# Monthly Newsletter



## In This Issue



### Website Links

- Cyber Security Page
- Ransomware Protection
- Ways to protect against Ransomware

### Ransomware News

- Methodist Hospital
- Police Departments
- Special Agent Bonavolonta

### Contact Us


Cyber Security Mobile Team

kirk.burns@dps.texas.gov


## Introduction


If you have been watching the news, you most likely have heard of the Ransomware (or Crypto-Ransomware) attacks that have hit hospitals, schools, businesses, government agencies, academic institutions, law enforcement agencies and individuals. Estimates from the FBI show Ransomware has reached an all-time high. Since the beginning of the year, 209 million dollars have been extorted by cyber-criminals. At this rate, Ransomware could easily be a 1 billion dollar crime before the end of the year. Reports show the number "is quite high" because a few organizations "reported large losses." However, it is believed that while high, these numbers could be far lower than actual values because some victims might have paid and decided, for various reasons, not to report the crime. (CNN article)

On Friday, March 18, the computer systems at Methodist Hospital in Henderson, KY were infected with Ransomware. The attack was so successful that it effectively shut down the hospital for five days and forced the hospital officials to declare an internal state of emergency. While the hospital claims to not have paid the ransom, other reports dispute that claim. A similar attack occurred against Hollywood Presbyterian Medical Center in Los Angeles. In this case the hospital administrators reportedly paid $17,000 in Bitcoins to restore their hospital system. The true amount is unknown since some sources report the amount paid was actually much higher.

Ransomware attacks on hospitals have been the main focus of the media. However, hospitals haven't been the only victims. School districts have also been victimized. The entire New Jersey school district was attacked with ransoms ranging from $500 to $124,000. Other public schools in Mississippi, Oklahoma, South Carolina, etc. have also been victims. Here in Texas, two school districts affecting twenty school campuses have fallen victim to crypto-ransomware.

Because of this significant and growing threat, this month's Newsletter will focus on Ransomware.

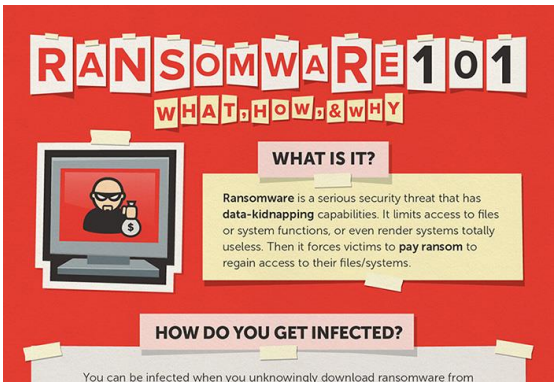
## What is Malware?

Before talking about Ransomware, it is important to have an understanding of Malware. Malware is a compound word derived from combining Malicious and Software. The word is an umbrella term used to describe several forms of hostile software. It can be thought of as the parent category with things like viruses, worms, Trojan horses, spyware, adware, scareware, ransomware, etc. being children. Malware comes in several forms. It can be executable code (.exe), scripts, active content (like in Word or PDF documents), or a variety of other ways. Malware has become an increasing problem for organizations as well as individuals. AV-TEST, an independent IT-Security firm, reports that as of 6 April 2016 that there were over 500 million different forms of Malware of which almost 40 million are new in this calendar year. https://www.av-test.org/en/statistics/malware/

# What is Ransomware?

Ransomware is a type of malware that restricts access to a computer system and demands the user pay a ransom in order to remove the restriction. Essentially it is the digital version of a hostage situation where files on the computer, or the computer itself, are the hostage.

The first instances of Ransomware occurred in 2005 in Russia and other parts of Eastern Europe. Shortly after, programs like Reveton, Cryptolocker and Hydracrypt started victimizing computers in the U.S. Reveton and Cryptolocker "lock" the computer and display an image supposedly from the FBI or Justice Department on the screen claiming that the computer had been involved in illegal online activity. Often these programs would turn on the webcam light to give the appearance the user was being monitored and threatened arrest if the ransom was not swiftly paid. Ransomware is difficult for the average user to remedy and scares many into paying the "fine" without even stopping to question if it is legitimate.




Ransomware has become a booming business. In September of last year, Symantec was able to gain access to CryptoDefense malware and got a glimpse of the hackers' haul based on transactions for two Bitcoin addresses the attackers used to receive ransoms. Out of 5,700 computers infected that day, about 3% of the victims appeared to pay the ransom. At an average of $200 per victim, Symantec estimated that the attackers hauled in at least $34,000 that day. Extrapolating from this, it is believed that CryptoDefense earns more than $394,000 a month. This is based on data from just one command server and two Bitcoin addresses; the attackers were likely using multiple servers and multiple Bitcoin addresses for their operation. http://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

Bitcoin has become the preferred payment method because it is a type of digital currency which uses encryption techniques to verify the transfer of funds. It operates independently of a central bank and is very difficult to track.

# What do I do if it hits me?

Joseph Bonavolonta, Assistant Special Agent in Charge of the FBI's Cyber and Counterintelligence Program in Boston, said "The ransomware is that good…To be honest, we often advise people just to pay the ransom."

Encrypted files are a very difficult thing to gain access to without the password. It is possible, but the encryption the cyber-criminals are using is so complex that it is highly unlikely that the average person or organization would be able to accomplish the task in a reasonable amount of time. That is why Agent Bonavolonta, and the FBI, gives this advice.

The best way to deal with Ransomware is to prepare for it before you become a victim. Things that can minimize the danger of becoming a victim and having to consider paying a ransom are:

- Regularly backup all critical files to a device that is then disconnected from all computers
- Keep your Operating System and all programs up to date
- Keep your anti-virus software up to date
- DO NOT click on suspicious emails
- Disable Remote Desktop Procedure (RDP) on your personal computer
- Educate yourself on best practices

Backing up your critical files is probably the single most important thing you can do to

protect yourself from being a victim of Ransomware. With a regular backup procedure in place, if you are a victim you shouldn't need to consider paying the ransom. All you need to do is delete the infected files, clean your computer of Malware, and then reload your saved files.

Only you can decide the correct course of action to take on your personal computer. But remember that even if you pay the ransom, there is no guarantee that you will have your files "released" or that you will not become a victim again. If your work computer becomes a hostage, follow the procedures you would for any Malware infection. Unplug the network line from your computer, disable the wireless card, and immediately notify the helpdesk.

## How do I protect myself and DPS?


It is impossible to completely prevent malware infection. However, it is possible to mitigate the chances of you or DPS being a victim. The first line of defense is to follow all policies and procedures. These policies and procedures are put in place to try to protect not only the agency but you as well. Be vigilant when opening any attachment sent to you via email, even if you believe it is from someone you know. If you didn't know the person was sending you that exact document, don't click on the attachment without first verifying the person did send it to you.

Currently the favored method of delivering Ransomware is via Macros. For those of you who don't know what Macros are, they are small programs that run inside other programs like Word and Excel. Macros are intended to increase work efficiency by automating repetitive tasks or keystrokes in the Macro enabled program. However, just like with anything, Macros can be used maliciously.

Because of this danger, DPS has developed a plan that will go into effect on July 1, 2016. That plan is to disable all Macros that haven't first gone through a Cyber Security code audit process. What this means is that departments who use Macros need to have **the owner of the Macro** send it to our division (Cyber Security) for a review and signing process. Once we have reviewed the Macro to verify it isn't doing something that could endanger the agency, it will be "signed" and returned to the owner. The owner can then distribute the Macro to other people in DPS and the Macro will work. Any Macro that has not gone through the audit process prior to July 1 will stop working on that date.

## For More Information

For information, tutorials and contact information about this month's topics, you can click the links on the side of the newsletter. For other Cyber Security news, please visit the Cyber Security website. Remember that security is a shared responsibility and,

"**Do Good Cyber**".

## Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has a BS in Criminal Justice, a BS in Computer Science, and an MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University with over 16 years of IT experience. Kirk serves as a member of the Texas Army National Guard and holds a current CISSP certification.

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He is happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.