Ransomware

by Steve Brown

In 1970 three burglars posing as a policeman and two burglar alarm technicians conned their way into the home of a British heiress. These thieves made off with two original paintings by Paul Gauguin and Pierre Bonnard and were on their way. The burglars then boarded a train, but reportedly got spooked while crossing the border from France into Italy so abandoned their loot on the train. Five years later, the paintings found their way into an auction of unclaimed train items and were purchased by a Fiat factory worker for $70. For years the paintings hung in the kitchen of the factory worker until 2013, when the man's son, a university student, came across the works in an art book. The family called in art experts who authenticated the paintings, which were then turned over to the authorities. The factory worker was ultimately awarded ownership of the paintings as the original owners were deceased and had no heirs. Art experts estimate the Gauguin to be worth around $48mm and the Bonnard to be worth about $700K. The family, who has always led a modest lifestyle, have decided to keep the Bonnard, but plans to sell the Gauguin.

We couldn't help but think how far criminals who target banks and other financial institutions have come since 1970. Unlike the heiress who met the thieves face-to-face, most criminals who target banks now do so anonymously through computers. One of the fastest growing threats to banks where time-sensitive information is crucial is a sophisticated form of malware known as ransomware.

As its name suggests, ransomware is a sophisticated virus that renders a computer (and connected networks) useless until a ransom is paid. Once a message containing ransomware is opened the virus is launched, quickly encrypting or removing the information contained on that computer (and ultimately, any connected network). The user of the infected computer then receives a message demanding payment of a ransom to release the computer's files, with instructions to pay using Bitcoin or wiring the funds to an offshore account. Users are usually given 24 hours to pay the ransom, with the amount increasing after each 24 hour period that passes, until the ransom is paid.

Most ransomware attacks have occurred on individual personal computers but hackers have become more sophisticated so banks and authorities are worried. These thieves will likely set their sights on financial institutions in an effort to extract even larger sums of ransom.

Though regulators and law enforcement agencies are well aware of the increasing number of ransomware attacks, even the FBI has admitted that there is little they can do about the problem. So far, one major issue is that it is virtually impossible to track Bitcom payments or offshore accounts. As if that weren't enough of an issue, hackers also morph these viruses rapidly, making it incredibly difficult for IT experts to stay on top of such threats. According to Intel, there were investigations into more than 250K samples of ransomware in the Q4 2014 alone, a 155% increase from Q3.

Given such threats, prevention is probably the best defense for the banking industry. Community banks should make sure employees are up to date about such risks and are repeatedly reminded about the danger of opening attachments and links within questionable e-mails. Banks keep

extensive backups of files and critical information, so this means perhaps that they could decide to ignore a ransomware attack and simply wipe an infected computer or network clean, but it may not be that easy. A downed network takes time to get rolling again as one must first wipe out the ransomware. That takes time and the downtime could ultimately prove more costly than the ransom. Time that banks spend rebuilding systems is ultimately of great value and just like fine art, it should likewise be protected.

BANK NEWS

Employees

A survey by the Society for Human Resource Management finds the top 5 things employees want from their jobs are respectful treatment (72%); trust between employees and senior management (64%); benefits (63%); compensation/pay (61%) and job security (59%).

Retirement

Fidelity reports balances in 401ks and IRAs have reached record highs as the stock market has climbed. As of Q1, the average 401k balance was $91,800 (+3.6% YOY) and the average IRA balance was $94,100 (+5.0% from Q4). Despite this, CNBC reports 40% of boomers have no retirement savings.

Financial Planning

A study by Northwestern Mutual uncovers some interesting facts about people and their financial planning efforts. It found: 67% consider themselves savers; 58% say their financial planning efforts could use improvement; 54% have a debt level that is equal to or larger than savings; 34% have done nothing to plan for their financial future; and 21% are not at all confident that they will reach their financial goals.

Generational Borrowing

A Bank of America survey of small business owners finds that 54% of Millennials say they have applied for a loan in the past 2Ys, along with 45% of Gen X and 21% of Boomers.

Major Actions

A Bank Director survey of executives & directors that asked respondents what major actions they intended to participate in over the next 1Y found these among the highest: purchase a healthy bank (47%); none of the options provided (38%); purchase one or more branches (18%); purchase a non-depository line of business (17%); merger of equals (14%) and purchase a loan portfolio (10%).

Mobile Banking

Did you know that as of the end of 2014 about 82% of US financial institutions offered mobile banking vs. 68% as of the end of 2013?

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.