E-NEWS

www.E-Safetech.om | 1-412-944-2402 | © 2019 E-Safe Technologies All rights reserved.

May

2019

In this issue...

How to protect yourself from cryptojacking

Hackers use cryptojacking to mine cryptocurrencies, and this process can cause PCs to run below optimal speeds. If you have a relatively new computer but are experiencing performance problems after clicking a link or visiting a website, you might be a victim of cryptojacking. Here's what to do.

Hijacked hardware

Instead of paying for computing power themselves, hackers opt to secretly use thousands of compromised computers to generate cryptocurrency. They gain control of a victim's PC by using phishing emails to lure them into clicking on a link, which then runs malicious cryptomining programs on the computer. Any cryptocurrency produced then gets delivered to the hackers' private server.

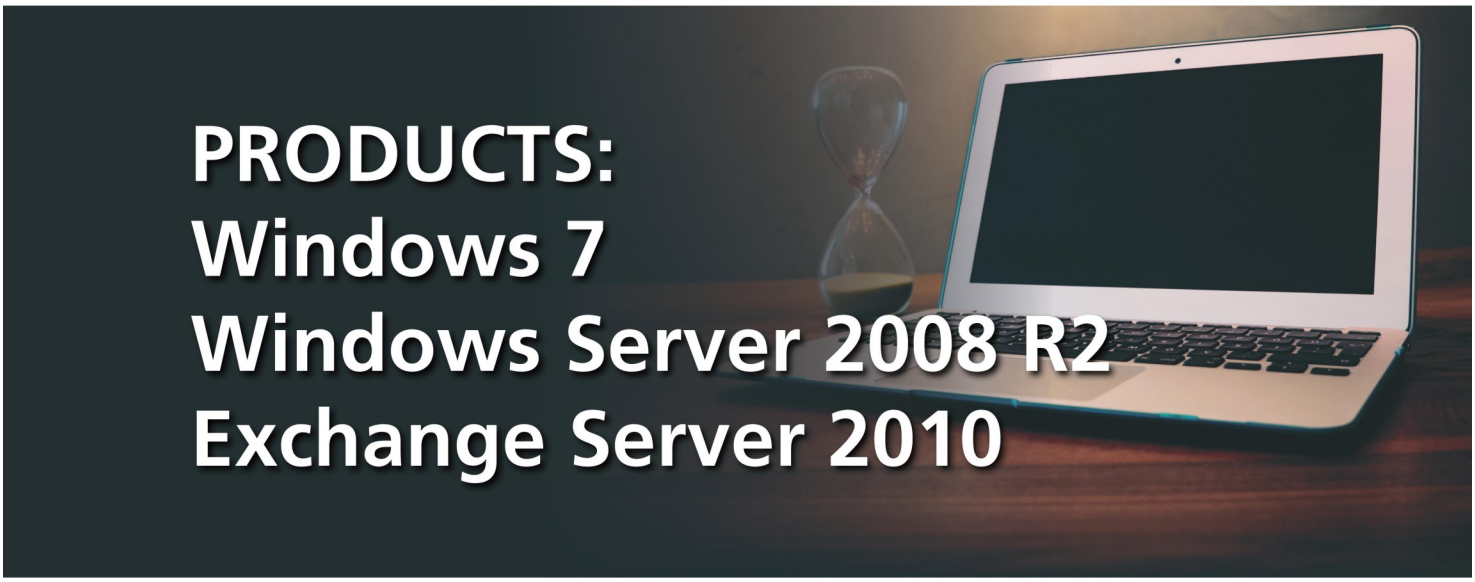
But wait, there's a more insidious tactic hackers use: infecting websites with ads and plugins that run cryptojacking code. By doing so, any visitor who loads the web page instantly gets infected with the malware, which sends their computer's processor into overdrive as it tries to generate cryptocurrency.

If there's a silver lining here, it's that cryptojacking software won't compromise your data unlike most malware do. However, it will hijack your hardware's processing power, so you'll experience decreased PC performance while your electricity bills increase.

Surge in cryptojacking

The biggest reason why cryptojacking is becoming so popular is that it's a low-risk, high-reward scheme. Instead of extorting money directly from the victim, hackers can secretly generate digital currencies without the victim knowing. And even if it's detected, it's almost impossible to track down who initiated the attack. was actually "stolen" (other than a portion of computing power), victims have little incentive to apprehend the culprit.

Microsoft Support End Of Life
January 14, 2020



END OF LIFE DANGERS:

- ✓ Security Vulnerabilities
- ✓ Software Incompatibility
- ✓ Compliance Issues
- ✓ High Operating Costs
- ✓ Poor Performance and Reliability
- ✓ Replacement Products Backorders

E-Safe is prepared and ready to help you transition to the latest operating systems and computers!!!

Stay ahead of the curve and contact us for a Microsoft End of Life Assessment to start planning your transition to avoid placing your business, users and customers at risk!

www.e-safetech.com

Moreover, since nothing was actually "stolen" (other than a portion of computing power), victims have little incentive to apprehend the culprit.

Cryptojacking is also a cheap investment. For as little as $30, anyone can purchase a cryptojacking kit from the dark web to force other computers to generate Bitcoin or Monero for them. And while it's difficult to tell how much exactly are hackers earning by cryptojacking, we can only surmise that it's more than the initial $30.

Because of these reasons, there's a good chance that this type of attack will be as popular as ransomware was in 2017. According to several reports, even sites like The Pirate Bay, Openload, and OnlineVideoConverter are allegedly using cryptojacking exploits to diversify their revenue streams.

Prevention and response

Prevention is always better than cure, so include cryptojacking in your monthly security training sessions. If employees practice extra caution in dealing with unsolicited emails and suspicious links, then hackers will have no way into your systems. Using ad-blocker or anti-cryptomining extensions on web browsers is also a great way to stay protected.

Beyond prevention, network monitoring solutions should also be used to detect any unusual computer behavior. For example, if you notice a significant number of PCs running slower than usual, assume that cryptojacking is taking place. And once it's confirmed, advise your staff to close browser tabs and update browser extensions as soon as possible.

Because cryptojacking doesn't steal data, it may seem less threatening than some malware, but in reality, its effects are just as severe — it can incur real power, cooling, and performance costs to your business when several systems are compromised. To make sure your business stays in top form (and that you don't end up enriching any hackers), contact us today. Our hardware solutions and cybersecurity tips will keep your business safe

Why it's costly not to virtualize

You've probably heard that virtualization saves money, but how can you take advantage of this? Did you know that choosing not to virtualize can hurt your business? Answer these four questions to discover why virtualization is good for you.

Studies have shown that over 70% of IT budgets go to "keeping the lights on." If that sounds like a lot of money, it is. You could be spending thousands of dollars powering your IT equipment and paying your staff to manage it, but it doesn't have to be that way. Virtualization can reduce your expenses without keeping you awake at night.

If you're ready to learn how, here are four questions you need to ask:

1. What's the cost of your data center?

We're talking about the whole kit and caboodle: your servers, backup power supplies, air conditioning, security devices, and the overhead costs for the space to store everything.

2. How much do you spend cooling your servers?

Keeping your servers cool is a fact of life. Have you ever considered how much this is costing you?

3. What is your budget for cabling and adapters?

Don't forget these. Aside from purchasing physical cables and adaptors, what's the cost of maintaining them?

4. How much does your IT staff spend to manage these resources?

It takes time for your staff to manage your IT, and time is money.

© 2019 E-Safe Technologies All rights reserved.

How does virtualization eliminate these costs? With virtualization, you can kiss the data center, servers, cables, and adapters goodbye (hello, new office space). Instead, equipment is stored off-site and delivered via the internet. Your computers and network continue to function normally. The only difference is they're out of sight. This equals lower maintenance costs, fewer overheads, less equipment, and fewer headaches.

And let's not forget the time it takes to manage all of your IT equipment. Virtualization frees up your IT staff, allowing them to focus on more important things, like your business's IT strategy and market. You may even have the option to completely eliminate your in-house IT staff. How's that for cost savings?

Ready to make the switch to virtualization? Need more questions answered? Let's talk.

Warning Signs Your Computer Has Malware

With the rise of eCommerce and online banking, cybercrime has evolved. Like criminals who pull smash-and-grab jobs, they go where the money is. However, unlike bank robbers, cybercriminals do their best to avoid detection by letting malware do the work for them. Viruses and ransomware sneak into PCs to quietly steal passwords, financial credentials, and other personal information to be sold on the black market for profit. Not all malware is stealthy though. Here are some telltale signs.

Slow computer

Are your operating systems and programs taking a while to start up? Is your data bandwidth suspiciously slow? If so, your computer may potentially have a virus.

However, just because your PC is running slower than usual doesn't necessarily mean that it's infected, as there could be other causes to your computer slowing down. First, check if you're running out of RAM. For Windows, open task manager (press Ctrl + Shift + Esc) and go to the Performance tab and check how many gigabytes of RAM are used up under the Memory section. For Mac OS users, you can open the Activity Monitor app and, under System Memory, you should be able to find out your RAM usage.

Other causes could include lack of space on your hard drive or even damaged hardware. Once you've ruled out other possible causes, then malware may have infected your device.

Blue screen of death (BSOD)

If your PC crashes regularly, it's usually either a technical problem with your system or a malware infection. You might not have installed the latest drivers for your device or the programs you're running could possibly be incompatible with your hardware. If none of these problems are apparent in your PC, then a virus could be clashing with other programs and causing your crashes.

© 2019 E-Safe Technologies All rights reserved.

To check what caused your last BSOD, go to Control Panel > System and Security > Administrative Tools > Event Viewer and select Windows Logs. Those marked with “error” are your recorded crashes. For trouble-shooting solutions, consult forums or your IT department to figure out what to do next.

Lack of storage space

There are several types of malware that can manipulate and corrupt the files saved on your computer. Most tend to fill up your hard drive with suspicious files. Ransomware, for example, is a notorious type of malware that denies you access to your data until you pay a so-called ransom. There are more aggressive forms of ransomware, like NotPetya, known for exploiting security holes to infect computers without needing to trick users.

If you find any unknown programs that you have never installed before, notify IT personnel in person immediately (do not email them) and have them handle the situation for you. Your device might not be the only one in your network that is infected with suspicious programs.

Suspicious modem and hard drive activity

Combined with the other warning signs, if your hard disk is working excessively while no programs are currently running or if you notice that your external modem is always lit, then you

Pop-ups, websites, toolbars, and other unwanted programs

Pop-ups come from clicking on suspicious pages, such as those where users are asked to answer survey questions to access a website’s service or install free applications. While they’re inherently harmless, they could be downright annoying. Refrain from clicking pop-up pages and just close them instead. Run malware scans and update your browsers.

You might think that downloading free applications is harmless, but the installation process can inject malware into your device. When you’re installing a program from the internet or even app stores, it’s easy to just skim over the terms and conditions page and repeatedly press next. This is where they get you. In the process of skipping over certain installation steps, you might have agreed to accepting a new default browser and opening unwanted websites and other programs filled with viruses. Be cautious when downloading something for free.

You’re sending out spam

If your friends are telling you that you’ve been sending them suspicious messages and links over social media or email, you might be a victim of spyware. Warn your friends not to open anything that appears to be spam and make sure to reset your passwords across all your devices and enable multifactor authentication.

Knowing how malicious software affects your computer can help you take the necessary precautions and steps to rectify the situation as soon as possible. Regardless of whether or not your system has experienced these symptoms, it’s always smart to perform regular malware scans to ensure your business is safe. To find out more about malware and IT security, contact us today.

© 2019 E-Safe Technologies All rights reserved.

The basics on 2-step and 2-factor authentication

Cybersecurity is a vital component to businesses these days. You need to make sure that criminals cannot just hack into your network. When it comes to verifying users' identity, there are two types of authentication used: two-step and two-factor. These two are so similar, many confuse one with the other. Learn the difference between the two, so you're more knowledgeable on keeping your network secure.

If you want to improve your business's cybersecurity for you and your customers, you should look at your authentication process. Two-step and two-factor authentication are two of the most commonly used options in cybersecurity. Many businesses use the terms two-step and two-factor authentication interchangeably. There are, however, subtle differences between the two.

Two-step authentication

A two-step authentication process requires a single-factor login (such as a password or biometric reading) as well as another similar type of login that is essentially sent to the user. For example, you may have a password for your first step and then receive a one-time-use code on your cell phone as the second step.

Two-step authentication adds an extra step in the verification process, making it more secure than single-step authentication (i.e., just the password). However, if a person or business is hacked, it won't be enough to stop hackers from getting a hold of whatever they are looking for.

Two-factor authentication

On the other hand, there is two-factor authentication (sometimes referred to as multifactor authentication), which is significantly more secure. This type of authentication requires two different types of information to authenticate a user's identity. For example, it could be a combination of a fingerprint or retinal scan as well as a password or passcode. Because the types of information are different, it would require a hacker a great deal more effort to obtain both forms of authentication.

The difference between the two

In essence, every two-factor authentication is a two-step authentication process, but the opposite is not true. With this information in mind, make sure that you are using the right type of authentication in your business to keep your company and customer information as secure as possible.

Your network needs the best security technology has to offer. The type of authentication you should use is just one of hundreds of choices that must be made to achieve that end. To take the stress out of securing and protecting your network, call us today for all the help you could ever ask for.

© 2019 E-Safe Technologies All rights reserved.