PROJECT REPORT

Data Breach Investigation

By- Abhinav Lather

Project Aim

To investigate a data breach in a financial institution which includes email address,account numbers etc.

->What is a Data breach ?

A data breach is any security incident in which unauthorized parties gain access to sensitive data or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) or corporate data (customer data records, intellectual property, financial information).

->Why data breach occurs?

- An Accidental Insider. An example would be an employee using a co-worker's computer and reading files without having the proper authorization permissions. The access is unintentional, and no information is shared. However, because it was viewed by an unauthorized person, the data is considered breached.
- A Malicious Insider. This person purposely accesses and/or shares data with the intent of causing harm to an individual or company. The malicious insider may have legitimate authorization to use the data, but the intent is to use the information in nefarious ways.
- Lost or Stolen Devices. An unencrypted and unlocked laptop or external hard drive — anything that contains sensitive information — goes missing.
- Malicious Outside Criminals. These are hackers who use various attack vectors to gather information from a network or an individual.

Targets in data breach

- Weak credentials. The vast majority of data breaches are caused by stolen or weak credentials. If malicious criminals have your username and password combination, they have an open door into your network. Because most people reuse passwords, cybercriminals can use brute force attacks to gain entrance to email, websites, bank accounts, and other sources of PII or financial information.
- Payment Card Fraud. Card skimmers attach to gas pumps or ATMs and steal data whenever a card is swiped.
- Third-party access. Although you may do everything possible to keep your network and data secure, malicious criminals could use third-party vendors to make their way into your system.
- Mobile Devices. When employees are allowed to bring their own devices (BYOD) into the workplace, it's easy for unsecured devices to download malware-laden apps that give hackers to data stored on the device. That often includes work email and files as well as the owner's PII.

The damage a Data Breach can do

In many cases, data breaches cannot just be patched up with some password changes. The effects of a data leak can be a lasting issue for your reputation, finances, and more.

For business organizations: a data breach can have a devastating effect on an organization's reputation and financial bottom line. Organizations such as Equifax, Target, and Yahoo, for example, have been the victims of a data breach. And today, many people associate/remember those companies for the data breach incident itself, rather than their actual business operations.
For government organizations: compromised data can mean exposing highly confidential information to foreign parties. Military operations, political dealings, and details on essential national infrastructure can pose a major threat to a government and its citizens.
For individuals: identity theft is a major threat to data breach victims. Data leaks can reveal everything from social security numbers to banking information. Once a criminal has these details, they can engage in all types of fraud under your name. Theft of your identity can ruin your credit, pin you with legal issues, and it is difficult to fight back against.

How to prevent being a Data Breach victim

Data breach prevention needs to include everyone at all levels — from end-users to IT personnel, and all people in between.

When you’re trying to plan how to prevent data breach attacks or leaks, security is only as strong as the weakest link. Every person that interacts with a system can be a potential vulnerability. Even small children with a tablet on your home network can be a risk.

Here are a few best practices to avoid a data breach

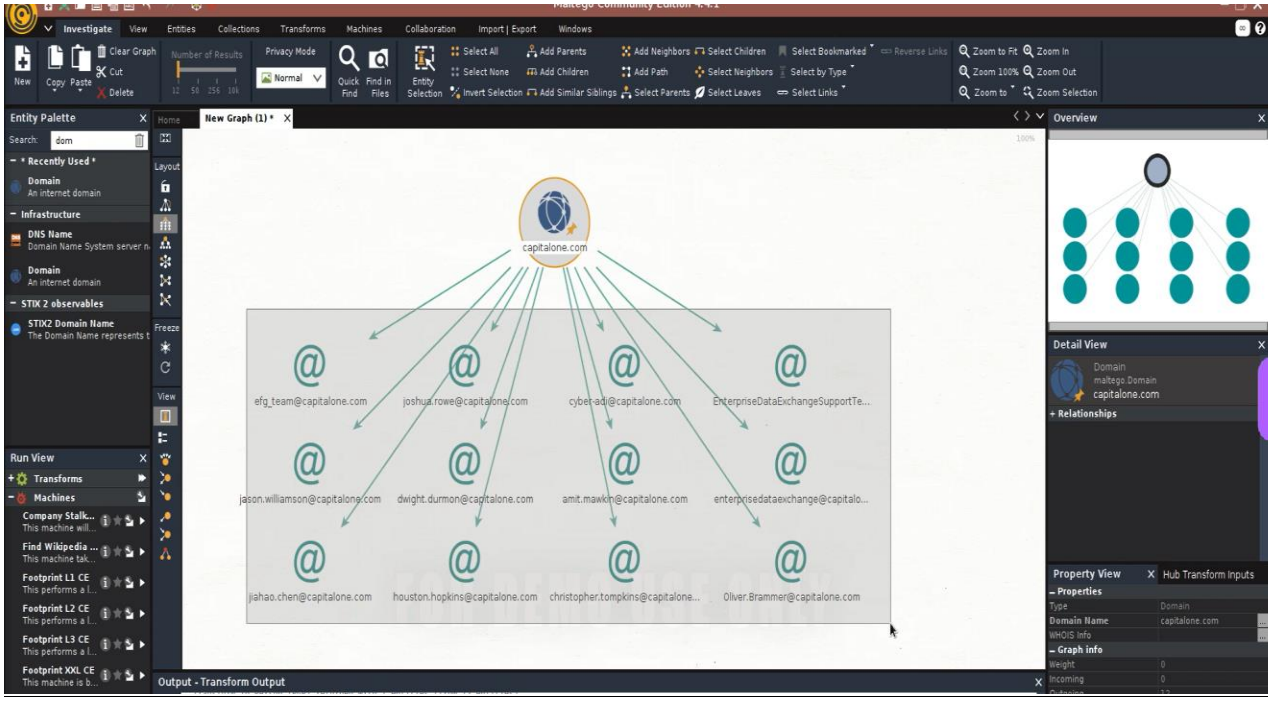
- Patching and updating software as soon as options are available.
- High-grade encryption for sensitive data.
- Upgrading devices when the software is no longer supported by the manufacturer.
- Enforcing BYOD security policies, like requiring all devices to use a business-grade VPN service and antivirus protection.
- Enforcing strong credentials and multi-factor authentication to encourage better user cybersecurity practices. Encouraging users to start using a password manager can help.
- Educating employees on best security practices and ways to avoid socially engineered attacks.

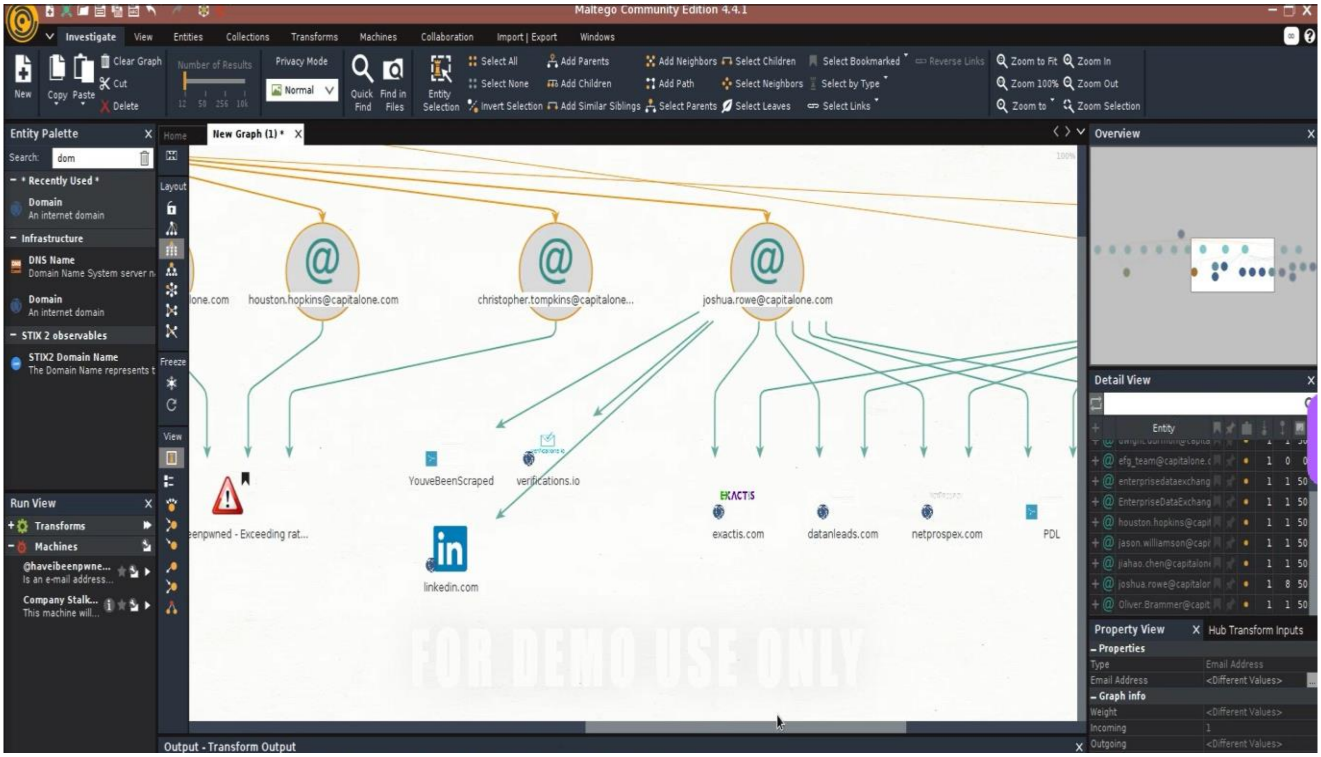
INVESTIGATION

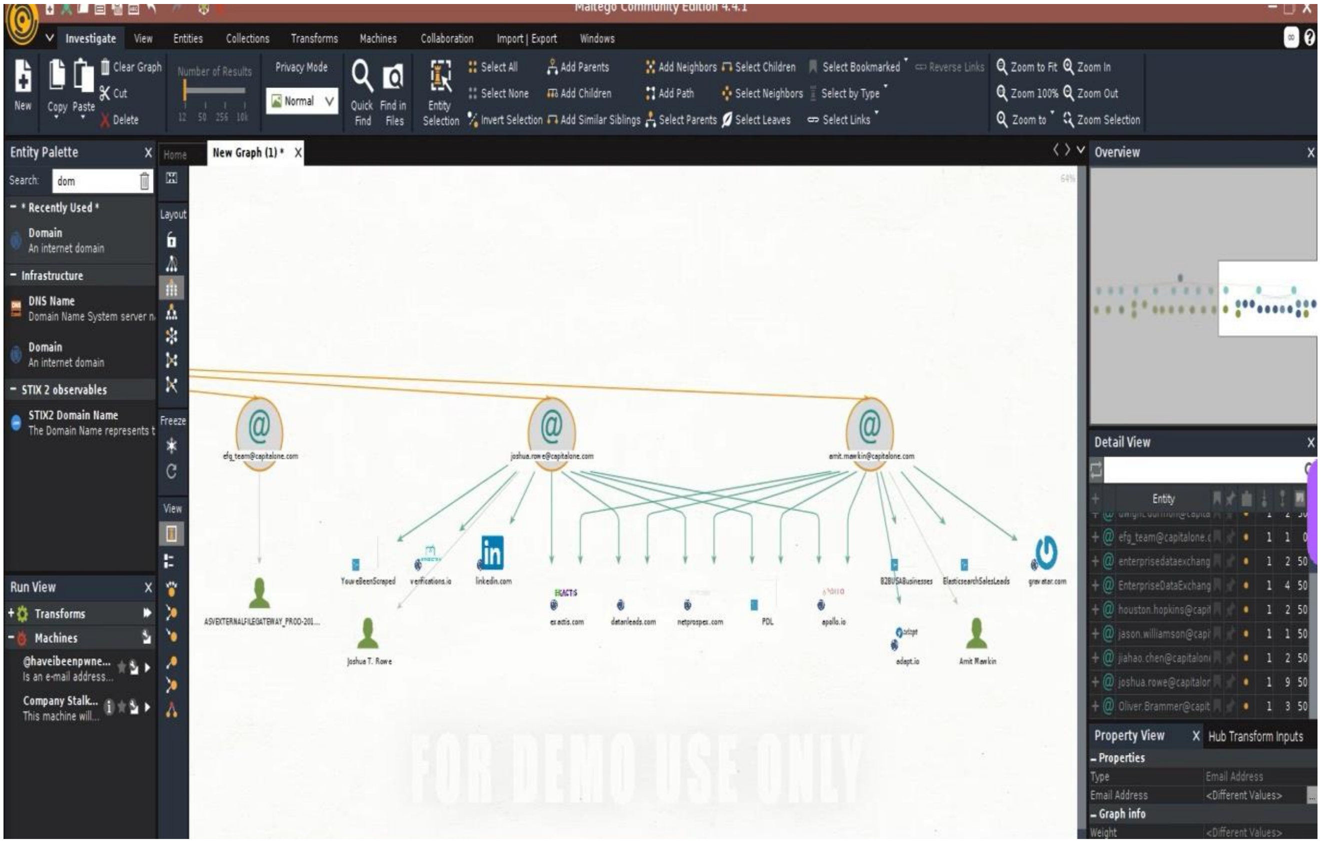
Tool; Maltego

- The whole data breach investigation was carried on by me on kali linux(Love of hackers).
- The main tool which was used is Maltego community edition(includes domain through internet).
- I was able to find emails or phone numbers related to any legal domain.
- After finding the emails a transform called "have i been pwned" is used.
- This transform helps us to find any kind of breached emails.
- In addition to this it gives information of the company involved in the breach and the names of the individuals related to the emails.
- Also i was able to find any kind of malware related to any domain through transform called "Polyswarm".

Some Screenshots of project


Maltego Community Edition 4.4.1
Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows
Entity Palette
Domain
DNS Name
STIX2 Domain Name
Run View
Transforms
Machines
Company Stalk...
Find Wikipedia ...
Footprint L1 CE
Footprint L2 CE
Footprint L3 CE
Footprint XXL CE
New Graph (1) *
capitalone.com
efg_team@capitalone.com
joshua.rowe@capitalone.com
cyber-adj@capitalone.com
EnterpriseDataExchangeSupportTe...
jason.williamson@capitalone.com
dwight.durmon@capitalone.com
amit.mawkin@capitalone.com
enterprisedataexchange@capitalo...
jiahao.chen@capitalone.com
houston.hopkins@capitalone.com
christopher.tompkins@capitalone...
Oliver.Brammer@capitalone.com
FOR DEMO USE ONLY
Overview
Detail View
Domain
maltego.Domain
capitalone.com
Relationships
Property View
Hub Transform Inputs
Type Domain
Domain Name capitalone.com
WHOIS Info
Graph info
Weight 0
Incoming 0
Output - Transform Output





Entity						
efg_team@capitalone.c			●	1	1	0
enterprisedataexchang			●	1	2	50
EnterpriseDataExchang			●	1	4	50
houston.hopkins@capit			●	1	2	50
jason.williamson@capi			●	1	1	50
jiahao.chen@capitalon			●	1	2	50
joshua.rowe@capitalor			●	1	9	50
Oliver.Brammer@capit			●	1	3	50

- Properties

Type	Email Address
Email Address	<Different Values>

- Graph info

Weight	<Different Values>