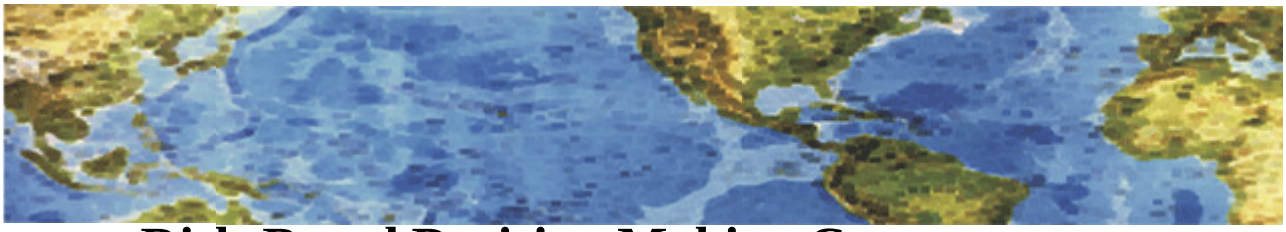
HALL ASSOCIATES



Risk-Based Decision Making Commentary
20 July 2014 Newsletter

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.

In a non-public advisory (see URL below) 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.

The actors would access publicly available computers in the hotel business center, log into their Gmail accounts and execute malicious key logging software. 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 and 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. 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, 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).

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. 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 or 10minutemail.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.

http://krebsonsecurity.com/2014/07/beware-keyloggers-at-hotel-business-centers/

HALL ASSOCIATES

This wafer-thin overlay skimmer includes a high-quality finish.

A translucent mini-skimmer made to sit (mostly) inside of an ATM's card acceptance slot. S

A mini-skimmer designed to slip inside of an NCR ATM's card acceptance slot.

The Rise of Thin, Mini and Insert Skimmers

Like most electronic gadgets these days, ATM skimmers are getting smaller and thinner, with extended battery life. Here's a look at several miniaturized fraud devices that were pulled from compromised cash machines at various ATMs in Europe so far this year.

According to a new report from the European ATM Security Team (EAST), a novel form of mini-skimmer was reported by one country. Pictured above (right) is a device designed to capture the data stored on an ATM card's magnetic stripe as the card is inserted into the machine. While most card skimmers are made to sit directly on top of the existing card slot, these newer mini-skimmers fit snugly inside the card reader throat, obscuring most of the device. This card skimmer was made to fit inside certain kinds of cash machines made by NCR.

New versions of insert skimmers (skimmers placed inside the card reader throat) are getting harder to detect. The miniaturized insert skimmer was used in tandem with a tiny spy camera to record each customer's PIN. EAST notes that the same country which reported discovering the skimmer devices above also found an ATM that was compromised by a new type of translucent insert skimmer, pictured above (center).

The device pictured above (left) is a slender skimmer powered by what looks like either a cannibalized MP3 player or mobile phone. Mobile-powered skimmers allow thieves to have the stolen card data relayed via text message, meaning they never need to return to the scene of the crime once the skimmer is in place. MP3-based skimmers capture card data as audio waves that specialized software can later convert into card data.

As the EAST report notes, ATM skimmers are still a problem in Europe, even though virtually all cash machines there only accept cards that include so-called "chip & PIN" technology. Chip & PIN, often called **EMV** (short for Eurocard, MasterCard and Visa), is designed to make cards far more expensive and complicated for thieves to duplicate. **Unfortunately, the United States is the last of the G-20 nations that has yet to transition** to chip & PIN, which means most ATM cards issued in Europe have a magnetic stripe on them for backwards compatibility when customers travel to this country. Naturally, ATM hackers in Europe will ship the stolen card data over to thieves here in the U.S., who then can encode the stolen card data onto fresh (chipless) cards and pull cash out of the machines here and in Latin America. "In countries where the ATM EMV rollout has been completed most losses have migrated away from Europe and **are mainly seen in the USA**, Asia-Pacific, and Latin America," the EAST report notes. "From the perspective of European card issuers the Asia-Pacific region seems to be eclipsing Latin America for such losses."

One of the simplest ways to protect yourself from ATM skimmers is to cover the PIN pad when you enter your digits. Still, you'd be surprised at how few ATM users actually take this simple but effective precaution.

https://us-mg5.mail.yahoo.com/neo/launch?.rand=beo2ciucu611c#1291665653