SEPTEMBER 2014

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

The Smarter Path

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

- Willie Kerns, SmartPath Technologies

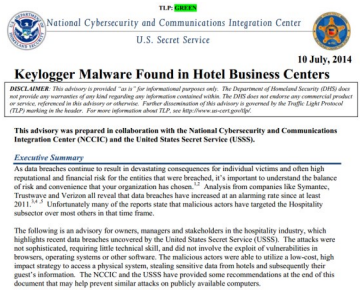
What's Inside:

Beware Keyloggers at Hotel Business Centers

The **U.S. Secret Service** is advising the hospitality industry to inspect computers made available to guests in hotel business centers, warning that crooks have been compromising hotel business center PCs with keystroke-logging malware in a bid to steal personal and financial data from guests.

A DHS/Secret Service advisory dated July 10, 2014.

In a non-public advisory distributed to companies in the hospitality industry on July 10, the Secret Service and the **Department of Homeland Security's National Cybersecurity and Communications Integration Center** (NCCIC) warned that a task force in Texas recently arrested suspects who have compromised computers within several major hotel business centers in the Dallas/Fort Worth areas.



TLP: GREEN

National Cybersecurity and Communications Integration Center

U.S. Secret Service

10 July, 2014

Keylogger Malware Found in Hotel Business Centers

DISCLAIMER: This advisory is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this advisory or otherwise. Further dissemination of this advisory is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

This advisory was prepared in collaboration with the National Cybersecurity and Communications Integration Center (NCCIC) and the United States Secret Service (USSS).

Executive Summary

As data breaches continue to result in devastating consequences for individual victims and often high reputational and financial risk for the entities that were breached, it's important to understand the balance of risk and convenience that your organization has chosen.[1] Analysis from companies like Symantec, Trustwave and Verizon all reveal that data breaches have increased at an alarming rate since at least 2011.[2,3] Unfortunately many of the reports state that malicious actors have targeted the Hospitality subsector over most others in that time frame.

The following is an advisory for owners, managers and stakeholders in the hospitality industry, which highlights recent data breaches uncovered by the United States Secret Service (USSS). The attacks were not sophisticated, requiring little technical skill, and did not involve the exploit of vulnerabilities in browsers, operating systems or other software. The malicious actors were able to utilize a low-cost, high impact strategy to access a physical system, stealing sensitive data from hotels and subsequently their guest's information. The NCCIC and the USSS have provided some recommendations at the end of this document that may help prevent similar attacks on publicly available computers.

"In some cases, the suspects used stolen credit cards to register as guests of the hotels; the actors would then access publicly available computers in the hotel business center, log into their Gmail accounts and execute malicious key logging software," the advisory reads.

"The keylogger malware captured the keys struck by other hotel guests that used the business center computers, subsequently sending the information via email to the malicious actors' email accounts," the warning continues. "The suspects were able to obtain large amounts of information including other guests personally identifiable information (PII), log in credentials to bank, retirement and personal webmail accounts, as well as other sensitive data flowing through the business center's computers."

The advisory lists several basic recommendations for hotels to help secure public computers, such as limiting guest accounts to non-administrator accounts that do not have the ability to install or uninstall programs. This is a good all-purpose recommendation, but it won't foil today's keyloggers and malware — much of which will happily install on a regular user account just as easily as on an administrative one.

While there are a range of solutions designed to wipe a computer clean of any system changes after the completion of each user's session (Steady State, Clean Slate, et. al), most such security approaches can be defeated if users also are allowed to insert CDs or USB-based Flash drives (and few hotel business centers would be in much demand without these features on their PCs).

Attackers with physical access to a system and the ability to reboot the computer can use CDs or USB drives to boot the machine straight into a stand-alone operating system like **Linux** that has the ability to add, delete or modify files on the underlying (Windows) hard drive. While some computers may have low-level "BIOS" settings that allow administrators to prevent users from booting another operating system from a USB drive or CD, not all computer support this option.

The truth is, if a skilled attacker has physical access to a system, it's more or less game over for the security of that computer. But don't take my word for it. This maxim is among the "10 Immutable Laws of Security" as laid out by none other than **Microsoft**'s own **TechNet** blog, which lists law #3 as: "If a bad guy has unrestricted physical access to your computer, it's not your computer anymore."

The next hotel business center you visit may be completely locked down and secure, or it could be wide open and totally overrun with malware. The trouble is that there is no easy way for the average guest to know for sure. That's why I routinely advise people not to use public computers for anything more than browsing the Web. If you're on the road and need to print something from your email account, create a free, throwaway email address at yopmail.com or10minutemail.com and use your mobile device to forward the email or file to that throwaway address, and then access the throwaway address from the public computer.

Written by Brian Krebs, KrebsOnSecurity

Shiny New Gadget of the Month

Jawbone UP

UP is a system, wristband + mobile app that tracks how you sleep, move and eat so you can know yourself better, make smarter choices and feel your best.
Jawbone UP (and UP24, for those who like Bluetooth capabilities and real-time syncing with the app) helps you understand how you sleep, move and eat so you can make smarter choices; this little wristband keeps you in touch with your body and on top of your health.

The new app displays movement and sleep, details and delivers insights, celebrates milestones and challenges you to make each day better. You can even team up with your friends in the UP app and share your accomplishments!

Because you can achieve anything when you take it one day at a time, the UP Insight Engine suggests daily goals based on your unique patterns. Go further, stay hydrated and sleep better for a sense of accomplishment each and every day.
It will also allow you to log your mood and discover connections that affect how you feel. It will remind you to move when you've been inactive too long.

For more information about the Jawbone call us at: (270)205-4709

Which Of These 4 Cloud Computing Solutions Is The Right Fit For You?

Most likely you've heard all of the commotion around cloud computing and know that it's the "Next Big Thing" in business technology. Yet, despite all of the hype, most businesses really don't understand exactly what cloud computing is and what it could do to help their business. "What are my options?" and "What is right for me?" are two of the top questions that I hear quite often. There are at least 4 types of cloud computing solutions for your business. Which one is right for you?

1. Pure Cloud: This is where all your applications and data are put on the other side of the firewall (in the cloud) and accessed through various devices (laptops, desktops, iPads, phones) via the Internet.

2. Hybrid Cloud: Although "pure" cloud computing has valid applications, for many it's downright scary. And in some cases it is NOT the smartest move due to compliance issues, security restrictions or performance issues. A hybrid cloud enables you to put certain pieces of existing IT infrastructure (say, storage and e-mail) in the cloud, and the remainder of the IT infrastructure stays on-premise. This gives you the ability to enjoy the cost savings and benefits of cloud computing where it makes the most sense without risking your entire environment.

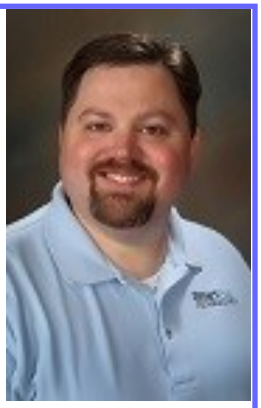
3. Point Solutions: Another option would be simply to put certain applications, like SharePoint or Microsoft Exchange, in the cloud while keeping everything else on-site. Since e-mail is usually a critical application that everyone needs and wants access to on the road and on various devices (iPad, smart phone, etc.), this solution is often a great way to get the advanced features of Microsoft Exchange without the cost of installing and supporting your own in-house Exchange server.

4. Public Cloud vs. Private Cloud: A public cloud is a service that anyone can tap into with a network connection and a credit card. They are shared infra-structures that allow you to pay-as-you-go and are managed through a self-service web portal. Private clouds are essentially self-built infrastructures that mimic public cloud services, but are on-premise. Private clouds are often the choice of companies who want the benefits of cloud computing but don't want their data held in a public environment.

Keep in mind that there is no "perfect" one-size-fits-all cloud solution for every business. All options have upsides and downsides. And which option is best for your business has to be determined on a case-by-case basis based on your company's needs and business requirements.

Call us to find out more information and which cloud is best for your business.

Meet Michael Rich:



Michael Rich was born in Goldsboro, NC, but he has lived in Western Kentucky most of his life. He is a dog lover at heart, who owns 7 of them: Ella (Pit Bull), Jade (Cocker Spaniel), Daisy (Mutt), Carly (Corgi), Cessa (Westie), Cora and Porkchop (Labs). Never backing down from a challenge, Michael thoroughly enjoys his job as our Service Manager. He is the one who oversees all of our engineers and their daily doings. It sure is a good thing that we have him working on computers instead of air conditioner units! One time while he was trying to fix the air conditioner at his church, he ended up breaking a second unit!

The Lighter Side…
Truly Random Facts

- If you have 3 quarters, 4 dimes, and 4 pennies, you have $1.19. You also have the largest amount of money in coins without being able to make change for a dollar.
- The numbers '172' can be found on the back of the U.S. $5 dollar bill in the bushes at the base of the Lincoln Memorial.
- President Kennedy was the fastest random speaker in the world with upwards of 350 words per minute.
- In the average lifetime, a person will walk the equivalent of 5 times around the equator.
- Rhode Island is the smallest state with the longest name. The official name, used on all state documents, is "Rhode Island and Providence Plantations."
- When you die your hair still grows for a couple of months.
- Every year about 98% of the atoms in your body are replaced.
- Elephants are the only mammals that can't jump.
- The average person makes about 1,140 telephone calls each year.
- You burn more calories sleeping than you do watching TV.
- The first product to have a bar code was Wrigley's gum.
- In ancient Rome, it was considered a sign of leadership to be born with a crooked nose.
- The word "nerd" was first coined by Dr. Seuss in "If I Ran the Zoo."

Don't Be a Domino Pusher

Photo by Kirk Taylor

You can line up DOMINOS in a beautiful pattern and spend hours doing it … but all you have to do to knock them all down is PUSH over the first one (the lead domino) and the rest will follow. The same is true about a business. You can spend years and years building up a great business with a super reputation and one employee can cause a customer to never do business with you again. One employee can PUSH a customer the wrong way and run them off … in other words … they knocked down one DOMINO. But, could that one upset customer cause other customers to follow them?

In today's society of instant global communication, one upset customer can put the story out over the internet of your RIP-OFF … AWFUL SERVICE … UNFAIR TREATMENT … and seriously hurt your business. PUSHING the one DOMINO can sometimes cause a whole lot of DOMINOS to fall ... maybe all of them.

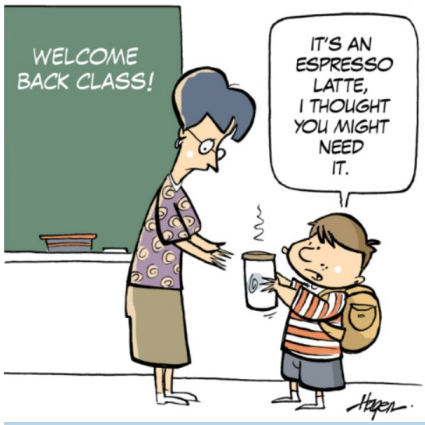
We found out today the appliance repairman who works for the company that has done ALL of our warranty work tried to pull a fast one on us; a $2,964.00 fast one. Before I spend that kind of money, I think a second opinion is in order. So, we got the name of a really talented repairman who had done work for our neighbor and had him diagnose the problem. He said it would only cost $74.96 to fix the problem. He had it fixed in less than one hour.

We had purchased ALL our appliances for our home from the first repairman's company and they had done ALL the previous small repairs for warranty work … but out of warranty … BANG! … time to soak the stupid consumer who has no idea what is wrong. That repairman is right. I don't know about appliances, but I do know how to dial a phone. I do know how to go online and get other opinions. I do have neighbors who may have had similar problems.

Now, what damage has been done by the first repairman? TRUST has been destroyed. CONFIDENCE in what the first repairman (and his company) says is now a thing of the past. Will I ever do business with them again? No! There are a lot of other companies who sell and service appliances. Will I tell my friends about what happened? You bet I will. Will they believe me? They sure will. More customers will be lost because of what happened to just one customer.

Every single day companies PUSH over dominos (customers) not realizing the potential damage that might be caused. I would suggest you start handling every customer like they are that Lead Domino who can possibly knock them all down. If you handle your customers with the care and honesty they deserve, then you won't have to worry about other dominos falling (customers leaving).

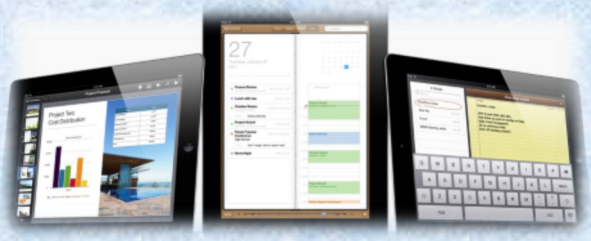
Your customers aren't obligated to do business with you. You need to assume your customers are always teetering, swaying, wavering … getting ready to fall over (go somewhere else) if you push them the wrong way … and on their way down they might just knock over some other dominos (customers) as well. Are there any DOMINO PUSHERS in your company? You better hope not.



Dr. Nido Qubein is president of High Point University, an undergraduate and graduate institution with 4,300 students from 40 countries. He has authored two dozen books and audio programs distributed worldwide. As a business leader, he is chairman of the Great Harvest Bread Company, with 220 stores in 43 states. He serves on the boards of several national organizations, including BB&T (a Fortune 500 company with $185 billion in assets), the La-Z-Boy Corporation (one of the largest and most recognized furniture brands worldwide) and Dots Stores (a chain of fashion boutiques with more than 400 locations across the country). As a professional speaker, Dr. Qubein has received many distinctions, including the Golden Gavel Medal, induction into the International Speaker Hall of Fame and as the founder of the NSA Foundation in Arizona.

7 Simple Ways To Keep Your iPad Secure

- **Don't leave it lying around** Although this is common sense, you've probably violated this rule more than once. iPads are easy targets for thieves, so don't let it out of your sight when in a public place – and don't leave it in plain view in your car or you might end up with a broken window in addition to a stolen iPad.
- **Use a passcode** Although it's not 100% hacker-proof, it will block unauthorized users from accessing your information.
- **Consider enabling automatic data erasing** You can configure your iPad to erase your data after 10 failed passcode attempts. Clearly this is not a good solution for anyone who constantly forgets a password or those who have kids who might try to endlessly log in to use your iPad.
- **Sign up for MobileMe** As mentioned opposite, this software will allow you to locate a lost iPad and, if it's not recoverable, you can remotely wipe the device of your private information.
- **Limit its capabilities** You can set your iPad to restrict certain functions such as access to Safari, YouTube, installing applications and explicit media content using a passcode. In the corporate world, an IT administrator could set these restrictions for company owned devices. At home, you can use this to restrict what your children can do with your iPad.
- **Install software updates** As with all software, make sure you have the latest security updates and patches installed to protect against hackers and viruses.
- **Only connect to trusted WiFi networks** Public WiFis are open territory for hackers and identity thieves. Whenever you connect, make sure it's a legitimate, secure connection.



Smart Path TECHNOLOGIES
Business Computer and Network Specialists

78 Ash St
Calvert City, KY 42029