NOMINATIONS OPEN FOR RETAIL BEACON AWARDS

THE HARDWARE Connection™

THE INDUSTRY'S DIGITAL LEADER

February 2015
Vol. 7, No. 1

Hiring the Best Employees

ALSO INSIDE:

Digby's Hardware Cartoon

Product Reviews From Tom's Shop

Trends in Paint and Decorating Products

By Fred Fischer

Could You be HIJACKED?

When buying or maintaining a POS system, make sure you invest adequate money in a good business-class firewall, antivirus software and a means to back up your data. If not, this can end up like the old Fram commercial about oil filters for cars. You can pay me now or pay dearly later.

What are the bad guys doing out there in the internet world? One current really bad activity is called being Hijacked and then paying a ransom. Much like overseas, where the pirates hijack a ship and then hold the crew for ransom.

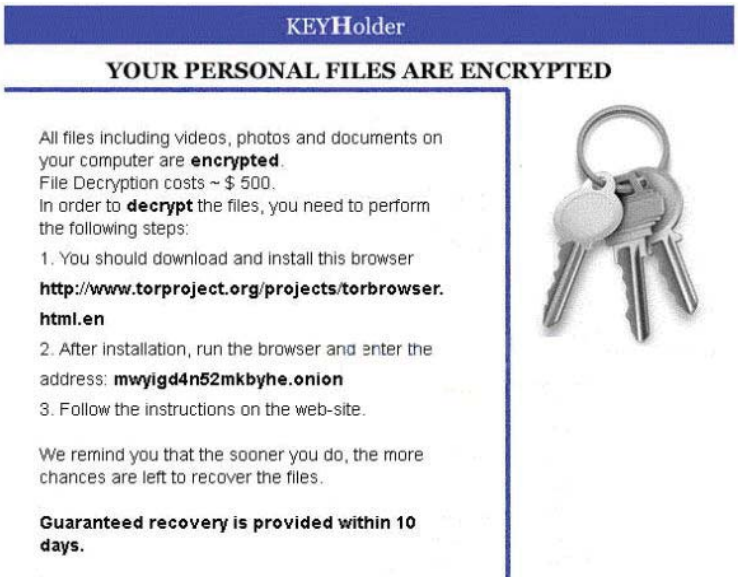
The following is a true story. A long-time hardware industry employee takes the plunge to go in business for himself and buys an existing hardware store. It has a POS system with more than 13 years of sales history.

On his 10th day of ownership when he started the computer, he gets a message "YOUR PERSONAL FILES ARE ENCRYPTED." The message reads if he wants his data back, he should send $500 in bit coin to a particular website (usually not traceable) and upon approval from the bad guys, he will receive a un-encryption key that will unlock his files. If he does not do this in 10 days the data will be lost.

He is told his computer has been hijacked by a program called KeyHolder. This particular malware version of the program started about the first week of December 2014 and is worldwide. Google the words "KeyHolder malware" and you see more information than you will care to read about "KeyHolder."

Crypto Ransomware is actually malware and not a virus. Usually it will not spread through a network. It is usually delivered by email. The user receives an email with a link or an attachment. The link is typically a Dropbox link. Many of the file extensions are usually a zip, exe, vbs or a txt file. Once clicked, the file installs a program, but you do not realize this is happening. Then, several hours later, software runs to install another program using the Internet and then the original program destroys itself so no trace of its activity can be found.

That newly downloaded program then goes out on the internet at an even later time and gets an encryption key. The sad part is this process changes slightly, sometimes more than once a day or every couple of days. That makes it almost impossible to break the encryption process. You have been Hijacked!



How many times have you gotten an email that looks very official? It says they could not deliver a package, a bank needs additional information, please confirm your prescription, you have a criminal case against you from the IRS, your Amazon order is pending shipment and the list goes on. Anti-virus programs have a tough time detecting these programs, because the attachment itself is not the malware.

What kind of damage can KeyHolder do? One office lost six years of medical records; a professional photographer lost 10 years worth of professional pictures, to mention a few. As for the picture files, the encryption key restored the files to thumbnail size, which were worthless. Some waited seven to 14 days to get the encryption key, which worked some of the times and not other times.

The cost to you can be very expensive. Just the labor to recover or set up data again can be costly. Some invoice data and other records may never be recovered. The loss of your POS system for several days cost in both labor and inventory management information. To say it could involve thousands of dollars is an understatement.

Why did this store get compromised? To save a little money, the previous owner's son built two new computers. The computers were OK. To save additional money, they were using free anti-virus software. If software is free, there is probably a reason. There was no firewall, only a router. The backup software was installed, but the scheduler had never been set up, so there were no backups for over 18 months. There was no recovery data.

How can you prevent this type of disaster? There is nothing that is 100 percent guaranteed. Good business-class, anti-virus software with live updates is a must. These updates are sometimes downloaded several times a day. This type of software is usually about $30 per computer and then has an annual renewal fee.

A real firewall is mandatory, one that has a subscription service that comes with it. The first-year cost is typically in the $400 to $700 range for both the hardware and the subscription package. Renewals vary from $200 to $400. You need the subscription service, because the bad guys are always changing their programs to attack your computers and that firmware needs to be updated.

Next are backups. These should be done nightly and stored for several days (a minimum of seven days).

There are companies that offer backup services. These services can back up both locally and off-site. Beware of some that offer low prices for large storage capacity. These are geared for home use. You are running a business. The reason the price is so low is they throttle how fast you can download the saved files. In some cases, it could take two or three days to get all your data downloaded to restore your POS system. Again, you get what you pay for. You need to get your business back up and running now, not two or three days later.

In summary, the one sure way to know you are protected if your data gets hijacked is to have good backups and be using a business-class service. If you have only a router and no firewall with a subscription service, or wireless that is not encrypted, no anti-virus software or are using the free version, and are not doing daily backups, then you are in trouble. If you are using a POS system, check out these things.

If you are considering buying a POS system and all they talk about is low prices and do not give you details about the equipment you are buying and what protection should be part of the package, then it may not be a very good deal. You can pay now or you can pay dearly later. ■

Fred Fischer is president of J3 Point-of-Sale – Ganymede Technologies Corp. Contact him at fred@j3pos.biz.