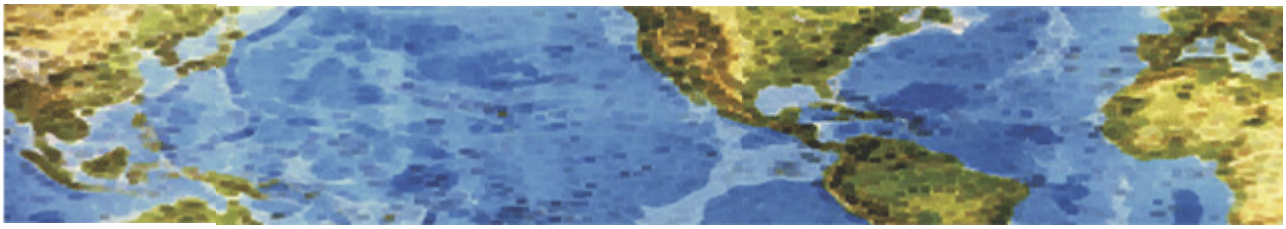
HALL ASSOCIATES



Risk-Based Decision Making Commentary
February 2013 Newsletter #2

Multiple Google Chrome Vulnerabilities Could Allow for Remote Code Execution

MS-ISAC ADVISORY NUMBER: 2013-023 **DATE(S) ISSUED:** 02/22/2013

Multiple vulnerabilities have been discovered in Google Chrome that could allow remote code execution, the bypass of security restrictions, or cause denial-of-service conditions. Google Chrome is a web browser used to access the Internet. Details are not currently available that depict accurate attack scenarios, but it is believed that some of the vulnerabilities can likely be exploited if a user visits, or is redirected to a specially crafted web page.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Google Chrome for Windows and Linux versions prior to 25.0.1364.97

Google Chrome for Mac versions prior to 25.0.1364.99

Successful exploitation of some of the above vulnerabilities could result in an attacker gaining the same privileges as the user. Depending on the privileges associated with the user, an attacker could install programs; view, change, delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

We recommend the following actions be taken:

Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google here:

http://support.google.com/chrome/bin/answer.py?hl=en&answer=95414

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

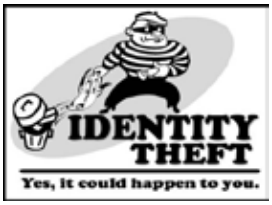
Remind users not to visit un-trusted websites, follow links, or open files provided by unknown or un-trusted sources.

REFERENCES:

Multi-State Information Sharing and Analysis Center : Center for Internet Security

31 Tech Valley Drive, Suite 2 East Greenbush, NY 12061 (518) 266-3460/1-866-787-4722

HALL ASSOCIATES



Small firm hit by 3-year hacking campaign puts face on growing cyber problem

For three straight years, a group of Chinese hackers waged a cyber war against a family-owned, eight-person software firm in California, according to court records. It started when Solid Oak Inc. founder Brian Milburn claims he discovered that China was stealing his company's parental filtering software, CYBERsitter. The theft hurt their business and sales, which was bad enough. But twelve days after he publicly accused Chinese hackers, he says he was inundated by attempts to bring down his Santa Barbara-based business.

Hackers broke into the company's system, shut down its email and web servers, spied on employees using their own webcams and gained access to sensitive company files. "We started watching sales go down," Milburn told FoxNews.com Thursday. "We depend on cash flow and it's not like we're Apple or Dell who have lots of money. We needed to pay our bills, pay our employees and pay our salaries."

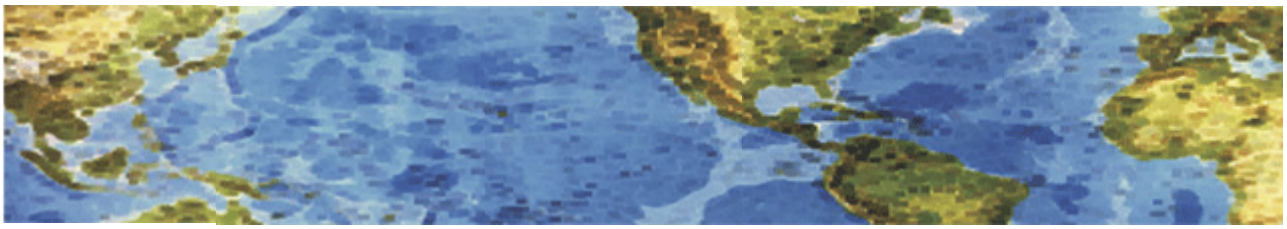
So Milburn waged his own one-man cyber fight against one of the most prolific and patient hacking teams around. He didn't have help from authorities, lacked the cash larger companies have and faced an unknown giant pretty much on his own -- and, last year, won a $2.2 billion settlement, from a decision in federal court in California. Milburn's case is rare in that it ended with a big judgment -- though he declined to say whether he's received the money. But, while Solid Oak is one of the few small companies that have spoken out in detail about being victimized by hackers, the threat of cyber-assault has become all too common.

Adam Levin, co-founder and chairman of Identity Theft 911, says that for most companies it's not a matter of if they will have a breach but when. "No company is ultimately immune to this," he told FOXBusiness.com. "A lot of the times this happens from spear-phishing -- employees at companies are opening things they think are from people within their organization or things that they think are related to their companies. They open the door, and we get killed."

According to cybersecurity experts, high tech spies have been targeting small- to medium-sized companies at alarming rates. Businesses that make the leap to computerized systems often leave their digital identities exposed and primed to be plucked by hackers.

Read more: http://www.foxnews.com/politics/2013/02/22/small-businesses-big-targets-for-cyber-snoops/?intcmp=obinsite#ixzz2LehmpkYc

HALL ASSOCIATES



Risk-Based Decision Making Commentary
February 2013 Newsletter #1

Scammers Target Businesses With Fake E-Mails

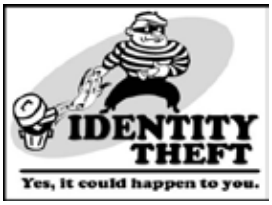
The Federal Trade Commission has issued an alert about Fake E-mail Scams. This one is for rip-off artists to pretend to represent a trustworthy and respected organization. The FTC has been hearing from businesses that have received e-mails exploiting the Federal Trade Commission name. These e-mails claim that the recipient is a target of an FTC investigation. Scammers have sent thousands of e-mails that really appear to be from the FTC. These e-mails claim that people have filed complaints about their business. So if you get an unexpected e-mail that claims to be from the FTC and asks you to click on a link or an attachment for further information about consumer complaints, DON'T OPEN IT. If you do, it will install malicious software on your computer. You can forward the e-mail to spam@uce.gov but definitely delete it. The FTC does **NOT** work complaints this way. **(www.onguardonline.gov/blog)**

Critical Safety Flaws Found in Millions of Home and Office Devices

There is a security advisory out about critical flaws in Universal Plug and Play, a networking protocol used by millions of routers, computer printers, storage drives smart TVs and lots of other devices. These flaws could let outside attackers invade your home and business network and cause havoc or steal sensitive information. Dozens of device manufacturers – including Cisco/Linksys, Netgrear, Sony, Siemens and Belkin – have been notified, but few have put out security patches yet. The US CERT advises all users to manually disable UPnP in their devices administrative settings. For that, you will have to refer to your owner's manuals or the manufacturer's websites to learn how.

The advisory is US CERT Vulnerability Note VU#922681 - Portable SDK for UPnP Devices (libupnp) contains multiple buffer overflows in SSDP.

HALL ASSOCIATES



Got Money? You Are a Prime Target For Identity Thieves

Identity thieves are zeroing in on affluent individuals. (defined as those with over $1M net worth excluding family residence) . This recent phenomenon even has a specific name – Affluent Identity Theft. It turns out that the affluent aren't just at greater risks of identity theft because they have more to lose, but they are often more vulnerable as well**. However, that doesn't mean those of use less affluent or our families are being ignored.**

In most cases, the thieves who targeted these individuals are pretty well organized. They research their targets thoroughly (Do you know how much information about you is available and where it is?). This research is a combination of what is available publicly as well as gentle attacks. A gentle attack is trying to hack into your accounts, doing social engineering on you or your family/employees to find out necessary information.

There are three main reasons such individuals are being targeted:

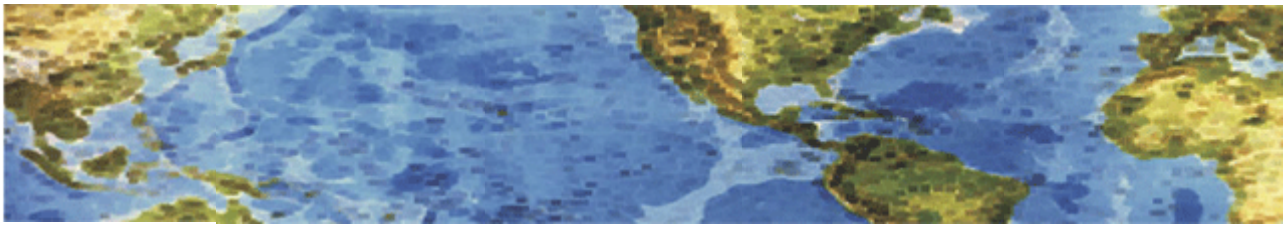
1. They have a lot of credit and they are not good at protecting it. That is basically a mixture of being too busy and arrogance. More like "No one would dare target me. Don't they know who I am?" Or "I have lawyers to deal with that.".
2. They often have multiple accounts with high amounts on deposit, so it is much harder to protect. They normally have business accounts, brokerage accounts, investment accounts or even trust funds. So that multiplies the number of passwords needed (Of course they are all different, right?) and the subsequent protection needed. Rather than take on that task, it just gets ignored (much like all of us – you do protect your different passwords, right?)
3. There are too many points of access and vulnerability. Affluent people tend to have too many people around them – secretaries, direct employees, administrative staff, personal financial advisors, legal advisors, even family. And each one of those represents a point of vulnerability. They are people that can be exploited via social engineering.

In addition, if one of these folks becomes a victim of identity theft, they seem very hesitant to go to the authorities because of the bad publicity that would result. They just want to make it go away as soon as possible and write it off as a bad experience – something identity thieves are aware of.

There are things affluent individuals (and all of us) can do to protect themselves and their money:

1. Take the security of their identities more seriously and more personally. Don't make the mistake of assuming "it won't happen to me" or my lawyer can fix it.
2. Be very care with account information. Have a routine for updating the security of your accounts periodically.
3. Ensure that everyone around them is aware of identity security. Be wary of all calls and e-mails – think security first. Double-check everything.
4. Take precautions . Check credit reports, freeze your credit report, shred personal information, be careful with regular mail.

HALL ASSOCIATES



Risk-Based Decision Making Commentary
July 2012 Newsletter

Why Should Small Businesses Use Risk Management?

Risk is a part of being in business. Risks can be managed and bad outcomes can be controlled in large part. The greatest challenge for small businesses is to find the proper balance between peace of mind and profitability. Trying to eliminate (or ignore) risk from your business is unrealistic and can be prohibitively expensive or cause you to be so risk averse that your business never grows. And the risk environment you face as a small business is constantly changing.

What is the main challenge? For most businesses it is to determine what risks pertain to them and to use a repeatable, effective and minimal cost process to identify, assess, control and monitor risk without interrupting their business activities. This series of newsletters will discuss what can affect you and how you should respond to protect your business, your employees and yourself. If you have any questions or comments, let me know at halld105048@yahoo.com.

One major example of a rapidly changing risk environment is that of Information Technology and Cyberspace use. Your business increasingly works with and through the Internet and IT systems, making the risks inherent in IT systems and cyberspace far more visible and significant than ever. There are more and different threats "in the wild" every few months, making use of the Internet and cyberspace increasingly more problematic. It's not a case of **IF**, but **WHEN** you will be troubled by one or more of these threats. IT and cyberspace risks, when they occur, can cause business losses - lost revenue, lost customers, lost reputation, lost personnel effectiveness, lost productivity. And if you don't know what risks you face in your business, you will not be prepared for them.

So what is an IT or cyberspace risk? Basically they are any threat to your information, data, critical systems and business processes. Why should you be concerned about them? Because anyone in a business, especially management, has a responsibility to identify areas of risk and respond in a timely fashion by improving processes, augmenting controls and requiring testing to ensure that the business is properly identifying and responding to risks. Failure to identify, assess, control and monitor risk sets the business up for serious problems and significant financial losses now and in the not-so-distant future.

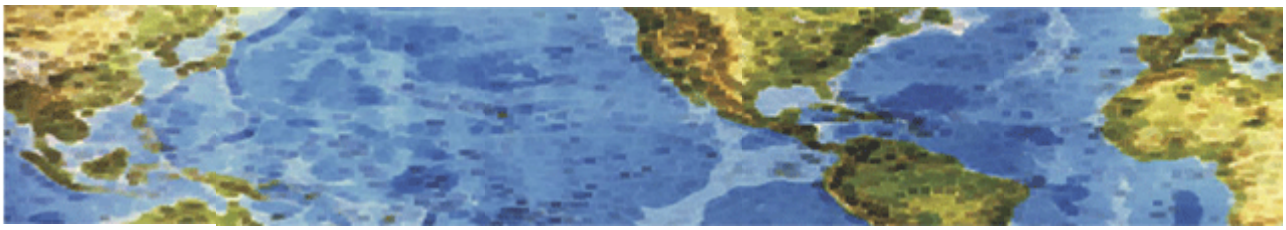
HALL ASSOCIATES

Latest Cyberspace Recommendations

We had a question at my last presentation about "Is PayPal safe to use?". PayPal is as secure as any other online credit account, but no such account is entirely safe, especially from the user side. Following are some recommendations I have found that should enable you to minimize (not eliminate) potential risks when using such sites. Note, however, that these are only recommendations and you should determine exactly what you need to do depending on your specific circumstances.

1. Don't link your PayPal account to your bank account or debit card account. If your PayPal account is compromised, it's money taken directly out of your bank account and by federal law (Regulation E) you only have two days to refute a fraudulent charge with your bank. . But if you link your PayPal account to your credit card and it's compromised, then you have 60 days to refute those charges with your credit card company. However, I did find a note that stated "A spokeswoman for Access Communications, acting as PayPal's representative, has said that PayPal's protection from unauthorized transactions gives the user 60 days to dispute the charges, no matter what the funding source".
2. Don't click on links in the body of emails from PayPal. Those emails might not really be from PayPal. Rather, they may be phishing e-mails from scammers designed to get you to enter your credentials. Instead, manually type in the PayPal address into your browser, log in to your account and see if there are any communications for you from PayPal. Remember, **NO** organization, be it PayPal, a credit card system, a bank, a commercial firm or the Federal Government, will **EVER** ask for your account information or personal information via e-mail.
3. Keep your PC, Cell Phone, I-Pad, etc. security up-to-date. Make sure you have installed the latest critical security patches to your operating system, as well as the latest browser patches and have updated antivirus/internet security software. If whatever you use to connect to a site is compromised with spyware or malicious software when you're using a financial site like PayPal, then others have access to your computer, phone, I-Pad, etc. and can access your user names and passwords. And that is not PayPal's fault.
4. Never log in to PayPal from a public PC or someone else's computer, phone or I-Pad. Each of these is only as secure as the person who logged in before you. Someone could easily have installed spyware or malicious software that will log all your keystrokes.
5. Maintain good records for all Internet commerce. It's a good idea to download and print final pages so that you have backups for purchases made and products bought and sold.
6. Treat your PayPal account like you treat your online banking account. You need to ensure that you have authorized any transactions, large or small. Typically, someone will start draining your account using a series of small withdrawals, hoping you won't notice. So you need to refute those charges as soon as possible and let PayPal know that your account may have been compromised.

HALL ASSOCIATES



Risk-Based Decision Making Commentary
29 Oct 2013 Newsletter

CryptoLocker: A Vicious Virus

Online attackers are using encryption to lock up our files and demand a ransom — and AV software probably won't protect you. Since this can hit anyone, please pass this information along to friends, family, and business associates.

This is a new threat to our data that we need to take seriously. I**t's already hit many consumers and small businesses.** Called CryptoLocker, this infection shows up in two ways. First, you see a red banner (Figure 1) on your computer system, warning that your files are now encrypted — and if you send money to a given email address, access to your files will be restored to you.

The other sign you've been hit: you can no longer open Office files, database files, and most other common documents on your system. When you try to do so, you get another warning, such as "Excel cannot open the file [filename] because the file format or file extension is not valid". This virus finds and encrypts all files you have access to — including those located on any attached drives or mapped network drives.

Cryptolocker comes in the door through social engineering. There are typically three ways you can receive the virus:

1) **Via an email attachment.** For example, you receive an email from a shipping company you do business with. **Attached to the email is a .zip file.** The phishing message could be purporting to be from a business copier like Xerox that is delivering a PDF of a scanned image, from a major delivery service like UPS or FedEx offering tracking information or a bank letter confirming a wire or money transfer.

2) **You browse a malicious website** that exploits vulnerabilities in an out-of-date version of Java.

HALL ASSOCIATES

3) Most recently, **you're tricked into downloading a malicious video driver or codec file**.

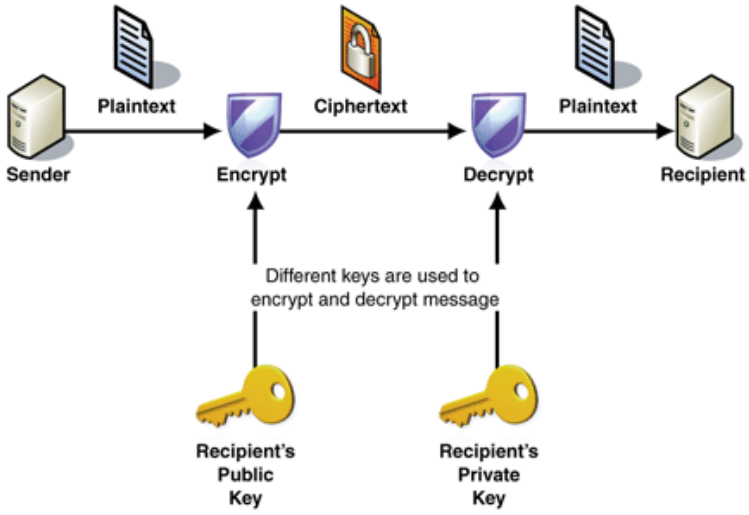
The virus is an executable attachment, but interestingly the icon representing the executable is a PDF file. With Windows' hidden extensions feature, the sender simply adds ".pdf" to the end of the file (Windows hides the .exe) and the unwitting user is fooled into thinking the attachment is a harmless PDF file from a trusted sender. It is, of course, anything but harmless. Once Cryptolocker is in the door, it targets files with the following extensions:
*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c

When it finds a file matching that extension, it encrypts the file using a public key and then makes a record of the file in the Windows registry under HKEY_CURRENT_USER\Software\CryptoLocker\Files. It then prompts the user that his or her files have been encrypted and that he or she must use prepaid cards or Bitcoin to send hundreds of dollars to the author of the virus. Once the payment has been made, the decryption usually begins. There is typically a four-day time limit on the payment option; the malware's author claims the private key required to decrypt files will be deleted if the ransom is not received in time. If the private key is deleted, your files will essentially never be able to be decrypted -- you could attempt to brute force the key, but as a practical matter, that would take on the order of thousands of years. Effectively, your files are gone.

There are no patches to undo CryptoLocker and, as yet, there's no clean-up tool — the only sure way to get your files back is to restore them from a backup. Some users have paid the ransom and, surprisingly, were given the keys to their data. This is, obviously, a risky option. But if it's the only way you might get your data restored, use a prepaid debit card — not your personal credit card. You don't want to add the insult of identity theft to the injury of data loss.

In this case, your best defense is prevention. Keep in mind that antivirus software **probably won't prevent a CryptoLocker infection**. In every case so far, the PC owner had an up-to-date AV application installed. Moreover, running Windows without admin rights does not stop or limit this virus. It uses social engineering techniques — and a good bit of fear, uncertainty, and doubt — to trick users into clicking a malicious download or opening a bogus attachment. There are several ways to prevent this from hitting you. The discussion below is only the basic method. For additional information on an advanced method and other options, such as application whitelisting, check out the articles noted at the end of this newsletter.

HALL ASSOCIATES



The basic prevention method is to ensure you keep complete and recent backups of your system. Making an image backup once or twice a year isn't much protection. Given the size of today's hard drives on standalone PCs, an external USB hard drive is still your best backup option. A 1TB drive is relatively cheap. For multiple PCs on a single local-area network, there are both local backup options as well as cloud storage (which brings other security problems into the mix). Small businesses with networked PCs should have automated workstation backups enabled, in addition to server backups.

Once again, keeping your antivirus software up-to-date is not the panacea for CryptoLocker. The hackers using this exploit are adapting the virus so quickly that AV vendors can't keep up with the many CryptoLocker variations in play. **It's up to individual users to stay vigilant about what they click**. The bad guys just keep getting badder.

To see additional information on the advanced and stronger protection methods, as well as more information on Cryptolocker, check out the following articles:

http://windowssecrets.com/top-story/cryptolocker-a-particularly-pernicious-virus/

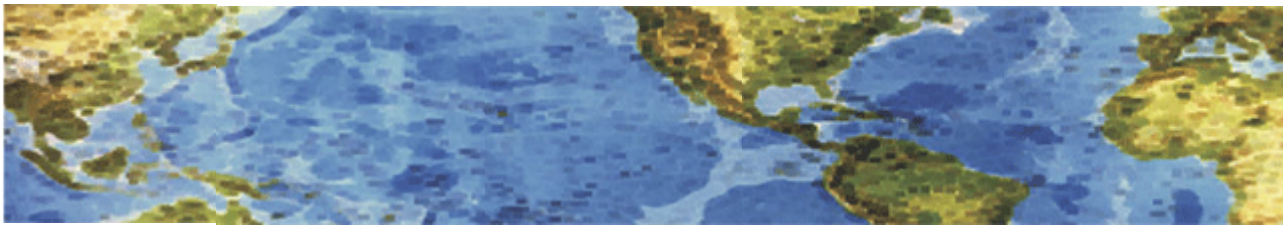
http://www.computerworld.com/s/article/9243537/Cryptolocker_How_to_avoid_getting_infected_and_what_to_do_if_you_are_

http://www.ibtimes.com/cryptolocker-virus-new-malware-holds-computers-ransom-demands-300-within-100-hours-threatens-encrypt

http://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/

http://www.theregister.co.uk/2013/10/18/cryptolocker_ransmware/

HALL ASSOCIATES



Risk-Based Decision Making Commentary
30 July 2013 Newsletter

US-CERT

Recent Reports of DHS-Themed Ransomware

This is a change in the type of Ransomware previously discussed. See page 2 for the original discussion.
US-CERT has received reports of increased activity concerning an apparently DHS-themed ransomware malware infection occurring in the wild. Users who are being targeted by the ransomware receive a message claiming that use of their computer has been suspended and that the user must pay a fine to unblock it. One iteration of this malware also takes a webcam (if available) photo or video of a recipient and posts it in a pop-up to add to the appearance of legitimacy. The ransomware falsely claims to be from the U.S. Department of Homeland Security and the National Cyber Security Division.
US-CERT and DHS encourage users and administrators not to pay the perpetrators and to report the incident to the FBI at the Internet Crime Complaint Center (http://www.ic3.gov/default.aspx).

Use caution when encountering these types of email messages and take the following preventive measures to protect yourself from phishing scams and malware campaigns that attempt to frighten and deceive a recipient for the purpose of illegal gain.

- Do not click on or submit any information to webpages.
- Do not follow unsolicited web links in email messages.
- Use caution when opening email attachments. Refer to the Security Tip Using Caution with Email Attachments (http://www.us-cert.gov/ncas/tips/st04-010) for more information on safely handling email attachments.
- Maintain up-to-date antivirus software.
- Users who are infected should change all passwords AFTER removing the malware from their system.
- Refer to the Recognizing and Avoiding Email Scams document (http://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf) for more information ..
- Refer to the Security Tip Avoiding Social Engineering and Phishing Attacks (http://www.us-cert.gov/ncas/tips/st04-014) for more information on social engineering attacks.
- Users who are infected with the malware should consult with a reputable security expert to assist in removing the malware, or perform a clean reinstallation of their OS after formatting their computer's hard drive.

https://www.us-cert.gov/ncas/current-activity/2013/07/30/Recent-Reports-DHS-Themed-Ransomware-UPDATE

HALL ASSOCIATES

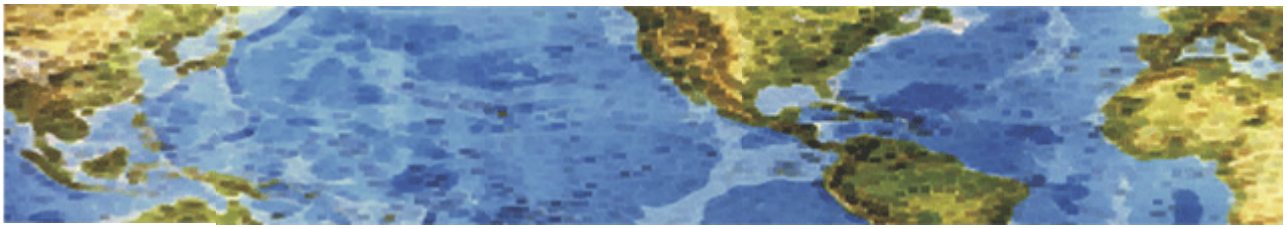
A new Citadel malware platform used to deliver ransomware is named Reveton. The ransomware lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States federal law. The message further declares the user's IP address has been identified by the Federal Bureau of Investigation as visiting websites that feature child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine to the U.S. Department of Justice using a Prepaid money card service. The geographic location of the user's IP address determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate in the background even tho your screen does not show it and can be used to commit online banking and credit card fraud.

This is an attempt to extort money with the additional possibility of the victim's computer being used to participate in online bank fraud. If you have received this or something similar, do not follow payment instructions. Turn off your computer and unhook from the internet immediately. Seek out a local computer expert to assist with removing the malware. You can file a complaint at **www.IC3.gov**.

Malware, scams, frauds and other cybercrimes continue to evolve and shift. Knowledge of these scams and frauds and of the fact that government organizations and legitimate companies will NEVER send out warnings like this is the main way to protect yourself.

HALL ASSOCIATES



Risk-Based Decision Making Commentary
28 May 2013 Newsletter

What is the Future of Privacy?

Everyone needs to understand how thoroughly cyber stuff permeates every aspect of our lives – both business and personal. I recently ran across several articles on how the Internet of Things affects/interacts with our information and have extracted some of the information in them for this newsletter. The URLS for the full articles are at the end of this newsletter.

The Internet has turned into a massive surveillance tool. We're constantly monitored on the Internet by hundreds of companies -- both familiar and unfamiliar. Everything we do there is recorded, collected, and collated -- sometimes by corporations wanting to sell us stuff and sometimes by governments wanting to keep an eye on us.

Ephemeral conversation is over. Wholesale surveillance is the norm. Maintaining privacy from anyone able to pay for information is basically impossible, and any illusion of privacy we maintain is based either on ignorance or on our unwillingness to accept what's really going on. It's about to get worse, though. Companies such as Google may know more about your personal interests than your spouse, but so far it's been limited by the fact that these companies only see computer data. And even though your computer habits are increasingly being linked to your offline behavior, it's still only behavior that involves computers.

The “Internet of Things” refers to a world where much more than our computers and cell phones is Internet-enabled. Soon there will be many more Internet-connected modules on our cars and home appliances. Internet-enabled medical devices will collect real-time health data about us. There'll be Internet-connected tags on our clothing. In its extreme, everything can be connected to the Internet. It's really just a matter of time, as these self-powered wireless-enabled computers become smaller and cheaper. Lots has been written about the "Internet of Things" and how it will change society for the better. It's true that it will make a lot of wonderful things possible, but the "Internet of Things" will also allow for an even greater amount of surveillance than there is today. The Internet of Things gives the governments and corporations that follow our every move something they don't yet have: eyes and ears.

Soon everything we do, both online and offline, will be recorded and stored forever. The only question remaining is who will have access to all of this information, and under what rules. We're seeing an initial glimmer of this from how location sensors on your mobile phone are being used to track you. Of course your cell provider needs to know where you are; it can't route your phone calls to your phone otherwise. But most of us broadcast our location information to many other companies whose apps we've installed on our phone. Google Maps certainly, but also a surprising number of app vendors who collect that information. It can be used to determine where you live, where you work, and who you spend time with.

HALL ASSOCIATES

Medical devices are starting to be Internet-enabled, collecting and reporting a variety of health data. Wiring appliances to the Internet is one of the pillars of the smart electric grid. Yes, there are huge potential savings associated with the smart grid, but it will also allow power companies - and anyone they decide to sell the data to -- to monitor how people move about their house and how they spend their time. Drones are another "thing" moving onto the Internet. As their price continues to drop and their capabilities increase, they will become a very powerful surveillance tool. Their cameras are powerful enough to see faces clearly, and there are enough tagged photographs on the Internet to identify many of us. We're not yet up to a real-time Google Earth equivalent, but it's not more than a few years away. And drones are just a specific application of CCTV cameras, which have been monitoring us for years, and will increasingly be networked.

Google's Internet-enabled glasses -- Google Glass -- are another major step down this path of surveillance. Their ability to record both audio and video will bring ubiquitous surveillance to the next level. Once they're common, you might never know when you're being recorded in both audio and video. You might as well assume that everything you do and say will be recorded and saved forever. In the longer term, the Internet of Things means ubiquitous surveillance. If an object "knows" you have purchased it, and communicates via either Wi-Fi or the mobile network, then whoever or whatever it is communicating with will know where you are. Your car will know who is in it, who is driving, and what traffic laws that driver is following or ignoring. No need to show ID; your identity will already be known. Store clerks could know your name, address, and income level as soon as you walk through the door. Billboards will tailor ads to you, and record how you respond to them. Fast food restaurants will know what you usually order, and exactly how to entice you to order more. Lots of companies will know whom you spend your days -- and nights -- with. Facebook will know about any new relationship status before you bother to change it on your profile. And all of this information will all be saved, correlated, and studied. Even now, it feels a lot like science fiction.

Lots of these devices have, and will have, privacy settings. But these settings are remarkable not in how much privacy they afford, but in how much they deny. Access will likely be similar to your browsing habits, your files stored on Dropbox, your searches on Google, and your text messages from your phone. All of your data is saved by those companies -- and many others -- correlated, and then bought and sold without your knowledge or consent. **You'd think that your privacy settings would keep random strangers from learning everything about you, but it only keeps random strangers who don't pay for the privilege -- or don't work for the government and have the ability to demand the data.** Power is what matters here: you'll be able to keep the powerless from invading your privacy, but you'll have no ability to prevent the powerful from doing it again and again.

HALL ASSOCIATES

If You Want True Privacy, Use Something Other Than Skype

Ever since Microsoft's acquisition of Skype in 2011, people with a predilection for secret communications have been increasingly suspicious of the massively popular VoIP app's claims surrounding privacy. And over the past week, reports have shown just how much Microsoft can see of people's messages. Simple technical tests proved a Microsoft machine accessed links sent over Skype. According to Ars Technica, that has proven Microsoft can and does look at plain text sent by users. This has blown away the myth that Skype provides end-to-end encryption, it was suggested.
A Skype spokesperson sent the following from its privacy policy: "Skype uses automated scanning within Instant Messages and SMS to (a) identify suspected spam and/or (b) identify URLs that have been previously flagged as spam, fraud, or phishing links. Skype will retain your information for as long as is necessary to: (1) fulfill any of the Purposes (as defined in article 2 of this Privacy Policy) or (2) comply with applicable legislation, regulatory requests and relevant orders from competent courts."

Skype does store information on users' interactions and it can access communications when it chooses, albeit by a scanning tool called SmartScreen. It remains unclear how exactly the technology decides which messages to scan, which has concerned some. Microsoft is doing so largely for security purposes, to check links aren't pointing users to malicious sites, and to respond to law enforcement requests when they come in. As noted in Microsoft's first ever transparency report from earlier this year, the UK police are particularly hungry for Skype data, making more requests for it than any other force in the world. To be fair, Microsoft's scanning of Skype messages isn't too different from techniques Facebook reportedly employs, and what any number of other online services do, too. These companies have a duty to make sure their services aren't abused to circulate malware.

Xbox One surveillance machine privacy

Microsoft announced the next generation of its gaming console today, called the Xbox One. Among the new features are biometrics that promise to know you inside and out, which raise some serious privacy concerns. We'll take you through them one by one.

The Xbox One has a lot of new features, including more powerful hardware that integrates with TV, a game DVR that always records your gaming so you can upload highlights later, and dual-screen capability, letting you do things like have a browser window open alongside a game screen (so you can look at a walkthrough or tweet about a game while you're playing it). It has voice activation and facial recognition. Every Xbox One will come with a Kinect, an accessory that tracks players' movements to tie what you're doing in your living room to what's happening in-game. It's been especially popular with dance and fitness games like Dance Central and Your Shape. The Kinect's built-in HD camera has 60% more field of vision this time around and "can see fine details like fingers and facial features." It can track up to 6 people at once, 4 more than the previous Kinect model.
The Kinect will also be able to detect heart rate, which will be helpful during those fitness games to check if you're working as hard as you should be (or if your heart suddenly stops beating, will the super intelligent Kinect call an ambulance for you?)

HALL ASSOCIATES

Voice recognition will let users navigate Xbox and TV menus without lifting a finger…unless they prefer to use gestures instead. Users will say "Xbox On" to turn on the system, which will not only turn on the Xbox but identify who's talking. We imagine voice and facial recognition will also support security features, such as unlocking user profiles or associated accounts.

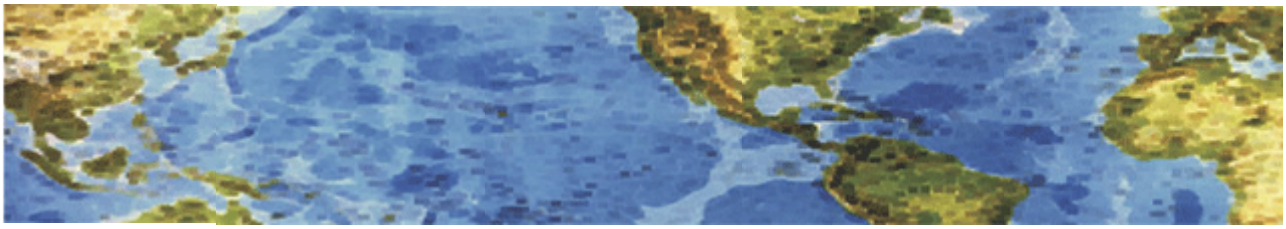
The privacy implications: Microsoft, game companies, and advertisers will know exactly who's sitting in front of the TV. They'll know your voice, your face, the games you like to play, the TV shows you watch, the music you have on the Xbox's hard drive, and the ads you see. It could enable a new era of targeted ads that are even more accurate because they'll change with whoever's using the TV. Microsoft has already filed a "living room snooping patent" that detects how many people are watching and makes them buy access to content, like movies, depending on how many eyes there are. Other companies are busily patenting ad targeting based on monitoring the conversations you have around the TV, which listens for who's talking, the tone of the conversation, and the words used.

Although you won't need to be connected to the Internet to do some things on the new Xbox, many games will require connectivity to work. There's also increased emphasis on cloud storage of game data, so say goodbye to traditional memory cards and hello to online storage, most likely integrated with Microsoft's SkyDrive and maybe with other cloud storage services, like Dropbox. Users can store movies, music, game data, and more in the cloud; they can even store gameplay videos and edit them online.

The privacy implications: Once you store something online, it's way easier for law enforcement and **other third parties** to access it. Unfortunately, the law is really far behind on protecting information that's stored in the cloud because of a legal principle called the third-party doctrine. In non-legalese, it means that if you have a document, and you share it with company A (such as Xbox's cloud storage), you lose privacy rights in it and law enforcement can get it without even a warrant.

http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google
http://www.techweekeurope.co.uk/comment/privacy-skype-silent-circle-116889
http://www.abine.com/blog/2013/xbox-one-will-know-your-face-voice-and-heartbeat/
http://arstechnica.com/security/2013/05/think-your-skype-messages-get-end-to-end-encryption-think-again/

HALL ASSOCIATES



Risk-Based Decision Making Commentary
27 September 2013 Newsletter

Beta Bot: A New Trend in Cyber-Attacks

"I don't think most banks are aware of these latest scams that are replacing Zeus, SpyEye and other financial Trojans, in terms of popularity and usefulness to the criminals," says an analyst at the consultancy Gartner. "This particular Trojan is using techniques that I've seen before, so I'm not sure if it's that unique. **But Beta Bot is most definitely indicative of the new trend in cyber-attack vectors."**

Beta Bot's Attack

The Internet Crime Complaint Center and the Federal Bureau of Investigation recently issued an advisory about Beta Bot, the new malware that targets e-commerce sites, online payment platforms and even social networking sites to compromise log-in credentials and financial information. When Beta Bot infects a system, an illegitimate but official-looking Microsoft Windows message box named "User Account Control" pops up, asking the user to approve modifications to the computer's settings. "If the user complies with the request, the hackers are able to exfiltrate data from the computer," the advisory states. "Beta Bot is also spread via USB thumb drives or online via Skype, where it redirects the user to compromised websites." **Beta Bot defeats malware detection programs** because it blocks access to security websites and disables anti-virus programs, according to IC3.

Mitigating Risks

IC3 and the FBI warn that if consumers see what appears to be an alert from Microsoft but have not requested computer setting modifications from the company, they have likely been targeted for a Beta Bot attack. If infected, running a full system scan with up-to-date anti-virus software is recommended. And if access to security sites has been blocked, then downloading anti-virus updates or a new anti-virus program is advised. This trend of continual compromise of login credentials, which compromises standard online authentication practices, should be concerning to banking institutions. **And they should be taking steps to educate their customers**. Financial institutions should be proactively alerting their customers to this new threat.

This is a good example of how criminals' methods are constantly evolving. They are coming up with sophisticated methods that appear so convincing, even people who typically would not fall for their schemes may do so.

http://www.govinfosecurity.com/beta-bot-new-trend-in-cyber-attacks-a-6099/op-1

HALL ASSOCIATES

The Basics of Social Engineering

A recent study indicates that 30% of Americans will open e-mails, even when they know a message is malicious. One in eleven admitted that they have infected their IT systems by opening a malicious e-mail attachment. The reasons given for doing this are telling. For women, messages containing invitations from social networks are the most alluring. For men, messages with suggestions of money, power and/or sex were the most tempting.

So, you have all the bells and whistles when it comes to computer and network security and you have invested in all the latest technology. **But a social engineering attack can bypass all those defenses.**

Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human psychology rather than breaking in or using hacking techniques. For example, instead of trying to find a software or operating system vulnerability, a social engineer might call an employee or family member and pose as an IT support person, trying to trick the employee or family member into divulging their passwords.

Social engineering has proven to be a very successful way for criminals to get inside your organization or your family. Criminals often take weeks or months getting to know a place before coming to the door or making a phone call. Such preparation includes finding a company phone book and an organizational chart, and researching employees on social networking sites like LinkedIn or Facebook.

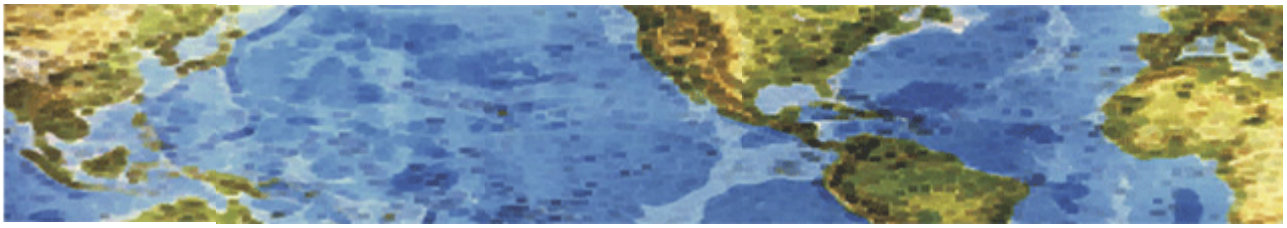
People fall for these cons every day because they have not been adequately warned about social engineering cons and invariably want to be helpful. Human behavior is ALWAYS the weakest link in any security program. Without the proper education, most people won't even recognize a social engineer's tricks because they are increasingly very sophisticated. Four basic principles in misleading people:

- They project confidence. Instead of sneaking around, they proactively approach people and draw attention to themselves.
- They give you something. Even a small favor creates trust and a perception of indebtedness.
- They use humor. Its endearing and disarming.
- They make a request and offer a reason. Psych 110 research shows people are likely to respond to any reasoned request.

Awareness is the number one defensive measure. Employees and family members should be aware that social engineering exists and also be aware of the most commonly used tactics. A lot of information is available on these tactics. One website to check out is csoonline.com. It has numerous articles about social engineering. Some of the best ones are (can contact me for copies) :

Social Engineering – The Basics
How to Rob a Bank: A Social Engineering Walkthrough
Four Signs of an Easy Victim on Social Networks
What It's Like to Steal Someone's Identity

HALL ASSOCIATES



Risk-Based Decision Making Commentary
March 26 2013 Newsletter

Do You Know How to Secure Your Mobile Device?

Think about the last time you used your smartphone or tablet. Did you check your email? Track your finances? Post a photo or check in to a location? Most likely, making phone calls is just one small part of how you use your mobile phone on a daily basis. The ease and accessibility of computing from your smartphone **brings increased risks**. Everyone should follow simple tips for safeguarding our phones the same way we protect our computers and laptops.

The Federal Communications Commission (FCC) recently released Smartphone Checker designed to help the many smartphone owners who aren't protected against mobile security threats. Go to http://www.fcc.gov/smartphone-security to access the Smartphone Security Checker.

The following are simple tips to secure your mobile device:

Set PINS and passwords. You should configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability available on most smartphones.

Do not modify your security settings. Altering your factory settings undermines the built-in security features offered by your wireless service provider and smartphone manufacture making it more susceptible to an attack.

Backup and secure your data. Backing up your data such as your contacts, documents, and photos will allow you to conveniently restore the information if it is lost, stolen, or accidently erased.

Only install apps from trusted sources. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents.

Understand app permissions before accepting them. Make sure to also check the privacy settings for each app before installing.

Install security apps that enable remote location and wiping. Visit CITA for a full list of anti-theft protection apps: http://www.ctia.org/consumer_info/safety/index.cfm/AID/12087.

Accept updates and patches to your smartphone's software. By keeping your operating system current, you reduce risk of exposure to cyber threats.

Be smart on open Wi-Fi networks. When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals.

Wipe data on your old phone before you donate, resell, or recycle it. Reset the phone to its initial factory settings.

Report a stolen smartphone. The major wireless service providers, in coordination with the FCC, have established a stolen phone database. If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider.

HALL ASSOCIATES

The U.S. Secret Service Electronic Crimes Task Force

In March 2012, the U.S. Secret Service, in coordination with U.S. Immigration and Customs Enforcement (ICE), arrested 19 individuals in nine states in "Operation Open Market." This was an investigation into transnational organized crime which operated on multiple cyber platforms and whose **members bought and sold stolen and personal financial information from ordinary citizens.** The group engaged in crimes such as identity theft and counterfeit credit card trafficking. This operation demonstrates how cybercrime extends beyond state lines and operates in the virtual networks and systems **that connect all of us.**

Over the years, the way we manage and spend our money has changed to include fewer cash transactions and more electronic methods, such as direct deposit, automatic payments, and online banking. Now that most financial transactions happen virtually, fraud artists to violent criminals are able to exploit technology to expand and diversify their criminal portfolio. Many crimes affecting individuals – including credit card fraud, identity theft, and embezzlement – are increasingly conducted, or at least facilitated, through the Internet.

As technology evolves, the scope of the Secret Service's mission has expanded from its original counterfeit currency investigations to include emerging financial crimes. To identify and combat electronic crimes, the Secret Service's Electronic Crimes Task Force provides a framework and collaborative crime-fighting environment that brings together federal, state, and local law enforcement, academia, and private industry. The Secret Service continues to work to provide a safer and more secure and resilient cyber environment by arresting cyber criminals.

While the Secret Service and other law enforcement professionals across the country are working hard to combat cybercrime, **emerging cyber threats require everyone, including members of the public, to take part in the shared responsibility to create a safer cyber environment.**

Below are some tips that can help you have a safer and more secure online experience.

Protect all devices that connect to the Internet. Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.

Check website security. When banking and shopping, check to be sure the sites is security enabled with "https://" or "shttp://"

Beware of unsolicited email or suspicious websites. **Never** provide your credit card number, bank account information, or other personal information in response to an unsolicited e-mail or on suspicious Internet web sites.

Visit www.dhs.gov/stopthinkconnect or http://www.secretservice.gov/faq.shtml#faq11for more information.