Sep22 Follow the Data: Dissecting Data Breaches and Debunking the Myths

5:00 am (UTC-7) | by Numaan Huq (Senior Threat Researcher)

Data breaches are daily news items. Reports of data breaches affecting governments, hospitals, universities, financial institutions, retailers, and recently an extra-marital affairs site, dominate the news with increasing frequency. This is merely the tip of the data breach iceberg, with the vast majority of incidents remaining unreported and undisclosed.

To better understand data breaches, it is important to define the term. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27040 defines a data breach [PDF] as:

> "Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed."

A wide range of sensitive data is compromised across all industries from businesses both big and small as well as individuals. These include PII; financial, health, education, and payment card data; login credentials; intellectual property, and others. In the news, data breaches are almost always attributed to hacking or malware attacks. While these play a big role in data breaches, they do not account for all incidents. Other breach methods frequently observed includes insider attacks, theft or loss, and unintended disclosures.

Perpetrators who compromise sensitive data are a diverse group that includes insiders, individual criminals, as well as organized and state-sponsored groups. Stolen data is commonly used to commit crimes such as financial fraud, identity and intellectual property theft, espionage, revenge, blackmail, and extortion.

Because data breaches have become an everyday affair, people may become desensitized to having their personal, financial, health, education, and other data compromised which then ends up for sale in criminal marketplaces. This desensitization could be the product of several factors, including:

- Daily data breach incident news overload
- Stolen sensitive data is not tangible like a stolen mobile phone
- No "instant" bad consequence of having sensitive data stolen
- Lack of understanding of the repercussions of sensitive data theft

The eventual penalty of having sensitive data stolen is high and some victims (identity theft and fraud victims, for instance) are left suffering for years through no fault of their own. Data breach disclosure laws exist in the US. But do these laws provide the protection required to truly safeguard the everyday individual? Are businesses abiding by them and disclosing data breach incidents when they occur?

The risk and impact of data breaches prompted us to come up with the research paper: ***Follow the Data: Dissecting Data Breaches and Debunking the Myths***, where we do statistical analysis of publicly disclosed data breach incident reports. All publicly disclosed data breach incident reports have been collected from Privacy Rights Clearinghouse's Data Breaches database. We look at the different types of crimes commonly committed using stolen sensitive data. Based on our analysis we created a Bayesian Network to model commonly observed data breach scenarios. We survey criminal marketplaces hosted in the Deep Web to profile the different types of sensitive data available for purchase and their selling prices. Finally, we outline defensive methods businesses and individuals can practice to prevent becoming victims of data breach crimes.

Some highlights from the research are:

- California leads other states with the most number of reported data breach incidents.
- Personally identifiable information (PII) is the most popular record type stolen.
- The healthcare sector is the most affected industry in terms of data breaches.
- Identity theft was most rampant crime that resulted from breaches in the healthcare industry.
- Payment card data breaches greatly increased starting 2010.

Find out what else we discovered about data breaches in our ***Follow the Data: Dissecting Data Breaches and Debunking the Myths*** page, where you can also download the full report and industry analysis.

The paper	**The companion material**

Search our blog:

Go

Featured Stories

Targeted Attacks versus APTs: What's The Difference?

Sanctions For Hacking: Good or Bad Idea?

Old-School Law Enforcement vs The Deep Web

Ashley Madison, Why Do Our Honeypots Have Accounts On Your Website?

Recent Posts

Follow the Data: Dissecting Data Breaches and Debunking the Myths

The XcodeGhost Plague – How Did It Happen?

How Exploit Kit Operators are Misusing Diffie-Hellman Key Exchange

Calendar

September 2015

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

« Aug

Email Subscription

Email Subscription

Your email here

Subscribe

This entry was posted on Tuesday, September 22nd, 2015 at 5:00 am and is filed under Bad Sites, Targeted Attacks . You can leave a response, or trackback from your own site.

The XcodeGhost Plague – How Did It Happen?

- Cloud Security Blog
- Consumerization Blog
- Fearless Web
- Internet Safety for Kids & Families
- Simply Security News
- Trend Micro Blog [German]
- TrendLabs Security Blog [Japan]
- Cloud Security APAC

Do you have a product related question? Visit our support website