VantagePoint
EMPLOYEE OWNED

SEPTEMBER 15, 2020

VPS Article

Your Computer May Be More Valuable to an Attacker than You Think

JOHN STREFF, IT SECURITY SPECIALIST

We hear so much about data breaches and cyber attacks these days. Learning that hackers exposed millions of credit card numbers or other pieces of personal information seems to happen more and more. Even large companies with well-funded security such as Facebook, Microsoft, and Equifax suffer at the hands of malicious cyber attackers. Considering how these mega-companies make such high-value targets, you may wonder, “How does this affect me? Why do I need to care about cybersecurity? Why would an attacker want my computer? There is nothing of value on it, and I only use it for email, social media, and occasional online purchases.” What many people forget is that hackers are not only dangerous because of what they can take from you, but also because of what they can give you. While it may be true that your personal computer does not store millions of credit card numbers, your PC still has potentially tremendous value to an attacker. You need to care about cybersecurity. So, what can an attacker do with your computer? Let’s look at some of the major reasons for which an attacker may want your computer.

If you have saved your email password to your computer so you don’t have to type it every time you log in, attackers may be able to access your email account. They could read your emails. They could even send emails in your name to wreak havoc in your life or damage your reputation. They could obtain the contact information of your friends and family. With access to your email, it would also be possible to reset the passwords of any online accounts that you have set up with that email address using the “Forgot my Password” button on a website’s login page. Access to your email provides wildcard access to most of your online accounts. Consider what these other online accounts are. Someone with access to your Amazon account could probably make purchases using the credit cards you have saved in your account. Think of the damage an attacker could do to your personal and professional reputation with access to your Facebook, Twitter, and LinkedIn accounts.

A hacked computer is also dangerous because it may allow attackers to access your computer’s webcam and microphone. Attackers could potentially take pictures of you without your knowledge. If the images captured were of a private nature, they could blackmail you. For this reason, it is always a good idea to keep your webcam covered when not in use.

With access to your computer, attackers could also install malware (malicious software) capable of encrypting all your files and making them unusable until you pay a price to have the files decrypted. This is commonly called ransomware as the attackers hold your computer for ransom. Even if you don’t have anything of value on your computer that you are afraid of losing, there is still danger. Some malware can spread from one computer to another on a network. Other computers on the network may contain important files that must remain safe.

As if all of this were not enough, an attacker could use your computer to host a malicious website that infects the computers of all who visit that site with malware. Your computer could spread malware all over the world without your knowledge! An attacker could even place illegal content such as child pornography on this website, and you are legally responsible for your computer's contents. An attacker could also use your computer's processing power to send spam emails all around the world. These emails may contain attached malware or links to malicious, malware-hosting websites. An attacker could also install malware that joins your computer to thousands or millions of other hacked computers around the world to form a "botnet," which is an army of compromised computers. This botnet could collectively overwhelm a target website (such as Amazon) and cause it to crash. This is known as a distributed denial-of-service (DDoS) attack. An attacker could also use your hacked computer to generate revenue through cryptocurrency mining. Cryptocurrencies such as Bitcoin are completely digitized forms of money. Sometimes, attackers will try to induce people to visit websites that host pirated movies. While the victim is spending time watching the pirated movie, the website "hijacks" the victim's Internet browser and uses its processing power to mine cryptocurrency.

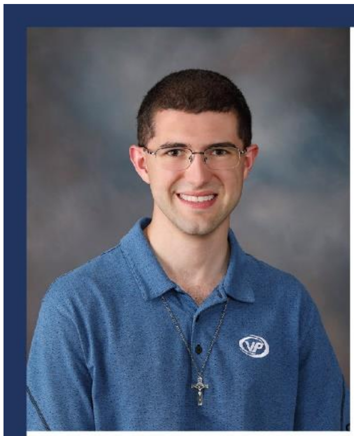
As you can see, a hacked computer is an asset to an attacker. Much more is at stake than your personal photos and text documents. Downloading and opening a malicious file or clicking a single link to a malicious website is enough to unleash the chaos described in the preceding paragraphs. There is, however, no reason to despair. You can take practical steps to protect yourself. First, be careful what you click on. Don't click on links or open attachments from emails you are not expecting. Verify the origin of the message. Hover your mouse over a link before clicking it to see where it will take you. If the site is unfamiliar or looks suspicious, do not click on the link. Second, do not use passwords. Instead, use passphrases! The length of a passphrase is far more important than the complexity. Often, websites will insist that you must use a certain number of uppercase letters, numbers, and special characters. The length, however, is far more important. Use at least 12 characters. An example of a good passphrase is "DeskComputerPhoneBottle20!" Third, apply updates when they become available, and do not repeatedly postpone them. Software vendors often release updates to fix critical security vulnerabilities. Fourth, use updated antivirus software. Fifth, Take regular backups of your important files in case of a ransomware attack. If you are the victim of ransomware, do not pay the ransom as this encourages the attackers. Simply reinstall everything on your computer and restore your important files from the backups. Sixth, keep your webcam covered when you are not using it. Seventh, monitor your financial accounts for suspicious activity. A good credit monitoring or credit freezing service can help with this. Finally, do not enter sensitive information such as credit card numbers into a form on a website that has HTTP in the address bar. Ensure that the site uses HTTPS, which means that your information will be encrypted when sent to the website.

Remember that even though you may not store millions of credit card numbers on your computer, you can still be a target. Recognizing that every computer has potential value to an attacker and taking the steps listed above will help you stay safe in the dangerous cyber world.

Additional Information

For more information or if you would like VPS guidance, please contact the Vantage Point Solutions banking team:

Kelly Pfeifer at (605) 995-1796, Kelly.Pfeifer@vantagepnt.com



John Streff

IT SECURITY SPECIALIST

As both a meticulous security analyst and a dedicated educator, John Streff brings tremendous strength to the Vantage Point IT Security Team. In his role as IT Security Specialist, he helps banks and credit unions secure their data networks through penetration testing, vulnerability management, policy, and other measures. Beyond technical mastery, John is especially strong at helping communicate the risks of cybersecurity breaches; and combined with his gift for training, this helps companies secure the human side of the organization – protecting entire teams and businesses from individual errors. He specializes in social engineering, security awareness training and publication, and malware analysis.

"I am passionate about security education and training because they provide a critical layer of protection for a client's cybersecurity by ensuring secure user practices."

EDUCATION

Bachelor of Science in Cyber Operations from Dakota State University, a Master of Science in Cyber Defense, and an Ethical Hacking Graduate Certificate

Kelly Pfeifer

CUSTOMER RELATIONS MANAGER

Kelly Pfeifer assumes a primary role as the problem solver for all client needs. He is committed to helping financial institutions deal with regulatory, network and security issues. Not only does Kelly provide a professional and helpful line of communication for the client, he also participates in social engineering testing. He is a master of disguise and an accomplished dumpster diver. His role as customer service manager is a central part of the financial services division at Vantage Point Solutions. Kelly double majored in Elementary Education and Business Finance at Dakota Wesleyan University. He began his career at Wells Fargo where he was twice named their top performer. He enjoys helping with Special Olympics and Junior Achievement. Kelly is also a Division I men's college basketball referee.

"I'm passionate about developing relationships because that's how I get to know the clients' priorities."

EDUCATION

Elementary Education and Business Finance at Dakota Wesleyan University