Arizona P.A.S.S.

Partners for Arizona's Safety & Security

Arizona Counter-Terrorism Information Center

SITUATIONAL AWARENESS

HOSPITALITY INDUSTRY HIT HARDEST BY HACKS

Trustwave report on data breach investigations shows hotels were breached more than financial institutions last year, and nearly all attacks were after payment-card data

By Kelly Jackson Higgins, DarkReading
Feb. 4, 2010
URL:http://www.darkreading.com/story/showArticle.jhtml?articleID=222601178

Hackers checked into hotel networks more than any other in 2009, and all organizations hit by attacks didn't discover breaches for an average of 156 days, according to a new report based on real-world attacks worldwide.

Nicholas Percoco, senior vice president of Trustwave's SpiderLabs, announced at Black Hat DC this week these and other findings the company compiled in 218 data breach investigations in organizations across 24 countries. Financial services companies accounted for about 19 percent of the breaches, but that was far fewer than in the hospitality industry, where 38 percent of all breaches took place. Retail (14.2 percent) and food and beverage (13 percent) also suffered a fair chunk of attacks, according to Trustwave's data.

And not surprisingly, a whopping 98 percent of targeted data was payment card information. Percoco said that credit card and debit card information is most in demand because it's easy "to turn into cash quickly."

Authentication credentials, financial information, healthcare, and other sensitive information each accounted for 1 percent of the targeted data. And the bad guys mostly hit software-based point-of-sales systems last year, Percoco said, with 83 percent of attacks hitting those systems, 11 percent e-commerce systems, and 3 percent payment processing systems. About 2 percent hit ATM machines. "We don't see a lot of raw hardware-tampering. But we do see it from time to time," Percoco said.

Percoco outlined the three main steps in a typical data breach and how attackers mostly operate at each level: initial entry, data harvesting, and exfiltration.

Nearly half of these attacks occur via remote access applications, of which 90 percent exploit default or weak passwords, according to the report. Around 42 percent of attacks occurred via third-party connections; 6 percent, SQL injection; 4 percent, exposed services; and 2 percent, remote file inclusion attacks. Interestingly, less than 1 percent began with an email Trojan. Around 54 percent of the attacks used malware to harvest stolen data: More than two-thirds (67 percent) deployed memory parsers; 18 percent, keystroke loggers; 9 percent, network sniffers; and 6 percent, malware that the bad guys control who accesses the malware, such as in ATM attacks, according to Percoco.

The actual exfiltration of the stolen data is executed in various ways. Nearly 30 percent used Microsoft Network Shares; 27 percent, native remote access apps; malware via FTP; and 10 percent, native FTP clients. SQL injection was used in 6 percent of the attacks.

Percoco also discussed a sampling of penetration testing data gathered by Trustwave in its report. "Attackers are using old vulnerabilities to get in and out. They know they aren't going to be detected [in many cases], so they are camping out and not trying to hide because no one's watching," he said.

***Analyst Commentary**: ACTIC has no awareness of information or intelligence regarding any specific and/or credible threats to any critical infrastructure sectors in Arizona. This information is Open Source and provided to the AZ PASS community for situational awareness purposes only. Please report suspicious individuals, activity, and threats, to law enforcement and the ACTIC at actic@azpds.gov.*