November 2016

TechTidbit.com

brought to you by Tech Experts

DDoS Becomes A 1 Terabit Phenomenon

Back in the middle of September, some amazingly terrifying things were happening in the world of technology. A DDoS (Distributed Denial of Service) attack reached a mind-boggling 1.1 Terabits per second. Not all users are familiar with DDoS attacks, but we'll explain how it scales to give perspective, why it affects smaller businesses, and how you can protect yourself.

First, what is a DDoS and why does it matter? A DDoS attack consists of many compromised devices targeting a single system. The compromised devices target the system by attempting to overwhelm an online service.

Once it is successfully overwhelmed, it can be temporarily unavailable or crash completely. There is generally not any irreparable damage to the system itself, but data that is mid-transfer can become corrupted and the system can become unresponsive preventing you from accessing it for work.

Secondly, we generally do not think in Terabits. People on a day-to-day basis are generally dealing with Kilobits and Megabits (which is 1000 Kilobits). When you download a file, you are likely doing it between 10-20 Megabits. This means that this new DDoS attack is 50,000 to 100,000 times faster than your average computer. These numbers are achieved by creating a series of compromised devices acting under singular actions, also known as a botnet.

Chances are, you have never been the victim of a DDoS attack. Unfortunately, that may change. In recent years, attacks on small businesses have increased substantially and the damaging potential has increased over time.

Part of the rise of DDoS attacks is the availability of easy-to-use tools off of disreputable markets and websites. With less skill needed to participate, more people can begin creating DDoS attacks.

So what can you do if someone decides to bombard you with a 1 Terabit attack? At that point, wait for it to end. Realistically, no one with that kind of botnet is going to attack a smaller business unless they have a personal vendetta against you.

More likely is a much smaller DDoS attack, something in the realm of sub-100 Gigabit attacks. But what can you do to defend yourself? Well, you might already be on the right track to preventing attacks not only to your business, but others as well. The main way smaller attackers are making a big impact is based on an open DNS resolver.

Now, what's an open DNS resolver? More or less, it is an error. A DNS can be open or closed; an open DNS resolver allows traffic and requests from any Internet source while a closed DNS limits who can use it. Using open DNS's, people can bounce off of open resolvers for both a larger attack as well as anonymity. How can you fix this? Most DNS clients are open by default, so make sure that when you set one up, you close it. When an attack does hit, it will generally give you an IP. Make sure to check out which DNS resolver it is coming from and to update the settings.

In the end, all you can do is make sure that your infrastructure is set up in a way that protects your data from a DDoS attack. Double-check your DNS resolvers to make sure they are not open, keep up to date backups available in case of the worst, and inform law enforcement when it does happen so that they may be able to track down the culprits and put an end to their childish games.

Chances are, you have never been the victim of a DDoS attack. Unfortunately, that may change. In recent years, attacks on small businesses have increased substantially and the damaging potential has increased over time.

Mistakes To Avoid When Setting Up Your Small Business Network

"Good management of your networking equipment will keep your network secure. Poor management can lead to vulnerabilities in the network due to a lack of updates and a lack of securing ports, leading to possible intrusion from hackers."

Anthony Glover is a Senior Network Engineer and Service Manager at Tech Experts.

Setting up your ideal network environment can be tricky. Here are a few things to avoid when setting up your network at your small business.

Lack of security on your network

Avoid this at all costs. A secure network is a happy network and, not to mention, a reliable one. This is especially needed if your business depends on confidentiality.

Lack of security leaves you vulnerable to hackers or curious individuals that could obtain information that could be vital to your business.

Ideally, a firewall is an essential choice when security is a factor in your networking environment.

Insecure wireless networking

A wireless connection is a convenient way for wireless devices such as printers, phones, laptops, or any other device that has wireless capability to connect to your network.

However, the convenience factor can turn problematic if left insecure.

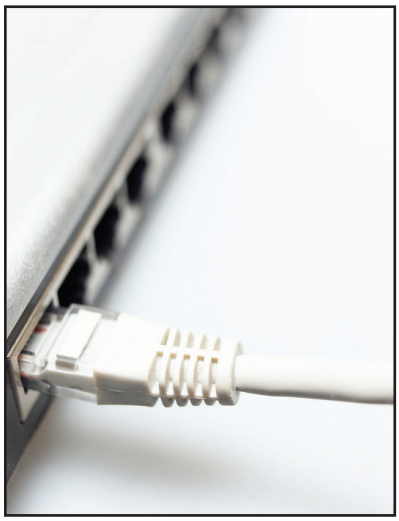
When it comes to wireless networking as a security factor, always set a password on your SSID (such as WPSK or WPSK2). Your password should – at the very least – include a capital letter, numbers, and special characters such as "!".

Poor network management

Poor network management is a much overlooked problem and can quickly become the worst thing that could happen to any small business network.

Good management of your networking equipment will keep your network secure. Poor management can lead to vulnerabilities in the network due to a lack of updates and a lack of securing ports, leading to possible intrusion from hackers.

Remember, all aspects of management are very important. This can include detailed and organized cabling, updating firewall firmware, updating servers and workstations, and securing ports on your server or end-user computers.



Network management – when done right - is ideal for your small business network and should be done by an IT professional such as Tech Experts.

Bad placement of Wi-Fi access points

Bad placement of a WAP can be a huge problem for wireless network signal performance. Poor signal strength can cause slow connections to both the Internet and your local area network and causes sluggish performance of your overall network.

It isn't enough to simply choose the strongest WAP; it also needs to be placed where it can work properly.

To make sure you get the best performance out of it, it should be located in the center of the area you need to cover.

You should also keep in mind that the weakest signal points are directly below and above your WAP.

Cutting corners on speed

Buying a 10 mbps switch just because it's on sale is a bad idea. Speed is your friend, especially when setting up your small business network.

A faster network will increase activity and save you time and money in the long run. 1 gbps equipment should be the ideal solution to not only transfer traffic faster, but access everything on your network faster.

We know networks aren't easy as pie, which is why we always recommend having a professional IT team set up your office.

Cheaper isn't better, especially when a poorly done set-up can cause large problems once you're operating.

If you're looking to set up a new building or relocate (or even redo your current office), give us a call at (734) 457-5000, or email at info@mytechexperts.com, to see what we can do for you.

Five Signs That You Need A New Work Computer

Luke Gruden is a Help Desk Specialist at Tech Experts.

A work computer is one of your greatest tools in the modern era. Like any other tool, you want to make sure you have the right one for the job – and that your tools are maintained and replaced if necessary.

Computers evolve and change faster than anything else and the demands of security and new software require that your computer be somewhat recent, not a museum piece.

The fastest way to tell if you need a new computer is if your computer boots up into Windows XP or to a Windows system older than 2000.

Windows XP is such old technology that Microsoft no longer provides security updates for it. This leaves XP computers vulnerable to security loopholes and hacking attempts. Even the most high-end computer from XP times would run very slow for modern programs, which often won't even load properly.

Google Chrome, the web browser, doesn't even run on an XP. If you boot up to a Windows XP, it is time to replace the computer. Windows Vista is your second sign that you might need to replace your computer soon.

The operating system is still receiving security updates from Microsoft, but not for much longer: April 11, 2017 is the last day of support for Vista. Windows Vista will be over 10 years old, which is about 90 years old in computer years.

In the computer world, we have Moore's Law, which means that roughly about every 2 years we're able to double processing power for about the same cost. After 10 years, a computer that would have cost $300 will not run at even a tenth of the speed of a modern computer of the same cost. It is about time to replace that Vista computer; if not this year, then definitely next year.

You might have noticed on different versions of Windows that it says 32-bit or 64-bit at the end of its title. This is important. A 32-bit OS cannot properly utilize newer computers. Without getting too technical: if your computer cannot support a 64-bit operating system, this is a good sign that you might need to replace your computer soon. Having a 32-bit OS is your third sign that you might need to replace your computer.

The fourth sign is if your computer came with a CRT monitor when it was new. A CRT monitor is an older monitor that is big and bulky with a square display instead of a widescreen display like all modern TVs and monitors.

If your computer came with a CRT monitor, replace this computer immediately. This computer will not run many modern applications. It may not even run basic websites that are out there today, let alone modern computer programs.

The last sign is that you're asking this question about your current computer. Chances are, if your computer is 4 to 6 years old, it could be time to replace your computer if you need to run modern applications. If 10 years is 90 in computer years, then 6 years old is getting up there in age.

If you are still questioning if it's a good idea to replace your computer, give Tech Experts a call. Once learn more about your particular situation, we can help you figure out if your current computer suits your work needs or if you should take the plunge to upgrade.

"In the computer world, we have Moore's Law, which means that roughly about every 2 years we're able to double processing power for about the same cost. After 10 years, a computer that would have cost $300 will not run at even a tenth of the speed of a modern computer of the same cost."

Create new service requests, check ticket status, and review invoices in our client portal: http://www.TechSupportRequest.com

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

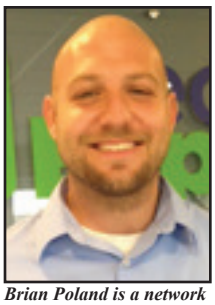
Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

To Firewall, Or Not To Firewall, That Is The Question



Brian Poland is a network engineer at Tech Experts.

When operating a small business, there are many things to consider regarding your communication. Whether it's within the office or to the outside world, efficient and secure communication is a key component to running a business effectively.

There's also the issue of transferring data, which can be considered the biggest aspect concerning the communication needs of your business. Internet and network security is a big topic these days, with all the changes inherent with technology, and all the vulnerabilities popping up all over the place.

Just last year, it was figured that roughly a million new viruses, spyware, and other malware created each day. Yes, a MILLON PER DAY. After that sinks in, consider this: it only takes roughly 82 seconds for sensitive data to be hacked, duplicated, and dispersed to the world at large.

Last year, 5 out of 6 companies were targeted by some piece of malicious software. Most of the new threats are things like digital extortion, sophisticated breaching attacks, and social media hacks.

A firewall is a good way to protect yourself and your company against an attack. A firewall is either a physical box or a piece of software that provides protection. They update on a regular basis to combat against the biggest and baddest hacker software out there. Even if they can't update quite fast enough, it's much better than just leaving your network unprotected.

The first, and simplest method, is to make use of the firewall that comes with your operating system. This is typically the built-in Windows Firewall.

This firewall is commonly used and is usually a good idea for a very small company. It's perfect for an organization with low traffic and not much sensitive data (such as credit card data, social security numbers, addresses, and other personal data).

A physical firewall is a better choice for bigger, more established business with a need for robust and reliable security. Don't get me wrong; even if you have a smaller business with little data transfer and communication, a physical firewall is always a good way to go. But you should really use a cost-benefit analysis to determine whether it's really worth going through the extra steps and money it would take to implement a solution like this.

Physical firewalls can be looked at like something that separates the outside world from your internal network.

They are robust, they provide an added layer of security, and you get what you pay for. It is always recommended that you use a physical firewall.

The downside of this, however, is two-fold. First, and most obvious, you have to splurge a little to get a decent solution. Secondly, someone has to know how to install, configure, and maintain it. This is where Tech Experts comes in.

Once it's all said and done, if your security measures are in place, you can rest assured that your days will be less stressful. You'll be able to sleep at night knowing your data and other forms of communication are protected from the outside world.