September 2017

TechTidbit.com

brought to you by Tech Experts

Wiperware: New Malware That Shouldn't Be Taken Lightly

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Any business can be a target for hackers who use ransomware. However, in recent months, a major new threat has emerged.

The recent Petya attack was initially perceived to be another form of ransomware.

However, as the firms involved took stock in the aftermath of the events, it became apparent that the attack took the form of "wiperware," code that is designed to completely destroy the files stored on any system.

What is wiperware?

Wiperware is designed with one goal in mind: total destruction. The malware asks users to install a software update and then it immediately takes control of the device. Once it has gained admin access, it completely overwrites all files on the device and in some cases the entire network. Any attached storage is also vulnerable, including USB external drives, memory sticks and network shared drives.

While the motivations behind Petya remain unknown, what is abundantly clear is that wiperware is a threat that needs to be taken very seriously. Here are a couple of things you can do right now.

Maintain and segregate backups to stop malware spread

In the recent Petya ransomware attack, the hackers had no intention of stealing files; they simply wanted to cause destruction.

The best method by which you can safeguard against this is by having a full and comprehensive backup of all your files and systems. This backup needs to be segregated from the network. A backup and disaster recovery unit that takes frequent images of your server is ideal. These images should be uploaded to secure off-site storage.

Adopt a heuristic approach to malware detection

The antivirus software that the majority of SMBs use are rather backward looking; that is, they are only capable of stopping known malware and viruses.

Typically, software companies learn about new risks and issue updates as new threats emerge. Heuristic detection solutions are much more sophisticated. They test unknown commands in a virtual environment to determine the effects they would have on the systems.

When this approach is employed, it is often possible to identify and block previously unknown strains of malware, including wiperware.

It is no longer sufficient to simply have a backup and recovery plan in place. You should contemplate an attack that destroys all of your infrastructure, and plan around that.

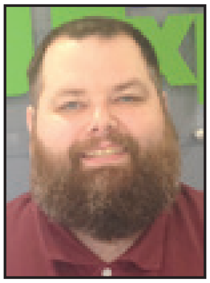
Given the rapid evolution of cyberattacks, it is critical that you proactively audit, update and test your defense and response mechanisms. ;

These activities should not be limited to business continuity plans but should also include ongoing employee education and training.

It is no longer sufficient to simply have a backup and recovery plan in place. You should contemplate an attack that destroys all of your infrastructure, and plan around that.

Do I Really Need A Firewall For My Business?

> *"Everyone who accesses the Internet needs a firewall of some kind. Without one, your computer will allow access to anyone who requests it and will open up your data to hackers more easily."*



Ron Cochran is a Field Service Engineer at Tech Experts.

Before we answer that, let's look at what a firewall actually is. No, no actual flames of any kind are involved whatsoever. A firewall is a barrier or "shield" intended to protect your PC, tablet, or phone from the data-based malware dangers that exist on the Internet.

Data is exchanged between your computer and servers and routers in cyberspace, and firewalls monitor this data (sent in packets) to check whether they're safe or not.

This is done by establishing whether the packets meet the rules that have been set up. Based on these rules, packets of data are accepted or rejected. While most operating systems (desktop and mobile) feature a basic built-in firewall, the best results can usually be gained from using a dedicated firewall application, unless you know how to set up the built-in firewall properly and have the time to do so.

Firewall applications in security suites feature a host of automated tools that use whitelisting to check which of your applications should accept and reject data from the Internet — something that most users might find far too time consuming to do manually.

So it makes sense, now that it's clear what a firewall is for, to have one installed and active. But just in case you're still doubtful of the benefits…

Everyone who accesses the Internet needs a firewall of some kind. Without one, your computer will allow access to anyone who requests it and will open up your data to hackers more easily.

The good news is that both Windows and Apple computers now come with built-in software firewalls (although the Mac's firewall is turned off by default). But businesses, especially those with multiple users or those that keep sensitive data, typically need firewalls that are more robust, more customizable, and offer better reporting than these consumer-grade alternatives.

Even a relatively small business engages in exponentially more interactions than an individual, with multiple users and workstations, and customers and suppliers. These days, most of those interactions are online and pose risks. Not only are businesses exposed to riskier online interactions, the potential damage from each interaction is also greater.

Businesses frequently keep everything from competitive bids and marketing plans to sensitive banking and customer data on their computers. When unprotected, the exposure is enormous.

Firewalls also allow computers outside of your network to securely connect to the servers that are inside your network. This is critical for employees who work remotely. It gives you the control to let the "good" connections in and keep the "bad" connections out.

Hardware firewalls must be compatible with your system and must be able to handle the throughput your business requires.

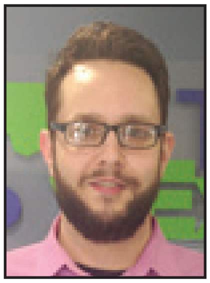
They must be configured properly or they won't work and can even stop your network from functioning entirely. You can use multiple hardware firewalls to take advantage of differing strengths and weaknesses.

Some industries (like medical and financial services) have specific regulatory requirements, so it's important to consult your IT professional before choosing a firewall to make sure you're not exposing your business to unnecessary liability.

It's also important for you, or your IT service company, to constantly monitor the firewall to ensure it is up and working, as well as to ensure that it is regularly updated with security patches and virus definitions.

If you currently are not protected by a firewall or would like to inquire about an upgrade to your network infrastructure, please feel free to email (info@mytechexperts.com) or call (734-457-5000).

VoIP Phones: Is It Time You Made The Switch?



Jason Cooley is a Network Technician at Tech Experts.

It's 2017 and, in case you didn't know, VoIP phone systems just keep getting better. Yes, the landline is losing ground to yet another competitor: VoIP. Cell phones have made home phones much less prominent, but for businesses, there is and likely always will be a need for dedicated multi-line phone systems.

What is VOIP?

For those less tech savvy folks out there, you may not have heard of a VoIP phone before. Even if you have, you may not know what it means. VoIP stands for "Voice over Internet Protocol." Very simply put: by using software or sometimes a physical converter, phone calls are made over the Internet.

Cell phones may be the reigning champion, but the need for dedicated phone systems will never go away. Many home users that do have home phones have VoIP and may not even know it.

If you are bundling phone service with your Internet and even cable television, then you most likely are using a VoIP system. In most home applications, it is common for your modem to have phone ports which can tie your existing phone jacks into the modem, allowing calls to be made.

For businesses, a VoIP system can be configured like you are used to. User extensions, call holds or parking, and line transfers – they're all there, including other features your business may find useful. Hold music, call directory, and even call recording are all easily put in place, too. There are many different solutions for businesses of different sizes, but the use of desktop multi-line phones works better for just about everyone.

Using a phone that connects directly to an Ethernet line provides great reliability. Most of these phones come with a second port allowing you to use your existing wired connection for your computer to connect the phone, which then sends the connection through to the computer.

This also allows for options of integration with your computer, such as software that can display incoming calls and outgoing calls, service queues, and the ability to call extensions or transfer calls with the click of your mouse.

So what's better about it?

There are a number of advantages to using a VoIP system. The call clarity is better. The quality is better. Conference calls are easier and more reliable.

The many features provided by using an Internet-based product are surely more than you'd think. There are so many things that make a VoIP system attractive, but none of those will speak to you like the sound of cutting your phone bill down by up to 40-50% a month. The number of simultaneous phone calls available to your business can be one of the biggest contributors to high costs.

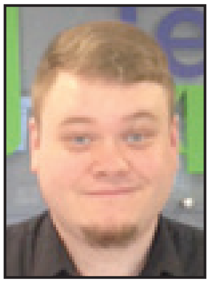
Long-distance on landlines can also add up whereas VoIP calling is cheaper per call than landlines, whether it's local or long-distance calling.

Many businesses can see phone bills over $2,000 a month with a traditional landline system. Imagine cutting that in half. That is $12,000 a year in savings versus landlines. Maybe you're a smaller business and have 10 employees. Your landline with multiple lines ringing in can cost you as much as $400 a month. Why not save yourself $2,400 a year?

Don't let the initial cost of potentially buying new phones scare you away. When you are saving 40% a month, you will recoup the initial investment faster than you think. After that, all you have to do is sit back and enjoy better quality, better clarity, and all that extra money in your pockets.

> *"The many features provided by using an Internet-based product are surely more than you'd think. There are so many things that make a VoIP system attractive, but none of those will speak to you like the sound of cutting your phone bill down by up to 40-50% a month."*

Helpful Tech Tips To Prevent Phishing



Jared Stemeye is a help desk specialist at Tech Experts.

Many of us have clicked on an email that appeared authentic, but was not. Those fortunate enough to identify any suspicious elements before an attachment is opened or a link is clicked are the lucky ones. But, sometimes, we don't notice those little things and click things we shouldn't.

These trick emails are one method of an effective scheme called phishing, run by cybercriminals to get information about you or your company. Even worse, this information is then bought and sold to the highest bidder to do with it as they wish.

At best, an ad agency might send some extra spam emails your way. At worst, your identity may be stolen or your company's network may be left exposed for all sorts of trouble. Fortunately, there are many things you and your workplace can do to avoid these phishing attempts.

Tips for employers

Just asking employees to watch out for suspicious-looking emails doesn't drive home the urgency of phishing.

Find recent news reports to share with your workforce. When an organization makes the front page for a data breach (usually because an employee opened an infected email), you can explain how something like that could happen to your organization. It's well-timed, newsworthy, and will be on forefront your employee's mind.

The best thing to do as an employer is to implement a program that encourages security awareness, education, and behavior modification. Changing up how you deliver that message to employees can be quite helpful. Start with a monthly email, memo, or bulletin.

Switch it up with in-person, individualized meetings. Using different approaches will help your message resonate with more employees. It is common to need to communicate a message multiple times for it to stick with everyone.

Tips for employees

Social media can be your worst enemy. Social networks are abundant with personal information, putting it right at the fingertips of cybercriminals.

Do not post any birthdays, addresses, or any other personal information on these websites. We know many domain and personal accounts use these for passwords despite the easy availability. Even with privacy settings maxed, there is always a way for cyber criminals to obtain the information.

Additionally, cybercriminals are getting more creative, especially with phone numbers. It is becoming very common for criminals to call high-risk employees and ask for information. For example, some of these "phishers" will call and pretend they are from their company's help desk and need to reset account credentials or "require verification" from the user.

When in doubt, don't give anything out. If something seems off or you don't know the person, ask for their contact information and look into it. In these cases, it's better to be cautious than courteous.

Overall, phishing isn't going anywhere and it should be incorporated into all online security training for workplaces. As long as people use social networks and email continues to be a primary workplace communication channel, phishing will be a top choice for cybercriminal's data theft. You can always contact Tech Experts at (734) 457-5000 if you'd like an in-depth review of any suspicious email you may have received.

With most people working at home..
Office parties aren't the same...

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(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) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com