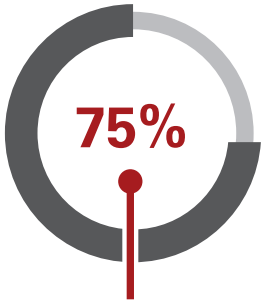
ITSC

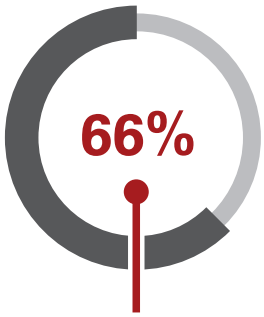
Summary of the 2013

Verizon Data Breach Report

Intruders follow the path of least resistance to the greatest payday, most often exploiting weak or stolen credentials.



DRIVEN BY FINANCIAL MOTIVES
AND RATED AS LOW DIFFICULTY



TOOK MONTHS TO DISCOVER
ACTIVELY HIDING INTRUDERS

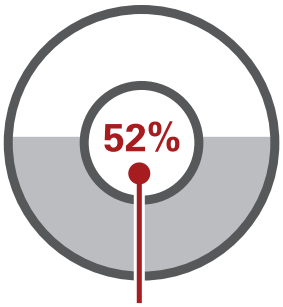
Key Points of Interest

- The majority of breach victims were financial firms and larger organizations.
- The vast majority of intruders were outsiders to the company.
- Around 75% were both driven by financial motives and rated as low difficulty.
- 66% took months to discover, with intruders actively trying to hide.

Firstly, it must be stated that this summary, as with every other, should not be considered a substitute for reading the Verizon Breach Report. The report contains such an abundance of information that it cannot be simplified, summarized or reviewed without losing a massive amount of valuable information.

This summation should be considered to be supplementary, an extra source of information to ensure that all the facts are sufficiently ingrained.

ITSC, Information Technology Security Council
1268 Prospect Street, La Jolla, CA 92037 | tel 866.611.4652 | info@itsecuritycouncil.com



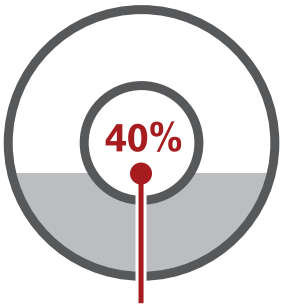
USED SOME FORM OF HACKING

It's Not Hopeless

One of the largest recurring themes present in the breach report is an "Assume you're breached" mentality. As incidents rise every year, the likelihood that any company has been or will be breached continues to rise. But according to the report it's not hopeless, "readers can consider the detection of failures (in a reasonable amount of time) a success." It's no longer about not being breached, it's about catching them in time.

The Methodology

The report studied 47,000+ reported security incidents, 621 confirmed data disclosures, and at least 44 million compromised records that were able to be quantified. Each incident was identified by the A^4 Threat Model. This Threat Model broke each incident down to the actors, actions, assets and attributes involved.

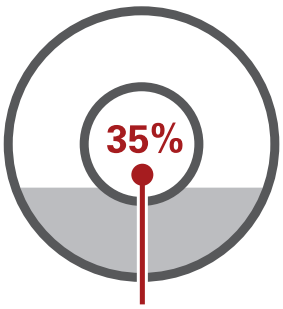


INCORPORATED MALWARE

The Raw Data

Breaches are multi-faceted and any one dimensional attempt to describe them fails to capture their complexity. However it is clear that nearly all of them involved some exploited weak or stolen credentials. Over half involved some sort of hacking while only 40% involved malware of any kind.

The report made the point that the demographics of breach victims were pivotal in understanding incident research. The victims of breaches ranged from manufacturing facilities to professional service firms, however the majority were financial firms and larger organizations.

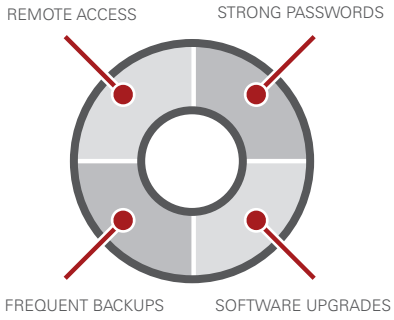


INVOLVED PHYSICAL ATTACKS

There were quite a few commonalities between the attacks but the two that stood out most were that 75% of them were driven by financial motives and around 75% were rated as low difficulty, prompted by opportunity more than specified targeting. As always, the easier the target and greater the value, the higher the risk (a good thing for CISOs to keep in mind when evaluating their own security risk.)

66% of these attacks also took months or more to discover, with perpetrators actively taking steps to hide their efforts. Over half were the result of a compromised server.

TIPS TO REDUCING
RANSOMEWARE



Insiders or Outsiders

Most of these breaches were perpetrated by outsiders (92%) or state-affiliated actors (19%) with only 1% coming from business implicated partners. The report pointed out that despite constant claims that insiders are 80% of all risk, according to the data insiders were accountable for far fewer breaches than outsiders.

Despite the smaller role they played, the report did catalogue some of the more telling characteristics of a malicious insider, including bragging about the damage they were capable of, utilizing company resources for a side business and attempting to gain passwords through trickery. In more than 70% of cases, the insiders stole information within 30 days of announcing their resignation. However, most were no longer employed by the company, and had gained access through accounts that were never disabled.

The Rising Threat of Ransomware

Another rising trend highlighted in the report was Ransomware. Ransomware involves a breach that encrypts the user's data, requiring the organization to pay a ransom to get it back. Several tips were given to reduce Ransomware schemes such as ensuring remote access, mandating strong passwords, confirming that backup have completed successfully and, of course, keeping the system up to date with antivirus software and updates.

The Take Away

According to the VDBIR, the best detection can be achieved through a combination of people, processes and technology. It's incredibly important to regularly measure things like "number of compromised systems" and "mean time to detection" in networks. The report also detailed the importance of evaluating the threat landscape to prioritize a treatment strategy. A "one-size fits all" strategy isn't as powerful as truly understanding the threat environment and reacting with a tailored, situation-specific strategy. Lastly, it was mentioned that CISOs should never underestimate the tenacity of their adversaries, nor the strength of the intelligence at their disposal.

SOURCE - The 2013 Data Breach Investigations Report, Verizon Risk Team. Verizon, April 23, 2013
www.verizonenterprise.com/DBIR/2013