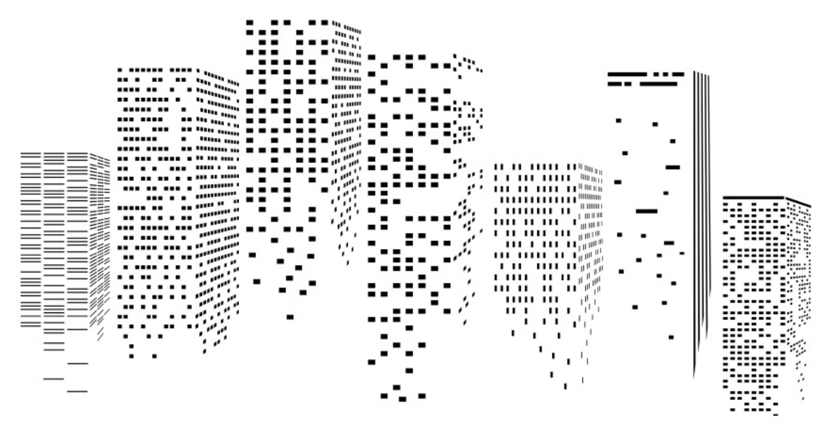
SECURITY NEWS

Follow the Data: Dissecting Data Breaches and Debunking the Myths

September 22, 2015



Myth # 3: Using hacking or malware is the best way to steal all types of data.

Looking at the probability, this one is actually true, only because these were the most popular methods attackers used this past decade. Hacking into a network—whether using brute force, social engineering, or malware—has the highest chance of returns. The second most preferred method is through insiders. These can be disgruntled employees who leak the data on their own volition.

Myth # 4: The retail industry is the most affected by data breaches.

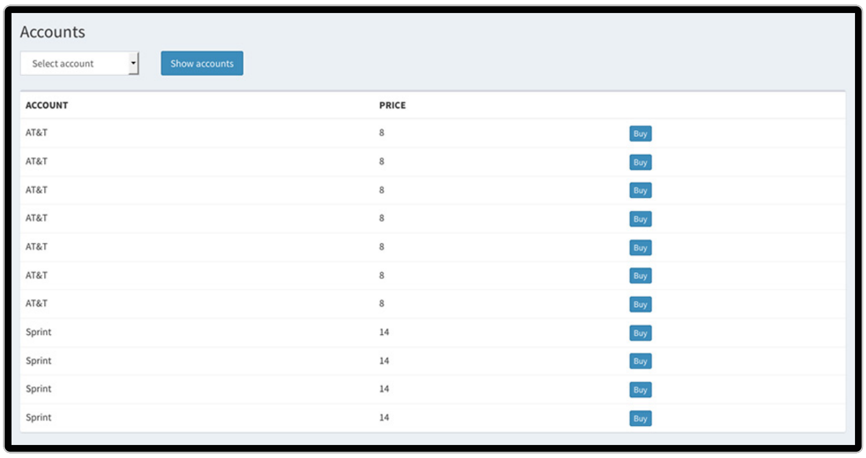
Although retailers have suffered many losses because of data breaches, the most affected industry was actually the healthcare sector, accounting for more than a fourth of all breaches (26.9%) this past decade. The second was the education sector (16.8%) followed by government agencies (15.9%). Retailers only come in fourth place with 12.5%. Although its share is not as big as the healthcare industry's, the effects of a breach for a high-profile retail giant can still be damaging in terms of reputation and revenue.

Industries affected by data breach

Myth # 5: PII is the most in-demand underground commodity in terms of breached information.

There's actually a big surplus of PII currently available in the cybercriminal underground. This has caused its price to drop significantly, from US$4 last year to US$1 this year. The same goes for credit card numbers which are now sold in bulk, regardless of card brand. Interestingly, the selling of stolen Uber accounts is gaining popularity. They're sold at around US$1.15 each.

PREVIOUS 1/20 NEXT



ACCOUNT	PRICE	
AT&T	8	Buy
AT&T	8	Buy
AT&T	8	Buy
AT&T	8	Buy
AT&T	8	Buy
AT&T	8	Buy
AT&T	8	Buy
Sprint	14	Buy
Sprint	14	Buy
Sprint	14	Buy
Sprint	14	Buy

Mobile phone accounts for sale

For a more detailed look at the end-to-end journey of stolen data, check out our research paper Follow the Data: Dissecting Data Breaches and Debunking the Myths [PDF]. There, you'll see more of the research, analysis, and insights that support the findings listed here. Also flip through its companion piece, Follow the Data: Analyzing Breaches by Industry, where you'll see a breakdown of stolen data and breach methods associated with each sector.

The data set used in this research was from the Privacy Rights Clearinghouse (PRC), a non-profit corporation based in California. PRC's mission is to engage, educate, and empower individuals to protect their privacy. They do this by raising consumers' awareness of how technology affects personal privacy, and they empower consumers to take actions to control their personal information by providing practical tips on privacy protection. PRC responds to privacy-related complaints from consumers and where appropriate intercedes on the consumer's behalf/or refers them to the proper organizations for further assistance. PRC documents consumers' complaints & questions about privacy in reports and makes them available to policy makers, industry representatives, consumer advocates, media, etc. PRC advocates consumers' privacy rights in local, state, and federal public policy proceedings.

DOWNLOAD FULL REPORTS

Follow the Data: Dissecting Data Breaches and Debunking Myths

Trend Micro Analysis of Privacy Rights Clearinghouse 2005-2015 Data Breach Records

Numaan Huq
Forward-Looking Threat Research (FTR) Team

A TrendLabs℠ Research Paper

Follow the Data: Analyzing Breaches by Industry

Trend Micro Analysis of Privacy Rights Clearinghouse 2005-2015 Data Breach Records

Numaan Huq
Forward-Looking Threat Research (FTR) Team

A TrendLabs℠ Research Paper

Click to view Follow the Data: Dissecting Data Breaches and Debunking the Myths

Click to view Follow the Data: Analyzing Breaches by Industry

Posted in Cyber Attacks, Data Breach, Hacking, Malware, Cybercrime

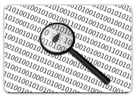
Related Posts

- Malware-Laced Xcode Tool Used to Infect iOS Apps
- FBI Warns Public on Dangers of the Internet of Things
- Sphinx Malware Update: Potential Scammers Just Got Scammed
- Key Raider Malware Steals 225,000 Apple Credentials from Jailbroken iPhones
- A Brief History of Notable Online Banking Trojans

Recent Posts

- Follow the Data: Dissecting Data Breaches and Debunking the Myths
- Malware-Laced Xcode Tool Used to Infect iOS Apps
- Let's Encrypt Project Issues Free Encryption Service
- FBI Warns Public on Dangers of the Internet of Things
- Sphinx Malware Update: Potential Scammers Just Got Scammed

We Recommend



HP Pulls Out of Hacking Contest, Citing Changes to Wassenaar Arrangement

The Kittens Strike Back: Rocket Kitten Continues Attacks on Middle East Targets

Q&A: The Deep Web, Anonymity, and Law Enforcement

1H TorrentLocker Landscape:
Targeting Even More Victims in Australia

1H TorrentLocker Landscape Shows A Growing Target Base

↑ Top of page