BankersHub
Getting from Here to There

Newsletter Article

December, 2016

RANSOMWARE IS ON THE RISE

By Clinton Wanner

ABOUT THE AUTHOR

Clinton Wanner is Security Analyst for Garland Heart Information Security. Prior to joining Garland Heart, Mr. Wanner was Technical Analyst for Constituency Management Group in Dallas. He received his Masters in Information Technology from the University of Texas, Dallas.

Email: info@garlandheart.com

Also at BankersHub

- Jan 5 – New FFIEC Guidance on Mobile Financial Services
- Jan 10 -12 – Wire Transfer 3-part Bootcamp
- Jan 12 – 2016/2017 Year End Compliance Review
- Jan 12 – Confidence Gap Addressed – Are Women Losing Faith in Your Company?
- Jan 18 – HSA Fundamentals
- Jan 18 – FFIEC Call Report #051
- Jan 19 – Insights for Growing Your Institution with Bank-At-Work

ABOUT BankersHub

BankersHub was founded in 2012 by Michael Beird and Erin Handel, 2 Financial Services professionals dedicated to educating and informing banks, credit unions, solution providers and consultants in the U.S. and worldwide. BankersHub delivers best practices, research insights, opinions, economic trends and consumer views through online web education, virtual events and conferences, live streaming activities, custom training and content development.

You receive a legitimate looking email with an attachment and open it. You determine that the email is not important or dismiss it as spam but it is too late. Quietly in the background an application begins running that encrypts or scrambles all the data on the workstation and mapped network drives. It is not until you try to open a needed file that the realization of what is happening occurs. You have been locked out of your own documents.

The Ransomware Threat

According to the Department of Justice, in 2015 there was over $24 million in losses directly related to ransomware. This is only the 2,500 ransomware incidents that were reported to the Internet Crime Complaint Center (IC3). The US Federal Financial Institutions Examination Council (FFIEC) has already warned banks that ransomware is on a sharp rise. This is due largely in part because it is a successful revenue generating scheme. The goal of ransomware is to catch organizations and individuals alike off guard and hold their data hostage until the affected party pays the ransom. Is your bank protected?

3-part Online Training
Advanced IRA
Retirement Issues
January 13, 2017
11:00 am – 4:15 pm ET
RETIREMENT SAVINGS PLAN
ascensus
Always have a plan
BankersHub
Getting from Here to There
Recorded Live at Ascend 2016
• Part 1: IRA and Roth Conversions
• Part 2: Handling Excess IRA Contributions
• Part 3: Advanced Beneficiary Concepts

2017
Upcoming 2017 ACH
Rules Changes
Payments Industry Webinar on
Compliance and Regulations
2 Webinar Dates to Choose
January 11, 2017 (12:00 – 1:15 pm ET)
February 14, 2017 (2:00 – 3:15 pm ET)
Speaker
Terri Sands AAP
Founder
Secura Risk Management
BankersHub
Getting from Here to There
One of the Most Impactful Years Ahead
for the Payments Industry!
Webinar Includes Same Day ACH and
Board of Directors presentation

Follow these seven steps to help prevent your bank from becoming victim to ransomware.

1. Train your employees. If your employees know what to look out for, they can become your most important line of defense in preventing a ransomware attack. Fun fact, the Human Resources department is most likely to be culpable in catching a ransomware infection due to their nature in opening attachments daily.

2. Utilize a spam filter to prevent compressed (.zip) and executable (.exe) attachments. Preventing files from entering your bank's network that have potential to hide ransomware could stop it dead in its tracks.

3. Disable macros from running. Ransomware creators are getting smarter and embedding their malicious code inside common MS Office documents such as docx, ppt, and xlsx. Disabling macros would prevent this code from being run on a potential victim's machine.

4. Ensure that each machine is running anti-virus software with up-to-date definitions. If a known version of ransomware manages to get to your system, your anti-virus software should be able to stop it before encryption starts.

5. Follow the rule of least privilege. Only grant users administrative access to their machine if necessary, and only use administrator accounts when essential.

6. Prevent programs from executing in Temp and AppData folders. These are the common directories where ransomware has been known to hide and execute from. Whitelist applications that need this access.

7. Get an Intrusion Prevention System (IPS). A good IPS can detect and stop known variants of ransomware from phoning home to get an encryption key. Without this key, certain types of ransomware cannot encrypt your data.

Your bank has been hit by ransomware. What do you do now? Initiate your incident response plan. You planned ahead and already have defined procedures for handling ransomware, right? Find the offending machine and remove it from your network immediately. This is paramount in stopping more files on your network from being encrypted and can reduce the amount of data needing to be recovered.

Remember that IT guy that kept bugging you for more money to let him create backups of everything? I hoped you listened. The only way to get out of this mess is to restore all affected systems from backups or roll the dice and pay the ransom. The FBI has previously said it “does not support paying a ransom to the adversary”. This is due in part because there are cases where a victim has paid the ransom in untraceable bitcoin but never received the decryption key. Defining and implementing a solid backup strategy will not only save you in the event of being hit by ransomware, but also aid in business continuity efforts after a hardware failure or natural disaster. Backup all critical systems regularly and test those backups to ensure your ability to restore from them if ever needed.

Visit us at www.BankersHub.com

Coming Soon to a Computer Near You!

Click on the Topic to Learn More and Register

Universal Branch Employees

What You Need to Know and What to Do

This 2-part webinar series covers the business case for utilizing Universal Branch Employees, as well as the best practices to implementing and managing these resources.

Ric Carey
Director – Peak Performance Consulting
Former EVP – Umpqua Bank

Part One – February 15, 2017 12:00 – 1:30 pm ET
Part Two – February 15, 2107 2:30 – 4:00 pm ET