Because of this negligence grc.com was attacked five more times. They were attacked on May 4th which brought the website down for seventeen hours. They were attacked on May 13th which brought them down for eight hours. They were attacked again on May 14 which directed the malicious packets this time to the IP address of their firewall. This time grc.com was forced to shutdown one of their T1 links to the internet. On May 15th they were attacked again and this time decided that they would have to remain offline and just begin to log data. And once again they were attacked on May 16th. The following diagram shows a summary of the attacks.



And as the summary shows, they were attacked on 18/19/20 which would be the sixth attack.

Shocking as it may sound, the number of malicious packets that were filtered out were 2,399,237,016. That is almost 2.4 billion malicious packets. All these packets were aimed at grc.com's bogus port number 666. The ability of a thirteen year old child to be able to cause this much havoc to a corporation is unbelievable. However, as we will find out it was not this young boy who created this bot. He just used it to cause damage. Just like any kid using a loaded gun can shoot it without understanding how it works, so can a child bring down a website without even understanding how the bot works.

On May 15th Wicked, the thirteen year old attacker, sent a comment in a newsgroup taking responsibility for the attacks against grc.com. The following is the transcript that was posted by Wicked.

hi, its me, wicked, im the one nailing the server with

udp and icmp packets, nice sisco router, btw im 13, its a new addition, nothin tracert cant handle, and ur on a t3.....so up ur connection foo, we will just keep comin at you, u cant stop us "script kiddies" because we are better than you, plain and simple.

As you can see from the above transcript the kid cannot even write properly. This is the kid who brought down grc.com. To this Mr. Gibson replied and began to initiate a means of communication with the Internet terrorist.

Once again the young thirteen year old terrorist attacked the grc.com website and gloated about it in his email back to Mr. Gibson. At this he called EarthLink to ask about the IP address the attacker was using in his email. However, EarthLink turned a blind eye and gave away no help to stop this kid. This time he decided to go to the FBI. Surely the FBI would be able to do something. However, they too said that unless there was evident damage they would not be able to get involved. They were already swamped with so many cases that spending time and money on this case would not be worth it. Once again it is apparent that there is no help out there. You are on your own and when faced with such an issue what are our options?

Finally there was a break which Mr. Gibson surely needed. He sent out a massive email asking for someone to submit a Zombie and some anonymous person did just that. Now that Mr. Gibson had access to a real Zombie he was able to study it and learn how it works. Using this knowledge he began to build his own bot that would spy on the IRC channel where Wicked was known to be in.

When Mr. Gibson decided to come out from spying he was in the presence of a hacker named ^bOss^. Mr. Gibson had a conversation with this hacker and told him that he has been watching their IRC channel using his own bot. He knew all about their new bots that they were planning on making and even addressed one of the mistakes he found. Mr. Gibson was finally able to get the thirteen year old Internet terrorist to stop attacking him, but it took a lot of time and of course a lot of money. However, stopping him did not mean putting the kid in prison or taking his computer away. He had to ask for the kid to stop attacking. This is daunting and it seems that we are losing the battle against hackers and script kiddies.

Reading this publicized security failure I found myself wondering if I would be able to handle this kind of problem. I realize how much trouble it is having to call your ISP and asking for help. This informs me that I must make an effort to have a good and solid relationship with the ISP I'm working with. I will have to work very hard trying to get people to help me out. As I have pointed out in this paper not a lot of people are willing to spend their time helping you solve

your problems. Knowing that any child can bring down my website is a dreadful thought and I am hoping I will never have to deal with such a predicament.

Although I am a bit timid now about network security, I feel much knowledgeable because of the paper I read on grc.com. This is a huge incentive for me to begin reading more articles and to learn how others have solved their problems. Although I know that we can never create a network that is 100% secure, I feel that with experience and defense in depth, we can provide a fairly safe service to legitimate users.

Resource

GRC.com, "The Strange Tale of the Denial of Service Attacks Against GRC.COM", <http://www.grc.com/dos/grcdos.htm>. Pages 1-29.