SearchSecurity.co.UK

E-Guide

Basic Techniques to prevent Identity Theft and Cybercrime

When it comes to cybercrime, identity theft techniques often vary from the technical -- computer forensics -- to the old-school -- calling victims to gather personal information. In this tip, our expert covers basic techniques to prevent identity theft.

SearchSecurity.co.UK
E-Guide

Basic Techniques to prevent Identity Theft and Cybercrime

Table of Contents

Cybercrime, identity theft techniques many and varied

By Ron Condon, UK Bureau Chief

It seemed a good idea at the time. The hotel put a fish bowl on its reception desk and encouraged visitors to drop in their business cards for entry into a regular prize draw.

Then one day the bowl disappeared, and shortly afterwards, former guests of the hotel began having their bank and credit card accounts raided by criminals. The information contained on the business cards had provided useful personal details for the criminals, who had also managed to steal credit card data from the hotel computer systems.

This case is just one example of the ways in which criminals combine high-tech methods and old-fashioned theft to gather the information they need to carry out a range of crimes, from financial fraud to identity theft. It is just one of many investigated by Matthijs van der Wel and his forensic team at Verizon Business, covered in the company's 2010 Data Breach Investigations Report, published in July.

The report analysed the impact of 141 major crimes discovered in 2009, 57 of which were investigated by Verizon and the rest by the US Secret Service. The crimes accounted for the compromise of 143 million records in total.

Speaking here recently at the Gartner Security and Risk Summit, van der Wel explained that, despite the apparent drop in the number of cases between 2008 and 2009, there is no reason to think the cybercriminals are beaten.

In 2009, 85% of all lost credit card records were stolen by means of organised crime, van der Wel said, and criminals resisted flooding the market in the following year in order to avoid driving prices too low.

It means that some companies may not even yet know they have had a breach. "We found that 70% of organisations do not discover the breach by themselves," he said. In other words, they don't know a breach has occurred until criminals exploit the stolen data.

And for all the worries about endpoint security, it appears that 98% of data is taken directly from servers and applications, with the majority (around two-thirds) of threats coming from outside the organisation.

As the fish bowl example demonstrates, when it comes to cybercrime, identity theft, and other malicious pursuits, criminals will use any method they think will prove effective. Van der Wel reported that hackers will readily call potential victims to gather information for a targeted attack if they need to, while at the same time, they will use forensic tools (originally designed to solve crimes) in order to identify sensitive data within companies' systems.

And yet, he said, in many cases it is possible to prevent theft by using basic techniques. For instance, malware may be used to assemble large files on company servers, and the stolen information will then be transmitted in batch to the criminals. "You just need to put in egress filtering to prevent this," van der Wel said. "Then, when someone asks why the company is sending large files every Saturday morning to an address in Bucharest, it might raise a few questions."

Similarly, the most popular method for breaking into Web-based systems is SQL injection: a 10-year-old vulnerability that should be easy to prevent if code is written correctly.

Van de Wel had one final simple tip for the audience: Look at your log files. "Hackers can spend months looking at systems trying to find ways in and gathering information," he said. "You don't need to find the needle in the haystack, but look at the haystack as a whole. If the size of your log file is growing, then it may mean that you are being attacked."

Find the cybercriminal.

(Never mind. ArcSight Logger already did.)

Stop cybercriminals, enforce compliance and protect your company's data with ArcSight Logger.

ArcSight™ An HP Company

Learn more at www.arcsight.com/logger.

Resources from ArcSight

Examining Control System Security and Compliance

Cyberwar: Sabotaging the System

About ArcSight

ArcSight (NASDAQ: ARST) is a leading global provider of cybersecurity and compliance solutions that protect organizations from enterprise threats and risks. Based on the market-leading SIEM offering, the ArcSight Enterprise Threat and Risk Management (ETRM) platform enables businesses and government agencies to proactively safeguard digital assets, comply with corporate and regulatory policy and control the internal and external risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage. For more information, visit **www.arcsight.com**.