Ransomware

With many of our clients working from home, hackers are finding easy targets for their malicious mischief. This is because most home networks and devices are not as secure as those at work, making the home user easy prey for the bad guys. In this article we'll take a look at one of the most insidious and harmful things that can happen to any user – catching a ransomware virus.

Recently TekResults was asked to help a multi-national company recover from a ransomware attack. The attack had encrypted files on their servers across the globe and had ground their company to a halt.

Sadly, this was not the first time we were called upon to help recover from a ransomware attack. The WannaCry virus (represented in the screen shot above) infected several Centre County networks a year ago and those companies required our assistance to mitigate the damage.

What is ransomware

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

How ransomware works

There are a number of vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they're downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

There are several things the malware might do once it's taken over the victim's computer, but by far the most common action is to encrypt some or all the user's files. The files cannot be decrypted without a mathematical key known only by the attacker. The user is presented with a message explaining that their files are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker.

Who is a target for ransomware?

There are several different ways attackers choose the organizations they target with ransomware. Sometimes it's a matter of opportunity: for instance, attackers might target universities because they tend to have smaller security teams and a disparate user base that does a lot of file sharing, making it easier to penetrate their defenses.

On the other hand, some organizations are tempting targets because they seem more likely to pay a ransom quickly. For instance, government agencies or medical facilities often need immediate access to their files. Law firms and other organizations with sensitive data may be willing to pay to keep news of a compromise quiet. But don't feel like you're safe if you don't fit these categories: as we noted, some ransomware spreads automatically and indiscriminately across the internet.

How to prevent ransomware

There are several defensive steps you can take to prevent ransomware infection. These steps are good security practices in general, so following them improves your defenses from all sorts of attacks:

- Keep your operating system patched and up to date to ensure you have fewer vulnerabilities to exploit. Note, if you are still using Window7, you ARE vulnerable! You should upgrade to Windows 10 right away.
- Don't install software or give it administrative privileges unless you know exactly what it is and what it does.

- Install antivirus software, which detects malicious programs like ransomware as they arrive, and whitelisting software, which prevents unauthorized applications from executing in the first place. TekResults can recommend an excellent antivirus solution. Give us a call to discuss (814-206-0000 option 1).
- And, of course, back up your files, frequently and automatically! That won't stop a malware attack, but it can make the damage caused by one much less significant.
- In our most recent encounter with ransomware, recovery was very difficult because the hackers were able to work as domain administrators and were able to destroy shadow copies, backup catalogs and just about anything that would help in recovery.

We believe it is a very bad idea to give domain administrator rights to anyone but restricted administrator accounts that do not get email and do limited web surfing. We would be happy to access your company domain policies to see how receptive to an attack you may be.

Help! My files are encrypted!

If you are attacked, the first thing to do is disconnect your computer and any other device on the network, from the network… pull the network cable out of the back of the computer. Do the same for your servers. By the time you realize you have a virus, the damage may have already spread, but disconnecting the computers and servers from the network will keep the damage from spreading any further.

After that, install and run good antimalware software and scan the system to find the ransomware program.

These are good first measures, but they won't decrypt your files. Their transformation into unreadability has already happened, and if the malware is at all sophisticated, it will be mathematically impossible for anyone to decrypt them without access to the key that the attacker holds. In fact, by removing the malware, you've precluded the possibility of restoring your files by paying the attackers the ransom they've asked for.

The best practice to ensure you can recover most of your files without paying the ransom is to make sure your files are backed up every day. If there are backups of your files, your files can usually be recovered, but keep in mind that backups can't make something out of nothing. You can only recover the files that have already been backed up. If it is a week or more since your last backup, you won't be able to recover the past week.

If you have questions or a comment, or would like to engage our services, we are eager to hear from you.

Referrals

TekResults owes much of our success to our loyal and enthusiastic clients. It's those of you who tell your friends about us that keep our company growing, and we'd like to say thanks. Just telling someone about us is all it takes. Just let us know you dropped our name and we'll drop a gift card in the mail for you to enjoy a great meal at a Dante's restaurant. See… who said talk is cheap!

The TekResults Team
support@tekresults.com
814-206-0000 Option 1

Our Services and Products

- IT problem solving
- Office 365 sales and support
- Business phone systems (Comcast, VoIPLy, Vonage, Fortinet)
- Infrastructure design and implementation
- Pre-Sales consulting
- Capacity planning/ system design
- Network cabling
- Security compliance review HIPAA
- Security compliance review PCI
- System installations
- System upgrades
- System auditing / documentation
- Desktop, laptop and monitor and other sales
- Network administration
- Network troubleshooting
- Business consulting software testing and service
- 3rd party software setup and support
- Computer security solutions (including PGP, encrypted mail, secured transactions)
- Custom application development
- Legacy system migration and rewrites
- System integration
- Application integration
- Network installation and integration
- Training and staff development