Security
April 15, 2009 5:03 PM PDT

Report: Payment card data was top target in 2008

by Elinor Mills

More records were breached in 2008 than in the previous four years combined as a result of a few large breaches involving payment cards, according to a report released on Wednesday.

Last year, 295 million records were compromised and there were 90 confirmed breaches, the Verizon Business **2009 Data Breach Investigations Report (PDF)** found.

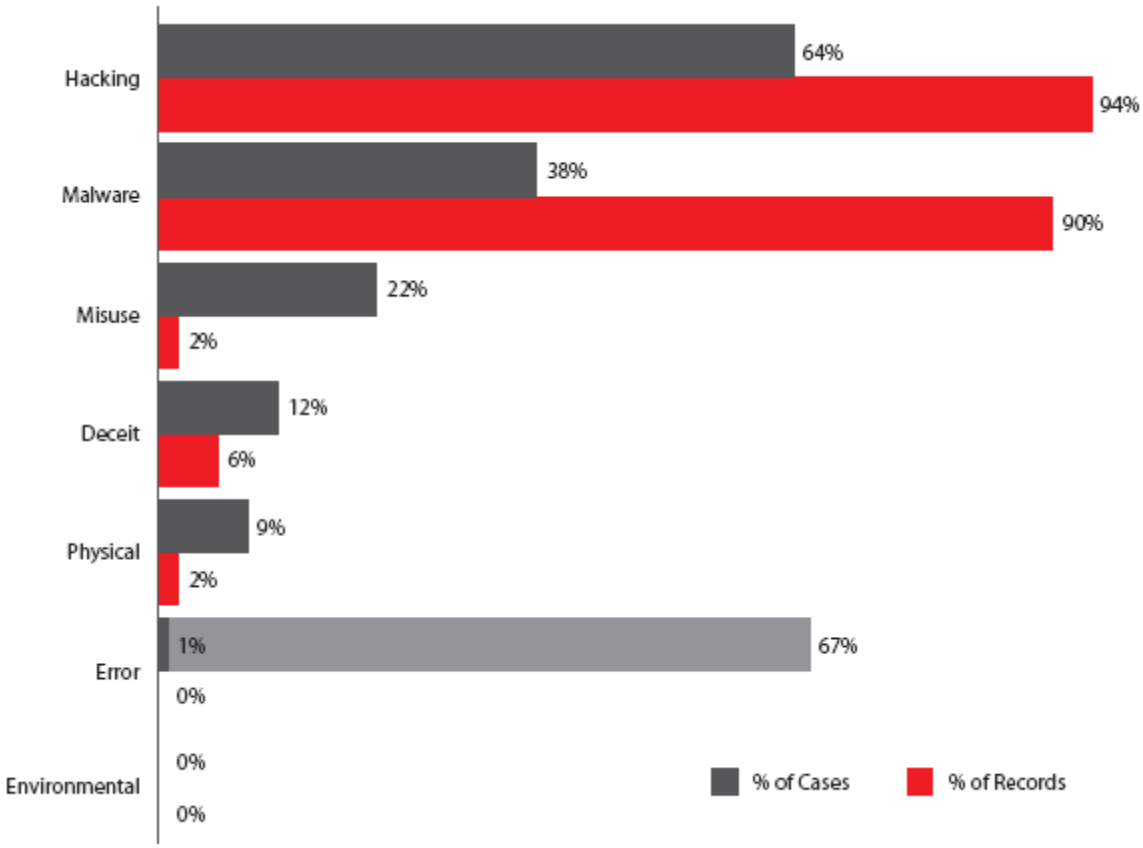
The top five breaches accounted for 93 percent of total records compromised and as a percentage of caseload, 80 percent were payment card breaches while payment card data represented 98 percent of all records compromised last year.

PIN data was increasingly targeted in 2008 in attacks in which magnetic-stripe data and PIN data was used for identity fraud. For example, criminals used the data to make ATM withdrawals from victim's accounts.

PIN data stolen in a breach at payment processor RBS WorldPay was used to clone cards and withdraw millions of dollars from victim bank accounts **last year**. Meanwhile, payment processor Heartland had a huge data breach of its own last year that it **reported in January** and there have been **reports of another breach** at an unidentified institution.

More than three-fourths of organizations suffering payment card breaches were found to be not compliant with PCI data security standards or had never been audited. The typical organization had met less than a third of the requirements in the standards, the

report found.



This chart shows threat categories by percent of breaches (black) and records (red). (Credit: Verizon)

Of the total breaches, 75 percent came from external sources, 39 percent involved multiple parties, 32 percent involved business partners and in 20 percent of the cases insiders were implicated. Three-fourths of the breaches were undiscovered and uncontained for weeks or months.

As far as types of breaches, 64 percent resulted from malicious hacking, 38 percent used malware, 22 percent involved privileged misuse, and 9 percent used physical attacks such as equipment theft or tampering.

In about four of 10 hacking-related breaches, an attacker gained unauthorized access to the victim via one of the many types of remote access and management software, typically provisioned to third-parties for remote administration.

During 2008, malware was involved in more than one-third of the cases investigated and contributed to nine out of 10 of all records breached.

"Malware is now an essential component to nearly all large-scale data breach scenarios," the report said. "Hacking gets the criminal in the door, but malware gets him the data."

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **Privacy & data protection**, **Vulnerabilities & attacks**

Tags: **data breach**, **Verizon**, **payment cards**, **credit cards**

Related

From CNET

Why a national data breach notification law makes sense

Data Robotics means business with DroboPro

Why Google buying Twitter would be a disaster (for one person)

From around the web

Clues to Massive Hacks Hidden in Plain S... Wired

Organized Crime Behind a Majority of Dat... Washington Post - Tech

More related posts powered by Sphere