**Ransomware: Understanding the Threat and Exploring the Solution**
Senate Judiciary Committee Subcommittee on Crime and Terrorism

**Charles C. Hucks, Jr.**
Executive Director of Technology
Horry County Schools
18 May 2016

February 8, 2016 started as just another Monday in Horry County Schools (HCS)—the sun was shining, our 43,000 students and 3,800 faculty and staff were returning for another week of world-class learning and teaching in coastal South Carolina. Little did we know that one of the most disruptive events in recent history was already well underway throughout our district.

The first indication something was awry was a call from one of our teachers informing the Help Desk she could access none of her documents and presentations and that all now had a funny filename extension of *.encryptedRSA*, or something like that. Given the current state of the online world this sadly was *not* the first time one of our users called to report such an event, a case of *rasomware*. *Ransomware* is a type of malicious, unwanted application that installs itself on a computer for (generally) the sole purpose of holding all the data—documents, presentations, spreadsheets, pictures, etc.—hostage until a ransom is paid for its release. This is accomplished by the encryption, or locking, of files with sophisticated mathematical algorithms that are, if implemented correctly, virtually impossible to crack without the corresponding key—a key which is only receive by paying the ransom.

Occurrences of ransomware at HCS up to this point were limited in scope and impacted a single user or at most a single school. Our backups are generally thorough and previous events were typically resolved by restoration of impacted files for the given user or school from backup. This process certainly took time and resources away from more important work but files were usually back online within a few hours and without paying the ransom for release, so while this first call was not good news it was not seen as a major event.

Within a matter of minutes another call from another school with the same problem was received, then another—and it became terrifyingly clear what was happening—we had been hit by a ransomware attack and *this time it was spreading like wildfire throughout our 52 schools, central offices and hundreds of servers.* This was orders of magnitude worse than anything seen before and the decision was made to *immediately* shut down *all* of the servers throughout the entire district in an attempt to stop the spread and encryption of files as quickly as possible.

Most organizations today are highly dependent on technology for daily operations and our schools are no exception. All teachers are provided, at a minimum, a laptop, all students in grades 5-8 are provided an iPad, all students in grades 9-12 are provided a Dell Windows-based tablet with keyboard, and students in other grades have access to a variety of shared computing resources. Administrators and teachers take full advantage of these resources to design, plan and implement teaching strategies and lesson plans that provide individualized learning opportunities and 21st century skills that are only possible through the efficient and effective application of technology into all aspects of the instructional day. When the decision was made to shut down *all servers district-wide* all of these devices became isolated islands with no ability to communicate with each other or the outside world. Access to email, social and instructional media, online digital content and instruction, collaboration, assessment tools, and network and cloud-based storage was lost.

A report to the computer crimes division of the FBI was created and the incident was reported immediately to the local FBI field office, SC SLED, SC Department of Education CISO, and the SC State CISO. All asked for continuing reports on progress and contact with/from the culprits and copies of any artifacts from the event, which were provided.

HCS has four staff members who spend most if not all of their time designing, building and managing the server infrastructure and as soon as all servers were down the task of slowly and methodically inspecting each server, cleaning and/or rebuilding if necessary and returning to service began. As previously stated, HCS has many hundred servers throughout the district, so this was going to take some time. Each server had to be brought up isolated from the network and checked for infection and encryption. If infected and encrypted the infection had to be removed or the server entirely rebuilt, files restored from backup and the server individually returned to service—very, *very* time consuming.

The first order of business was to try to determine where the infection entered the system, how it spread and *if it would continue to spread*, picking up where it left off when servers were powered back up. Known infected servers were isolated, powered up, and logs inspected to search for the source of the infection. Within a little less than two hours staff had identified what was thought to be the entry point, the method of replication and the type/name of the particular ransomware present.

Just as other activities involving a ransom typically contain a ransom note of some sort, ransomware is no exception. All infected computers contained multiple copies of the ransom note appropriately named *HELP_DECRYPT_YOUR_FILES.html*, a copy of which is provided as an Attachment. This note states the key to unlock files on one computer may be obtained for a payment of 1.5 Bitcoin (at the time about $580) or the keys for *all* infected computers may be obtained for a payment of 22 Bitcoin (at the time roughly $8,500). As a point of information, technology leadership *immediately* recommended the payment of the full ransom of $8,500 as most expedient way to get any and all encrypted data files back.

All previous ransomware infections at HCS were the result of misguided user interaction—opening an infected attachment or clicking a malicious link in an email were the usual culprits, but this infection was different. This time the infection was actively and purposefully installed on an older HCS server that was accessible from the public Internet. This server was used for access to historical data only and was running an old version of a software package called JBoss. The version of the application used requires an old version of JBoss, one that contains known vulnerabilities of remote code execution, and these vulnerabilities were used to install software on the server, take control of the server, and replicate throughout the server infrastructure of the district. No one had opened an attachment or clicked a link for this infection to occur, it was actively executed once the vulnerable server was found by bots (software that runs automated tasks) searching the Internet for such targets.

Once the source of entry and ransomware were identified the task of returning servers to service began. First were the domain controllers, the servers that identify and allow devices and users to connect to the network. The restoration of these servers during the afternoon and evening of Day 0 and early morning of Day 1 allowed users to connect to the wired and wireless networks as well as access the Internet.

Inspection, cleansing, and rebuilding/restoration from backup of servers continued on a priority and business impact basis, with initial efforts focused on financial and HR systems (including payroll), student information systems, and food service/lunch room systems to name a few. Progress was being made and systems were returning to service through the rebuild/restoration process, but it was very time consuming. During this time the superintendent and Board were discussing the possibility of paying the ransom to obtain the decryption keys.

The often heard directives regarding ransomware are 1) never pay as it rewards bad behavior and 2) if you ensure you have good, current backups there is no need to ever pay a ransom. While both are certainly good advice, each overlooks the challenges encountered in an event of the magnitude HCS experienced. Just as many frivolous lawsuits are settled out of court just to make them go away, the same justification may be made for paying a ransomware ransoms. Extortion of this type (not unlike frivolous lawsuits) should not be condoned, but sometimes payment (settlement out of court) is the best decision for the business. Likewise, even when backups exist a restoration effort of this size to remote servers can take weeks and weeks and each day students and teachers do not have access to data that has been encrypted has a dollar value which rapidly exceeds the cost of the paying the ransom. For this reason HCS chose to pay the full ransom to obtain all decryption keys so access to user data was restored more quickly that was possible via backup restoration.

An additional stress factor in dealing with the event was the fact that the ransom note required the payment to be made in the digital, anonymous currency of Bitcoin. While familiar with Bitcoin in concept, no one at HCS had ever dealt with or traded in Bitcoin. It was discovered that there are many, many sites online that are happy to take your money for Bitcoin, but buyer beware. Many are not reputable or secure, but research revealed *coinbase.com* to be a reasonable choice. However, even this site had per-day limitations that would not allow the quantity (now close to $10,000 due to the varying value of Bitcoin to USD) needed to be exchanged in the short timeframe the ransom note required.

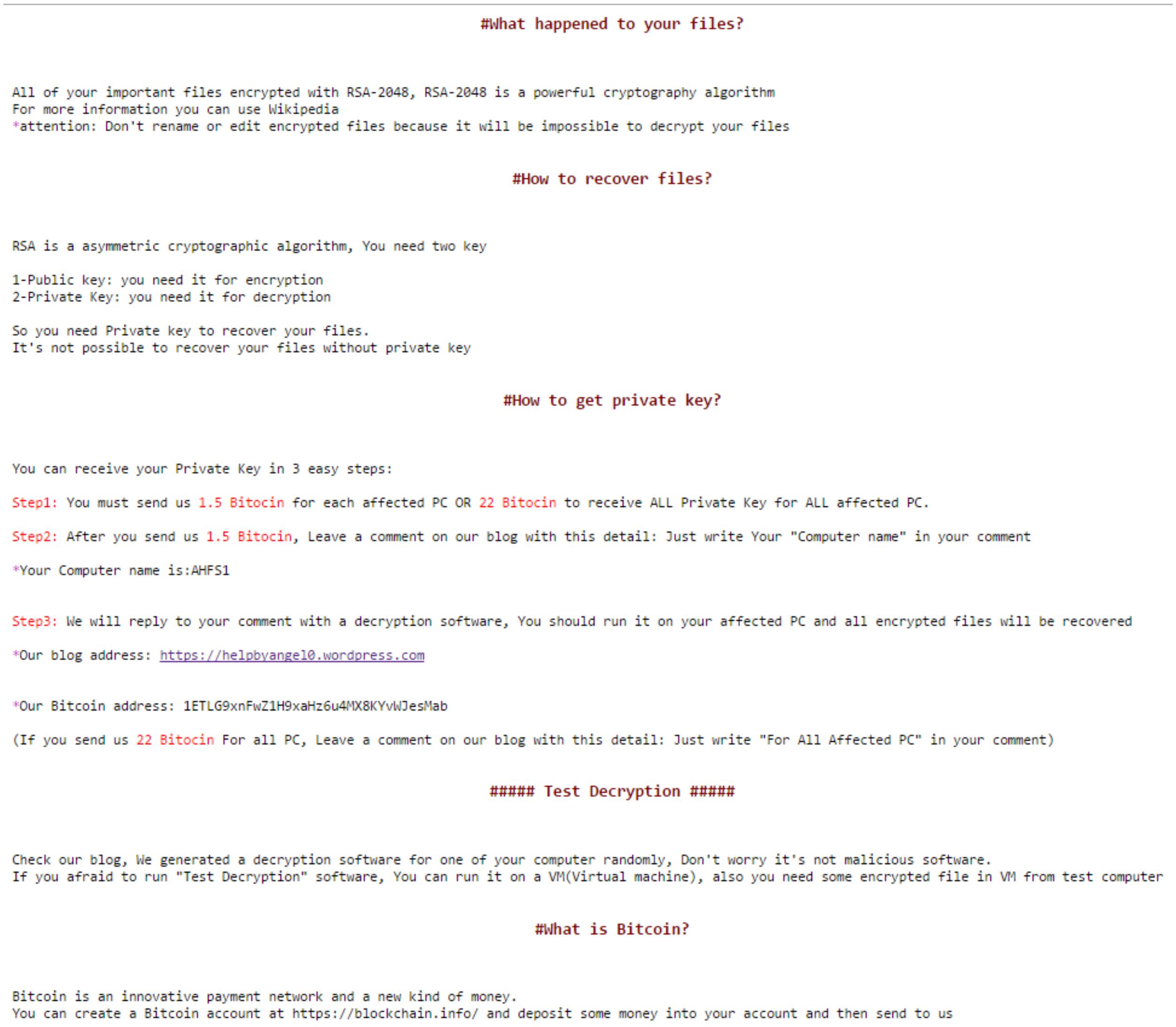
Thankfully, Troy Wilkinson, CEO of Axiom Cyber Solutions in Las Vegas, NV was once involved in law enforcement in Horry County and had heard of the event through news channels. He contacted us to offer assistance which they were able to provide by facilitating the payment of the ransom through their Bitcoin account.

Once the payment was made the decryption keys were in hand within hours and used to decrypted files and systems that had yet to be restored from backup. While it is always a concern that the culprits will not come through once payment is made, the ransomware “industry”, like most is based highly on reputation—if enough people pay and do *not* receive the services for which they’ve paid, very soon no one will pay.

As systems were returned to normal an independent security firm, Dell SecureWorks, was engaged to confirm our conclusion on the entry point of the attack and to monitor and inspect our systems for a few weeks to confirm there were no lingering components from the attack still present. The entry point identified by our staff was confirmed by this outside expert, but they further revealed the compromise of the entry point actually took place Friday, 5 Feb. The intruders spent the next couple of days mapping out the network and preparing for the attack, which began in the early morning, of Monday, 8 Feb. Monitoring and forensic analysis showed no signs of data extraction or continued infection.

Needless to say, the event and recovery were a learning experience for all involved. As expected, all servers and infrastructure has been reviewed, secured, and processed improved to reduce the likelihood of a repeat occurrence. HCS is also involved with FBI’s Infraguard, the state of South Carolina’s SCCyber initiative and ongoing security training.

# ATTACHMENT: Ransom Note Left on All Infected Computers



#What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
*attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us 1.5 Bitocin for each affected PC OR 22 Bitocin to receive ALL Private Key for ALL affected PC.

Step2: After you send us 1.5 Bitocin, Leave a comment on our blog with this detail: Just write Your "Computer name" in your comment

*Your Computer name is:AHFS1

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our blog address: https://helpbyangel0.wordpress.com

*Our Bitcoin address: 1ETLG9xnFwZ1H9xaHz6u4MX8KYvWJesMab

(If you send us 22 Bitocin For all PC, Leave a comment on our blog with this detail: Just write "For All Affected PC" in your comment)

##### Test Decryption #####

Check our blog, We generated a decryption software for one of your computer randomly, Don't worry it's not malicious software.
If you afraid to run "Test Decryption" software, You can run it on a VM(Virtual machine), also you need some encrypted file in VM from test computer

#What is Bitcoin?

Bitcoin is an innovative payment network and a new kind of money.
You can create a Bitcoin account at https://blockchain.info/ and deposit some money into your account and then send to us