Acuris Risk Intelligence

White Paper

The Cost of Stolen Data - Exploring the growing impact of information and identify theft

The Cost of Stolen Data - Exploring the growing impact of information and identify theft

In an era dominated by technology and digital services, it is almost impossible to be offline. We shop, share and store data online on a scale that was unthinkable in the past. In 2017, global internet traffic had grown to 46,000 gigabytes per second from 100 gigabytes per hour in 1997.[1] And globalization has made the movement of goods, capital, services and data easier and more intensive. Business activities taking place thousands of miles apart are today interconnected and interdependent. Electronic commerce has flourished both within and across countries. Critical infrastructure essential for of the functioning of society and economy can't operate without technology. The global financial system has also evolved, introducing new transaction methods such as mobile payments, digital wallets and cryptocurrencies like Bitcoin. At the same time, social media channels have grown in numbers and popularity, giving users instant access to information and entertainment.

Criminals have adapted to the modern environment and are taking advantage of the flexibility of this globalized life. Stealing data is often much easier than stealing goods, and can be done on a larger scale, with consequences that are hard to control.

Types of stolen data

People typically have relationships with many organizations and content providers online and the sensitive data they disclose can fall in the hands of criminals. The more data that is shared, the more is at risk. Vulnerable data includes ID information such as national security numbers, social security numbers, addresses, passports and driver's licenses, all of which can be used for ID theft. A report from non-profit organization the Document Security Alliance notes that a counterfeit driver's license with an expired date has been the most favored falsified document for decades.[2]

Personal data can also fall into the wrong hands. Criminals can steal e-mail addresses and domains, secret questions and answers, employer and payment provider IDs, usernames and passwords. If all these details are compromised, entire businesses can be at risk as confidential information, proprietary data and internal correspondence can be disclosed to competitors and criminals.

Financial data is the most profitable item on the black market. It includes account numbers, sort codes, routing numbers and card information, including PINs. Breaches of financial data may not be detected immediately because offenders have become highly proficient in their techniques. Banks and customers may not find out that someone else has access to the cards for months. Fraudsters may check whether stolen card numbers are valid by making small payments that can remain unnoticed. If the first attempt is successful, criminals use cards regularly and perform increasingly larger transactions. As with other goods, stolen data is also sold, this time in forums and platforms in the unindexed web. Credit card information can be purchased for USD 5-100, depending on the information available. Cards with cardholder names and security codes are more expensive, while those accompanied with account balances command premium prices. [3]

How is data stolen?

Data can be stolen in different ways and criminals use many sophisticated methods. Companies can fall victim to business e-mail compromise (BEC) and e-mail account compromise (EAC). BEC perpetrators use social engineering or unauthorized access to computers to penetrate

[1] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html
[2] https://www.documentsecurityalliance.org/forms/counterfeit_solutions.pdf
[3] https://www.thebalance.com/how-credit-card-information-is-stolen-4028975

corporate e-mail accounts and conduct illicit wire transfers through them. Targets are usually companies with international partners and cross-jurisdictional activities that involve making payments on a regular basis. EAC is similar to BEC but relies on already hacked e-mails through which payment requests are made.[4]

Other common methods are phishing and spoofing. With spoofing, a fraudster impersonating someone else send e-mails on their behalf to obtain access to data. Often used alongside spoofing, phishing involves perpetrators sending an e-mail that falsely claims that they are representatives of a legitimate company, and aims to obtain sensitive information such as passwords, credit card numbers or bank account details. Typically, the malicious e-mail contains a link that directs to a criminal entity.

Data breaches can be carried out by insiders who leak confidential data to unauthorized users for money, or they can constitute illegal breaches in a company's network. Data breaches can happen in personal networks as well.[5]

"Ransomware isn't new but it is in fashion", says a New York Times article published earlier this month.[6] The US Cybersecurity and Infrastructure Security Agency, which is part of the Department of Homeland Security, also confirms that it has seen an increased number of ransomware attacks on a global level.[7]

Considered to be the *"ultimate form of social engineering malware"*[8], these types of breaches rely on phishing e-mails that contain links, ZIP files or other attachments. The emails may look legitimate because they come from providers that users are usually familiar with, like banks, electricity companies or partners. However, they disseminate malicious code that is activated with one click and blocks the victim's access to their files. Users can also be threatened that their private information will be posted online. The only way to recover their data, is to pay a ransom – in cryptocurrencies, pre-paid cards, vouchers or other payment tools that are difficult to trace. The first case of ransomware was registered in 1989. Back then it was not very sophisticated, and experts could reverse the encryption and find out who created the code.[9] Today, the situation has changed dramatically. Ahead of the US 2020 presidential elections, experts fear that hackers could target voter registration databases and electoral systems with ransomware in order to falsify the results and provoke instability.[10]

What is the impact for organizations and individuals?

Internet fraud and data theft can have detrimental impacts on individuals, companies and societies. On an individual level, people can lose valuable information and money as well as inadvertently becoming involved in criminal activities they have nothing to do with. For companies, the impacts are also severe. Firms that store sensitive information are required to have systems that prevent abuse. Should they fail to do so, in addition to incurring serious financial losses, entities can be subject to severe fines from regulators and authorities. The strict rules are in place because a weakness in one organization can affect the many other companies with which this organization has a relationship, and ultimately impact customers.

For example, in November 2013, US retailer Target became a target of cybercriminals who gained access to its systems by using credentials stolen from a third party. The offenders were able to penetrate Target's customer service database and install malware to obtain full names, phone numbers, e-mail addresses, payment card numbers, credit card verification codes and

---

[4] https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud
[5] Ibid.
[6] https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html
[7] https://www.us-cert.gov/Ransomware
[8] https://www.techworld.com/news/security/ransom-trojans-spreading-beyond-russian-heartland-3343528/
[9] https://www.techrepublic.com/blog/it-security/ransomware-extortion-via-the-internet/
[10] https://www.reuters.com/article/us-usa-cyber-election-exclusive/exclusive-us-officials-fear-ransomware-attack-against-2020-election-idUSKCN1VG222

other sensitive data, affecting 41 million customer payment card accounts. The contact information of more than 60 million customers was also compromised. Target cooperated with state authorities and in 2017 agreed to pay a USD 18.5 million settlement, which at the time was considered "the largest ever for a data breach".[11]

In 2017, it was revealed that most adults who have credit in the USA had become secondary victims of a massive data theft from Equifax, one of the major credit reporting agencies.[12] Between mid-May and July 2017, hackers had been stealing names, social security numbers, dates of birth and addresses of nearly half of the population of the country.[13] Former CEO and chairman Richard F. Smith was forced to retire and had to testify before the House Committee on Energy and Commerce to explain how this was allowed to happen.[14] In July this year, the Federal Trade Commission announced that the company had agreed to settle the case by paying USD 700 million.[15] Some 147.9 million American citizens were affected by the cyberattack and the company has been struggling to regain the trust of its customers since 2017.

In September 2018, Facebook announced that hackers had taken advantage of weaknesses in its systems to gain access to millions of phone numbers and e-mail addresses via 400,000 accounts that allowed them to abuse the access tokens of 30 million Facebook users. Access tokens save time for those who prefer the convenience of logging in without entering passwords. Facebook also admitted the 14 million users had stored additional sensitive information in their accounts such as gender, relationship status and places they had checked in, all of which was visible to hackers. [16] Systems such as Spotify, Pinterest and Yelp were also threatened by the attack because access to them is available via Facebook's tokens.[17] Facebook's shares fell to USD 151.30 per share after the breach was announced.[18]

Identity data theft can also have national security implications. The Document Security Alliance report says that religiously motivated terrorist and home-grown extremists have used counterfeit driver's licenses to rent cars and trucks, to buy components for explosive devices and avoid detection by the competent authorities.[19] The report of the 9/11 Commission that investigated the attacks against the World Trade Centre, said that *"the need for travel documents dictated Al-Qaeda's plans"* and that *"for terrorists, travel documents are as important as weapons"*.[20] Al-Qaeda operatives have also used counterfeit or forged documents to obtain loans, which were subsequently spent to finance terrorist activities in North America, Europe and the Middle East. The loans have never been repaid.

Modern technologies have made people's lives easier, by allowing them to carry out fast transactions, shop worldwide without formalities and interact with peers and friends from all over the globe. Businesses, too, rely on technologies and their activities depend on the internet. However, using these tools, criminals have turned trade with stolen information into profitable business. Using sophisticated methods, they have compromised countless gigabytes of personal and financial data, which has led to more insecurity and substantial financial and reputational losses for many organizations.

---

[11] https://eu.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/
[12] https://www.latimes.com/business/story/2019-08-02/equifax-data-breach-settlement
[13] https://www.latimes.com/business/story/2019-08-02/equifax-data-breach-settlement
[14] https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf
[15] https://www.latimes.com/business/story/2019-08-02/equifax-data-breach-settlement
[16] https://www.cnbc.com/2018/10/12/facebook-security-breach-details.html
[17] https://www.theguardian.com/technology/2018/oct/02/facebook-hack-compromised-accounts-tokens
[18] https://www.cnbc.com/2018/10/12/facebook-security-breach-details.html
[19] https://www.documentsecurityalliance.org/forms/counterfeit_solutions.pdf
[20] https://www.9-11commission.gov/report/911Report.pdf