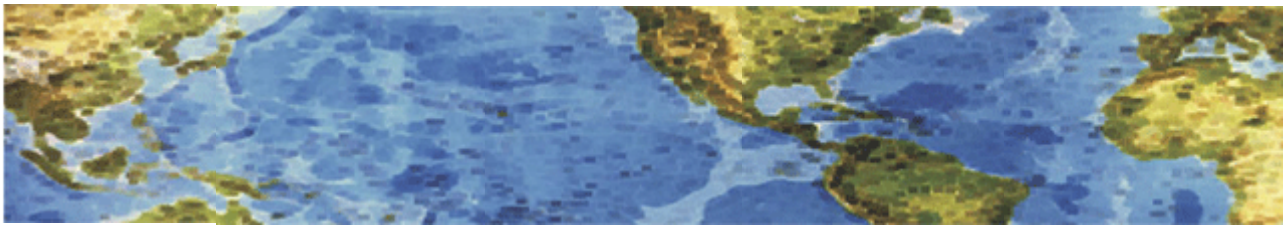
HALL ASSOCIATES



Risk-Based Decision Making Commentary
20 May 2014 Newsletter

Cybercrime Boss Offers Ferrari Prize for Most Lucrative Online Attack

New video highlights the problem legitimate organizations have in recruiting the best talent.

A global cybercrime gang has offered hackers-for-hire a Porsche or Ferrari if they win an "employee of the month" competition, highlighting the increasingly lucrative rewards on offer for those who decide to make a living from the darknet.

A cybercrime boss appeared on a professionally shot video in a car showroom "with a couple of blondes" offering up the luxury prize for the associate who makes the most from an online attack campaign, according to The Independent. Head of the European Cybercrime Centre, Troels Oerting told the paper the video is currently under investigation. He said the scheme shows just how attractive such online operations can be, especially given the relatively low risk of being caught, with gangs recruiting talented programmers from universities.

He added that cybercriminals typically base themselves in jurisdictions where Europol has struggled to penetrate, with 85% of online crime currently coming from Russian-speaking countries. "They are very, very good at locating themselves in jurisdictions that are difficult for us. If we can pursue them to arrest, we will have to prosecute by handing over the case," Oerting told The Indy. "Even if they will do it, it's a very cumbersome and slow process. You can wait until they leave the country, then get them. That's a comparatively small volume. The police ability stops at the border."

He added that Africa is also increasingly being used as a base to launch attacks from, as its broadband infrastructure improves. Lancope CTO TK Keanini told Infosecurity that the luxury automotive prize offer could even be limiting, given that **"some of the people innovating in this area may not be of driving age**". "On average, a Ferrari costs $200,000; but there are people on the dark markets paying well into $250,000 for zero day exploits on specific platforms. When you consider how much money they can make monetizing this type of capability, it is cheap," he added.

Martin Sutherland, managing director of consultancy BAE Systems Applied Intelligence, argued that the news further demonstrates the extent to which the online world is "fast becoming the new frontier for organized crime".

The conclusion is becoming increasingly clear – we have now entered the age of digital criminality - a modern cybercrime combination in which well organized and well-funded criminal groups are using sophisticated cyber techniques to carry out theft and fraud on an unprecedented scale. Responding to this challenge is going to require us to work together more closely than ever before - sharing threat intelligence, and using the most advanced fraud prevention techniques to stop these attacks before they do more harm to businesses, consumers and the economy as a whole.

http://www.infosecurity-magazine.com/view/38367/cybercrime-boss-offers-ferrari-prize-for-most-lucrative-online-attack/

HALL ASSOCIATES

Postal Service: Beware Stamp Kiosk Skimmers

The United States Postal Inspection Service is investigating reports that **fraudsters are installing skimming devices on automated stamp vending machines at Post Office locations** across the United States. Sources in the banking industry are talking about fraudulent debit card activity on cards that were all recently used at self-service stamp vending machines at U.S. Post Offices in at least 13 states and the District of Columbia.

Asked about the activity, a spokesperson for the U.S. Postal Inspection Service confirmed that the agency has an open investigation into the matter, but declined to elaborate further beyond offering tips for consumers to help spot skimming devices that may be affixed to automated stamp vending machines at post office locations. USPIS said it is urging USPS employees to visually inspect the Automated Postal Center (APC) machines multiple times during the day, and that it is asking customers to do the same.

USPIS recommends customers who use the APC machine **should personally visually inspect** the machine prior to use. Look for any type of plastic piece that looks like it has been slid over the actual credit card reader. Look for any other type of marking on the machine that looks as though it has been applied by a third-party. The USPIS is asking customers who see something that appears to be out of place on the machines to notify the local post office supervisor immediately.

According to sources at two separate financial institutions whose customers have been impacted by the activity, the fraud began in late November 2013, and has been traced back to self-service stamp vending machines in Arizona, California, Colorado, Florida, Georgia, Kentucky, Massachusetts, Nebraska, New York, Oregon, Pennsylvania, Utah, Virginia, and Washington, D.C. Banking sources said the fraud follows a fairly consistent pattern: The thieves are targeting debit card users and somehow stealing the PINs associated with the cards. Ostensibly, the fraudsters then fabricate new cards and make cash withdrawals at ATMs ranging from $500 to $800 per card.

Skimmers typically employ some type of device used to steal the data stored on the magnetic stripe on the back of the cards, as well as a hidden camera or PIN pad overlay to record the customer entering his or her PIN. It is not clear what type of skimming devices may be used in this fraud scheme, but the APC kiosks appear to be custom-made by Wincor-Nixdorf, a major ATM manufacturer. As such, many types of skimming devices sold in the cybercrime underground and made for Wincor ATMs may work just as well with this kiosk.

One way to protect yourself against this type of fraud is to use a credit card in lieu of a debit card whenever possible. With a credit card, your liability is maxed out at $50 in the case of fraudulent transactions. Things get more complicated with debit cards. Although many banks also will observe the $50 limit on debit card fraud, customers could be facing losses of up to $500 if they wait more than two business days after learning about the fraud to report it. Also, while your bank is straightening out the situation, any cash you may be missing could be held in limbo, and other checks you have drawn on the account may bounce in the meantime if the fraudsters manage to clean out your checking account.
In addition, it’s a good idea to cover the PIN pad when you’re entering your PIN. Doing so effectively prevents thieves from stealing your PIN in cases where a hidden camera is present.
http://krebsonsecurity.com/2014/05/postal-service-beware-stamp-kiosk-skimmers/