VERSION 1.0

MAY 21, 2017

# RANSOMWARE, MALICIOUS CODE, HACKERS, VIRUSES & WHAT TO DO ABOUT IT

ISSUES, CONCERNS FOR THE HEALTH AND HUMAN SERVICES PRIVATE & PUBLIC SECTOR

PRESENTED BY: DAVID GUERRA
DAVEGUERRA.COM
PO BOX 3693 • EDINBURG, TX 78540

# RANSOMWARE, MALICIOUS CODE, HACKERS, VIRUSES & WHAT TO DO ABOUT IT

Recently, the issue of ransomware has reared its ugly head. The "WannaCry" attack on the British National Health System and other major organizations throughout the world have brought to light the vulnerability of Information Technology systems that are not up to date and the interruption in service that comes as result of not paying attention to the details.

## RANSOMWARE, MALICIOUS CODE, HACKERS, VIRUSES & WHAT TO DO ABOUT IT

Recently, the world experienced what I call the beginning of the shape of things to come. The "WannaCry" ransomware attack in England, especially the attack on the National Health System's computer and telephone systems. With operations rescheduled, no access to patient records, and telephone system outages everyone with a splinter between their toes to tumor removal surgery was affected. Why is this the shape of things to come? When one exploit is found and used to the advantage of the black hats, you can rest assured another exploit is just around the corner. This is where you and your organization must do what it takes to step up and stay ahead of the next exploit. Of course, a commitment from the PC manufacturer, Operating System (i.e., Windows, Linux) developers is nothing if you are not willing to do your part. How you and your organization handle the current state of affairs when it comes to protecting the most valuable asset you and your organization possess: information. Information of your clients and patients.

To begin protecting information vital to you, your organization, and your clients let us look at what happened. The "WannaCry" attack began when a flaw or exploit was discovered in an update package. The individual, individuals, or group behind the attack created the code behind the "WannaCry" malware and made with the help of spam email attached the code to a "click here" link and it was off to the races. In no time, some unsuspecting or untrained individual opened the email attachment, the code began wreaking havoc on computer networks and network connected PCs. Soon the data was encrypted and without the "unlock key" code the data was worthless. Of course, it is at this point that you will righteously proclaim that you "never click on any email attachments" and I can promise you that in England, many people said the exact same thing, yet here they are and here we are. The only way to recover the data was to pay the "ransom" and the "unlock key" would be provided to decrypt the data and things would be back to normal or so the end-users believed.

It is not always an attack by opening email attachments. Attacks can occur by visiting bad websites. A few years ago, a co-worker was looking for Narcotics Anonymous locations in the Dallas-Fort Worth area for a client. The top link in the Google listing, unbeknownst to the caseworker had been hacked. When she clicked on the link, the hijacked website then took her to another website that had not only inappropriate images on the page but a "CLICK HERE" to return to Google dot com button. When she clicked the return to Google button that was when the trouble began. She inadvertently caused her browser's home page to be hijacked to another inappropriate website. Thus, every time she opened the Internet browser that page loaded first. Luckily, for everyone she had the common sense to move to a different PC and do her work there. Unfortunately, this occurred on a Friday evening and I was not able to address it until Monday morning.

Now that is not all that can cause the spreading of malicious content. The use of portable hard drives and flash drives are other devices that can aid in the spreading of viruses and malware. Being diligent and ensuring that the portable devices you use are not infected is critical to preserving the integrity of the data on those devices as well as the data on the network or PC.

## WHY DO SUCH THINGS AS VIRUSES & RANSOMWARE OCCUR?

The answer varies. It varies as much as why there are so many shades of the color red. However, some are easy to explain. In the case of ransomware, the objective is money. Plain and simple, because data is priceless. Without data or information, we cannot do our job. In most cases, we cannot perform our assigned duties. Imagine the night before annual taxes are due and you have no W-2s or 1099s; you file for an extension and hope you can find your W-2s and 1099s before the six-month extension ends.

Hackers hack because they can and that is usually the reason they give when they are caught. As for viruses, the same reason applies as hackers because the coders/creator of the virus want to show the world what they can do. The reasons for other forms of computer attacks varies and no matter the reason, the outcome is always the same: inability to work because the data/information is NOT there. Does this mean that everyone has to be on their toes 24 hours a day? YES!

## WHAT IS AFFECTED?

In the case of the “WannaCry” ransomware attack, the data was encrypted. Thus, essentially you could say the entire hard drive was encrypted and the ransomware developers allowed on the necessary system functions to remain unencrypted so the ransom note could be delivered to the end-user. However, not all forms of attacks are that encompassing or engulfing, some attack specific file types such as Microsoft Word documents or files that have the .docx file extension or Excel spreadsheets with the .xlsx file extension. Then others just attack the main boot record (MBR) and create the end-user’s (your) inability to boot the device let alone log-in.

Then there is the worst attack of all, the one that erases all the contents off your system’s hard drive. Everyone that does not have a backup and recovery system in place fears this form of attack. Even those with a suitable backup system in place also fear the data loss because it will mean time devoted to recovery and not production. Personally, I would rejoice in knowing that I would only need to rebuild data that was lost since the last back up and not rebuilding my entire practice.

## WHAT TO DO ABOUT IT?

The most obvious is also the most difficult for some people: Stay Up-To-Date. By staying up to date with your operating system’s updates, software patches and most recent anti-virus definitions, you are less apt to fall victim to any type of attack including the ones you initiate yourself (i.e., clicking on email attachments or unknown links on the web).

Operating System (OS) updates come directly from the software company and never through email but through the OS itself in the case of Microsoft, through Windows Update app. The windows updates can be automated to do their bidding in the wee hours of the morning. By scheduling the updates, you can rest knowing your system will be up-to-date when you are ready to get to work, after that first cup of coffee, of course. If you are not having your Operating System updated on a normal schedule then be prepared to have it take over updating your system for up to two hours during the time you need it the most. Folks, this even applies to machines that you only use for a specific function. Do not be caught having a client wait for your PC to come back online.

Software patches are typically announced through the software in the CHECK FOR UPDATES link or my email notification (that is if you signed up for notifications). Some software packages will give you the option of updating automatically or to notify you when updates are ready such is the case with Adobe

Acrobat, Flash, and Air. Other software packages will give you other options. In all cases, I want to be notified when the options are ready. The trick is to allow the updates to occur and not ignore them as I do with the iTunes notifications.

When it comes to Anti-virus applications, I encourage everyone to have that set to automatically update your system. This ensures that I do not forget to click on the update now button and it ensure that I do not delay in patching an exploit that will cause me more heartache with lost, damaged, or corrupted data instead of losing a few minutes while the anti-virus package updates.

For those of you that work in public sector organizations, rest assured and have faith in your IT department. They are usually on top of things. Having multiple individuals address specific topics such as one group handles hardware issues and another handles software issues they are able to take a shotgun approach to resolving issues. This is the advantage you have when working with organizations that have an IT group versus those of you in private practice or working on your own. You are not only the President, CEO but you also have to be the Custodian, Gatekeeper, IT department and HR department.

## YOU CANNOT BE ALL THINGS TO ALL PEOPLE

However, you can try, especially when you are starting out. Unfortunately, when trouble strikes, you go into reactive mode and trouble strikes twice. In the case of ransomware, you want your data back and you pay the ransom. In the UK, the starting ransom was 300 British Pounds for single systems to be decrypted that comes out to just under $400 USD. Does not seem like a lot of money to get your data back, we have yet to hear if anyone that paid the monetary demand has had their data released. If you paid once, what is to stop them from asking for more? Think about it. They did it once. Who has ever heard of an ethical thief?

Still in reactive mode and after the attack has occurred, updating the PC, Laptop, or Tablet is akin to closing the stable door after the horses have left. It is too little too late and will do absolutely nothing to recovering the lost information. You have to let go of being REACTIVE to be thinking & living PROACTIVELY.

## TREAT YOUR DATA LIKE YOU TREAT YOUR CLIENTS

Just as you treat your clients in a manner to help them live a better future, you have to treat your Information Technology systems to protect your data for a long time to come. In addition, being proactive does NOT mean you make you technology decisions on what your friends say or the next-door neighbor's 12-year-old kid says. Unless your friend is an IT professional, please do not waste your time. As for the 12-year-old kid next door, when his Nintendo 3DS breaks or he cracks the screen on his iPad he or she has Mom and Dad to buy them another one. Will your Mom or Day buy you a new iPad? What is the ROI on their two cents?

Unfortunately, people very seldom seek out a professional, someone with more than a HS education or has taken a seminar on how to use Microsoft Word. A professional is someone who is out there being paid to protect your data. To ensure that you will not have to consider paying ransomware.

A word of advice when seeking out a TRUE IT PROFESSIONAL. Seek one that does not want to work with you for an extended amount of time. Someone that is a TRUE PROFESSIONAL will want to come in get the work done, train you, and get the heck out of dodge. Then if you have to call them back, it is to fine-tune the little things. Anyone that wants you to finance their kid's college education is NOT a True Professional and may do things to ensure they keep coming back. Caveat Emptor.

Have a recent backup of all your data at all times. Unfortunately, most people or small organizations that have backups are from the beginning. When the good intention was to start a data backup cycle and continue it for the life of the organization. However, as time passes and life happens the data backup cycle turns to the occasional backup then to the inevitable forgotten backup. If you are at the occasional backup, try to get back to a six month or three month plan as something is better than nothing.

Another possibility is that you can get with minimal effort a clone copy of your hard drive made. Once you learn how to do it, you can do it on your own. It involves a small device with two hard drives slots (one from your PC and the other is a blank hard drive) and with a button to initiate the duplication of the hard drive from your PC. Then once duplicated the once blank HDD is stored for future use (if needed). Then once a month or so the process is repeated. If you are ever attacked, you can swap out hard drives and you are back in business.

It does not matter what you choose to do please have a backup plan and use it.

## USE IT, DON'T IGNORE IT

When it comes to protecting information, you have to live by the following: It is not if an attack will occur but when will it occur. I guarantee the British National Health System was not thinking of an attack the day before the ransomware attack, yet it occurred. I guarantee you are not thinking of it either however; the writing is on the wall. It will happen again, however by taking the time to enable updates on your machines, having an installed and updated anti-virus application running, a decent data backup plan you will be ready to deal with the fallout and be back in business with minimal down time. As you deal with the future of your clients, you sometimes have to reach out to peers, colleagues and other professionals for guidance and assistance. It behooves you to reach out to professionals to help protect the future of your data and information. The information that is the basis of your livelihood. Remember being prepared for the worst and it never arrives is better than not being prepared at all when the worst does arrive.

## I HOPE THIS HELPS

Let me know by email: dave@daveguerra.com or Twitter: @daveguerra

Thank you

David Guerra, MBA
IT Professional with +25 years Real World Experience