First Data Market Insight

Shore Up Your Cyber Defenses Against These Emerging Threats

Ocean’s Eleven is a very entertaining movie: it’s great fun to watch master thief Danny Ocean and his eleven accomplices plan and execute a brilliant robbery in which they physically carry millions of dollars out the door of a Las Vegas casino and escape into the night. While the movie’s plot seems plausible, today’s most feared criminals are much more likely to be masterminding and executing their crimes while sitting at a computer keyboard. What’s more, the currency isn’t physical but digital.

Picture this: A cyber criminal uses a command and control computer to direct a massive botnet toward a bank’s website in a distributed denial of service (DDoS) attack. He sends code to the bank’s servers to probe them and steal whatever sensitive data can be exfiltrated. It’s a boring plot for a movie, but an intensely scary and increasingly common scenario in the real world.

Unfortunately, cyber criminals have developed many “plots” for how they compromise our computer systems, steal valuable personal data and other information, and commit fraud and other acts that cause individuals and businesses irreparable harm. Computer security firm Symantec reports that worldwide losses resulting from consumer cybercrime including malware attacks and phishing hit $110 billion between July 2011 and the end of July 2012.

There are myriad threats to data security and often they are combined to create even more havoc. Here are just a few examples that are keeping the security experts up at night.

**DDoS Attacks**

By now every financial institution is well aware of the series of DDoS attacks being directed at the banking industry by the hacktivist group Izz ad-Din al-Qassam Cyber Fighters. As the third round of the [publicized attacks](#) gets underway, there is evidence that the attackers are doing more than simply blocking legitimate customers from their accounts; they are also stealing account data. Moreover, many security experts view these attacks as diversionary tactics that give the hackers time to scan for system vulnerabilities and plant malware that will net them big payoffs later.

**Spear Phishing**

A spear phishing attack involves sending an email to a targeted individual or department within an organization. The email, which appears to come from someone the individual trusts, often asks for confidential information such as a login ID and password, or it directs the recipient to click on a link or attachment that will embed malware on the computer. Spear phishing is on the rise, aided by the vast amounts of personal information that can be gleaned from social networking sites and used to create confidence with the targeted victim. Security vendor Proofpoint asserts that financial services organizations are targeted by phishing campaigns three times more often than other industries. Defense against spear phishing is especially challenging because it depends on people being wise to the tactics and suspicious of emails that appear to come from trusted sources.

**SMiShing**

This is a form of phishing that exploits the SMS/text messaging services of a cellular phone. With more than 6 billion cell phone subscriptions in the world, criminals are going where the opportunities are. According to the security company Cloudmark, SMS spam grew by 400 percent in the first half of 2012, and one-third of this spam involves a SMiSh attempt. SMiShing has big implications for companies that allow BYOD, the practice of allowing employees to use their personal mobile devices to access corporate resources. A compromised mobile device can quickly lead to compromised servers and data breaches.
Shore Up Your Cyber Defenses Against These Emerging Threats

Mobile Malware

Speaking of BYOD, it’s putting numerous organizations at risk from mobile malware that’s getting onto workers’ smart phones via games and other apps downloaded from app stores; malvertising, or mobile ads that take users to drive-by websites; and of course, SmiShing. TechRepublic reports that 62 percent of companies already allow BYOD or will by the end of 2013. Unfortunately, many of these companies have insufficient safeguards to prevent cross-over contamination between the mobile devices and corporate network-based assets.

Universal Man-in-the-Browser (uMitB) Scams

Security vendor Trusteer is sounding the alarm about a new type of scam that could be a significant threat for card fraud. This plot collects data such as login credentials and credit card numbers entered in the browser at all websites and uses generic real-time logic on the form submissions to parse the logs and extract the valuable data; for example, the unsuspecting victim’s card information. Amit Klein writes on the Trusteer blog: The data stolen by uMitB malware is stored in a portal where it is organized and sold. It could be used to automate card fraud by integrating with and feeding freshly stolen information to card selling web sites. The impact of uMitB could be significant since information stolen in real-time is typically much more valuable than “stale” information, plus it eliminates the complexities associated with current post-processing approaches.

Memory-Resident Malware

This is a very advanced type of threat whereby malware is loaded into the memory (RAM) of a computer and never written to disk. This makes it extremely hard to detect and eradicate. Once loaded in a server’s RAM, the malware can run undetected for months at a time, siphoning very sensitive data as it is being processed in the clear (i.e., it is not encrypted when in memory). Since encryption keys are also loaded into RAM only, they, too, are vulnerable to theft or exploitation via the malware. Detecting memory-resident malware requires sophisticated training that few security experts have had, making this an especially insidious threat.

Advanced Persistent Threats (APTs)

APTs are a unique threat classification because they may utilize a range of computer intrusion technologies and techniques. These types of attacks are usually directed by humans and are much less automated than other types of attacks. The people behind them are often trying to achieve a specific objective; for example, stealing high value intellectual property, or disabling critical infrastructure (including financial systems). Rather than overwhelming the target computer with attack traffic, APTs tend to use “low and slow” techniques that are hard to detect. Computer security company Trend Micro has identified spear phishing emails as a top vector for allowing advanced persistent threats (APTs) onto company networks.

Like the masterminds behind the robbery in Ocean’s Eleven, cyber attackers know exactly what they are doing and are successful much of the time. Michael Hayden, the former director of the Central Intelligence Agency and National Security Agency, says that companies should focus on primary defenses and then develop strategies for dealing with the results of a cyber attack. “Know they are getting in,” says Hayden, “and manage the consequences.”

For more information, contact your First Data Sales Representative or visit firstdata.com.

© 2013 First Data Corporation. All rights reserved.