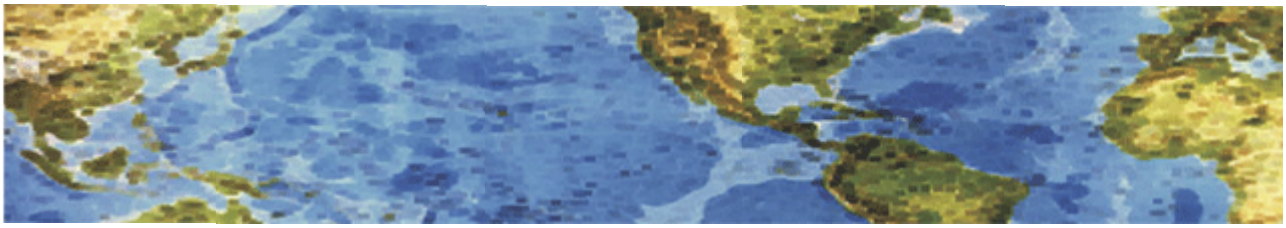
HALL ASSOCIATES



Risk-Based Decision Making Commentary
20 January 2014 Newsletter

DHS Alerts Contractors to Bank Data Theft

A security breach at a Web portal for the U.S. Department of Homeland Security has exposed private documents and some financial information belonging to at least 114 organizations that bid on a contract at the agency last year. "This letter is to inform you that your company's bank account information may have been improperly accessed because of this incident," reads a letter sent to affected organizations earlier this month by DHS. "The incident appears to have occurred sometime over the prior four months."

The letter was sent to organizations that bid on a 2013 contract to help DHS's Science & Technology division develop new communications technologies for first responders. According to DHS, the documents were downloaded from a department Web portal by unauthorized persons outside of the agency, although it hasn't yet determined the cause or source of that access. A spokesperson for DHS said that as a result of this unauthorized access, 520 documents including white papers/proposals, decision notification letters, documents regarding contract and award deliverables and other supporting materials were improperly accessed. That person said that of the approximately 114 organizations that were potentially impacted, only 16 had bank information in potentially accessed documents, and all were promptly notified by S&T. Additionally all affected companies are being provided a list of their accessed documents for their specific determination of business sensitivities and impacts, DHS notes.

The portal in question is run by Herndon, Va. based REI Systems Inc. The company declined to comment for this story, so it remains unclear whether the unauthorized access at REI Systems was limited to the DHS data, or if it affected other REI government projects. According to a page at REI's Web site, **the firm provides similar technology services to the Department of Health and Human Services, the Department of Justice, the General Services Administration, the Internal Revenue Service, NASA, and the Federal Aviation Administration, among others.**

(http://krebsonsecurity.com/2014/01/dhs-alerts-contractors-to-bank-data-theft/)

Ransomware is becoming a major problem for businesses and individuals

The introduction of CryptoLocker and other malware like this "ransomware" poses a new security threat to organizations and individuals.

So what this virus is and what sort of damage it can wreak on an organization/individual?

CryptoLocker is called ransomware because when it infects a system it encrypts the files and keeps the encryption key locked away, so that the only way to get access to those files is to pay a ransom. Ransomware is not a new class of malware, but CryptoLocker and its newer variants is far and away the best of this class. It's only a couple of months old and it's already infected a wide range of organizations of various sizes—it's pretty indiscriminate. Just who is behind CryptoLocker is not known. We do know that they are pretty sophisticated in their understanding of cryptography and they have been able to deal with a large volume of victims so that speaks to their ability to operate to scale. It may be weird to say this about a criminal endeavor, but this is really an enterprise IT operation.

HALL ASSOCIATES

What do the people perpetrating the crime stand to gain from this?
The motive is purely financial. There has to be a level of trust there, too—if they were going around and taking ransoms and not turning over the keys the whole thing would fall apart, so these are very business-oriented people. They've probably made millions of dollars and they're not going to jeopardize that by being unreliable.

How does it work? How might CryptoLocker slip through traditional security defenses such as antiviral software (AV)?
There's no actual malware or virus in the initial attachment, so it's not something that would be detected. It's a very simple program. Once you double click on that benign-looking attachment, usually sent to you in an email—it might appear as a zipped PDF or audio file like a voicemail coming from someone you know—and then it downloads the malware. At that point it's already bypassed the AV and it's encrypting files. By the time an AV company figures out the file used the perpetrators will change it, so AV will detect it after the fact—it won't prevent it.

What can be done, then, to mitigate or prevent it?
To detect and stop CryptoLocker before it can encrypt all your files, you'd have to have a security solution such as Carbon Black in place, monitoring the system constantly for CryptoLocker-type of behavior—not the files used by CryptoLocker per se. Carbon Black is unique because it runs all the time so you could catch CryptoLocker in the act. It is equally important to ensure that your backups are working. Test them! I have seen any number of customers who thought their backups were working only to find out once they become victims that they were wrong. **Finally and most important, train employees to be suspicious of attachments.** It only takes one click to get infected and in a large enterprise that's sharing files and drives that one click will enable CryptoLocker to access everything. If employees do notice errors or corruption warnings when they try to open files, they should turn their computers off to stop CryptoLocker from working on that system. At that point forensics could pull any unencrypted files from the victim's drive.

What steps must be taken to remedy the damage?
Once it's run, you really only have two options. If you have a backup you can restore your system from that. But if you don't, you have to pay the ransom demanded, and you won't get your files back unless you do. Some people have a serious ethical problem with paying for the ransom. But you may have to put your morals and emotions aside in this case - if there are no backups you stand to lose the lifeblood of your business. Calling a security company to do traditional incident response will cost more than the ransom and in the end it won't help because no amount of forensics will get the key needed to unlock your files. It's best to think of it as a business transaction.

Assume you do pay the ransom: what's the procedure and what's the typical cost?
The magic of CryptoLocker is that the ransom is always more cost effective than any kind of incident response. If you pay within 72 hours, it's usually 300 dollars, payable in Bitcoins or possibly via some payment site. Beyond 72 hours the cost goes up. If you call an incident response company they should not charge you any more than a few hundred dollars to help with the transaction and decryption. The criminals will provide a program to decrypt the files and **maintain a web site with an online forum with FAQs** to help people having trouble getting their files back.
http://juntoblog.net/2014/01/14/unpacking-cryptolocker/?goback=.gde_4387290_member_582889185651093094 7#!