

Security and Your Business



Newsletter # 9 – November 2010

Welcome to the Archimedes Technologies, LLC Security Newsletter.

Archimedes Technologies is sending this newsletter to discuss serious threats to your business. It has been some time since we last published our newsletter -- time flies when you're having fun. Joking aside, we are working behind the scenes every day to make sure your business is protected. This newsletter focuses on one portion of our managed services: outside break-in attempts. We were seeing a disturbing trend, and so for the month of October 2010 we started tracking break-in attempts in a different way. We tracked each and every IP that attempted to break into one of our managed clients back to the originating country. The results were surprising and we detail it in the following article. If you are a client and would like to know specific attack statistics, including the number and origin, we have that information for you. Please contact us with your request.

Server Attacks and Why Abuse Email Doesn't Work

Overwhelmed ISP's and useless reporting

As part of a Good Practices policy, each outside domain should have an Abuse Email address. This policy applies for Internet Service Providers (ISP's) and individual domains that have an email server. The structure is used for reporting multiple types of bad behavior, such as SPAM, unauthorized access, law enforcement requests, copyright infringements, etc. This policy sounds reasonable, until you try and report an infringement. Just out of curiosity, I ran a report on our email archive and found that we have reported what we call "internet bad players" 569 times to ISP's on our customer's behalf. I can count on one hand the number of people who actually communicated with me or responded that they had fixed a problem.

For the month of October 2010 we started reviewing the logs for offenders attempting unauthorized access to our client servers and the ArchTech servers. In one month the total reached 142,071 attempts to compromise security. That is 142,071 separate logon attempts. Some of these attempts were to our smaller clients on DSL which essentially shut them down for the period. The count is lower than it would be due to our intervention in blocking traffic at customer firewalls which artificially lowered the

unauthorized access attempts. Our policy of the same IP address making more than one day's attempt on the client server was enough to get that IP banned at the firewall.

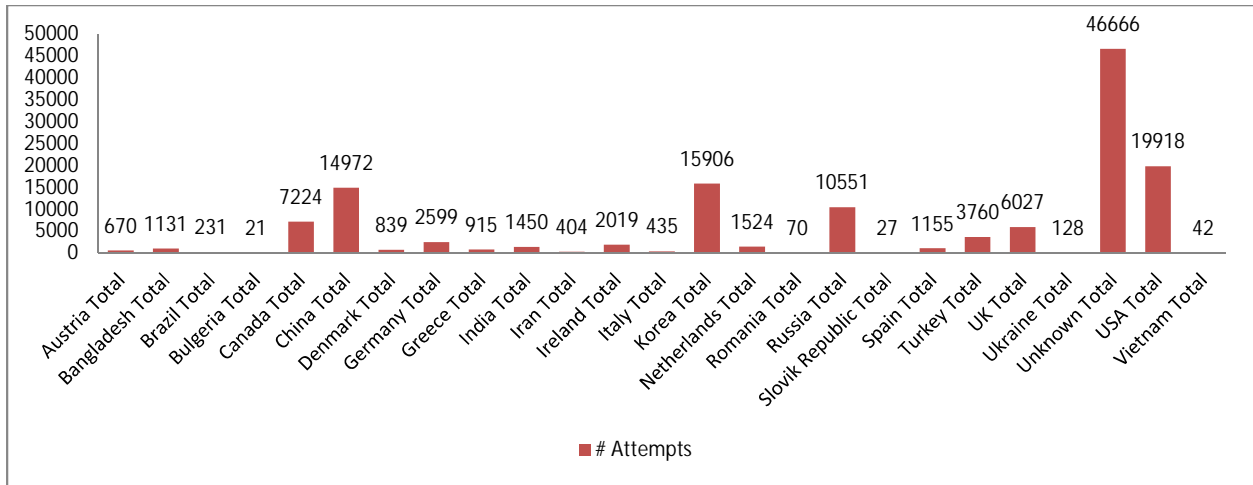
Anatomy of an attack on your server

We observed a couple of different patterns in our review. If you were a client on Comcast and we saw an unauthorized attempt, we would most likely find that IP on another Comcast client by the end of that day's review; same of Cablevision, FIOS and DSL customers. Basically, these are automated attacks that are running the list of published IP addresses and seeing who responds. We have always placed access schedules in customer firewalls (blocking access between midnight and 6 a.m.) so we started wondering how they knew to attack the server when the firewall was already in "stealth mode." We dug deeper and found a single attempt during the business day and then the attack would take place that evening. On some of our clients we found the offending IP in the web page logs (where we host the web site) and then we saw the server attempt. This was especially apparent in the non-profits we support where we would see foreign IP addresses looking at the web site and then thousands of break-in attempts that evening. The thought process being that non-profits can't afford security in the same way that business concerns can.

We are always asked "why would someone want to get into our server?" There are many reasons, such as identity theft, making the server a Spam Bot using your IP and good name to spam the world, credit card theft...the list is endless. The attack is normally a "brute force" dictionary attack. When we review the logs we will find user names such as Webmaster, Sales, Manager, Administrator, Accounting, etc. Then we will see all common first names. The password attempts can't be seen from the logs but they follow the names and then normally start a number substitution for letters, then date substitution trying to get those birthday passwords. If you don't think this works, I would like all of our customers to think about how many passwords we have broken on your behalf in the last 4 years. Word, Excel, Quicken, QuickBooks, PDF, your PC logon, etc all through programmatic or brute force attacks.

Who is attacking your business?

Please look at the chart for the list of countries we found attacking in October, 2010.



Please note all of these attacks were recorded on servers running Microsoft Server 2003. Our clients running Server 2008 and requiring certificates to log on do not respond to these types of attacks.

The unknown line was the most disturbing. These attacks came in with 0.0.0.0 as an IP address or nothing at all. These are the more serious attacks and they are essentially untraceable. I was surprised at the country results. A few years ago we saw many more attacks from the Eastern bloc countries or Russia. This report shows USA, Korea and China have now surpassed those attempts. Of course, the unknown attempts can't be categorized so they skew the country totals.

What happens when you are attacked?

These programmatic attacks depend on the frequency of the attack. When we audit a client from the outside, our programs allow us to set the frequency of logon attempts. These operate the same way. We saw multiple attempts per second and we saw one attempt every 3 seconds and even one attempt every 5 seconds. Since we are in the small-to-medium business space most of our clients do not have intrusion protection systems or high-end firewalls that trap these IP's and shut them down automatically. For most clients these devices would cost as much or more than the servers they use to operate their business. The attacks look like any other remote logon. Almost all of our small business clients have remote employees and require this access to be open for their use. That remote access is what is exploited for the attack.

The server records each of these failed logon attempts in the security log. That log is reviewed for our retained clients on a daily basis. When the attempts are egregious we save the log in case we require it for future action. Now we have seen the attack and track the IP (if available) to an ISP. This is where the process fails.

Each ISP has their own abuse policy, making reporting difficult but not impossible. The process starts by sending an email to their abuse email address. This will be responded to 99.99% of the time with an automated email requesting more information. Although some ISP's, such as, AT&T, Time Warner, Comcast and Cablevision are reputable and have network operation center teams, some are fly-by-night outfits or overseas operations that may or may not be complicit in the attack. The majority of ISPs have an innocent until proven guilty policy. They want you to do all the leg work to prove them guilty. This is

useless. As a policy we will not send security logs or identifiable information to any ISP. When we report on your behalf, we specify the time, the date, the number of attempts, the source port and the receiving port. That is enough information to review a bad player and track it to the source. If we see that IP come up again, attacking the same server we reprogram the firewall to block the IP. There is a very good chance that the offending IP will come up again in another attack and we record them all and can search the IP address to see if this is the case. We will then program all of the customer firewalls on the attacked ISP (Comcast, Cablevision, etc.) to block that IP.

Occasionally we will be good internet citizens and assist offending companies. During the month of October we reached out to two businesses that didn't know they were infected and informed them directly by speaking to their IT teams. This is normally more effective than reporting them to their ISP and the problem is normally gone in a day or so. In October we also reached out to the Supreme Court system of Florida, informing them their systems were attacking client servers. Considering every court case involving an individual has a Social Security number on file, I would not want to be listed in their computer systems.

The other case was an ISP in the southern US that handles school districts. We traced the attack to a high school and notified the ISP. To our surprise we received a phone call and they were very helpful. What we found out later is they were also powerless to stop it as each school had separate support groups and this group was incapable of fixing the issue. At the end of the month, we still saw this IP attacking our clients and was forced to do something we don't like do, we contacted CERT.

US-CERT – Computer Emergency Response Team

CERT was originally formed as part of Carnegie Mellon University in 1988 in response to one of the first computer worms. Since that time it has been rolled into Home Land Security's National Cyber Security Division. There are over 250 organizations that contain CERT in their name and function. The Home Land Security CERT will coordinate with state governments, private, and academic organizations in performing its function. We became aware of CERT while working for Wall Street firms while securing critical infrastructures.

When we email an attacking host IP to CERT we normally do not receive a response to the email. What we do see is that within 24 hours the IP is removed from the internet. It is just gone. For a small business that is not properly secured that is a death sentence which is why we reserve contacting CERT for only the worst offenders. However, as you can see from the chart, when we have attacking IPs traced to Iran, Turkey, Russia and China we have no problem with informing CERT there is an attack from an offending IP.

Conclusion

Someone is after your server on a daily basis. It happens every single day and normally intensifies on weekends when they believe there is less coverage. These attacks impact your bandwidth and server performance. Of the 142,071 October attempts to break in, none were successful.

We cannot stop people from trying to break in to your server. The trend of our client base has been to ask us to lighten up on security over time. This is not recommended. We have been asked to lengthen the time between password changes and to shorten the password lengths. I hope this report helps explain our reluctance to reduce any security.

Contact us

Please contact us to discuss your security requirements. We can be reached on the web at Info@archimedestech.com or at 973-845-6027.

If you would prefer not to receive mail from Archimedes Technologies, LLC please click here and send the mail. [Remove Me](#).