Threatlandscape

Access: Credentials

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022

In this presentation we focus on how malicious actors gain access to information assets.

Big Question

How do they gain access?

Big Question
How do they gain access?

Now that we know who all is out there, let us take a look at how they do what they do.
According to DBIR 2021 report, 85% of the breaches involved some sort of human involvement.
61% of the breaches involved credentials.

All Roads Lead to Information

- Credentials
  - Legitimate Credentials
  - Stolen Credentials
  - Bruteforce
- Vulnerabilities
  - Configuration
  - Bugs
- Human Element
  - Social Engineering
  - Insiders

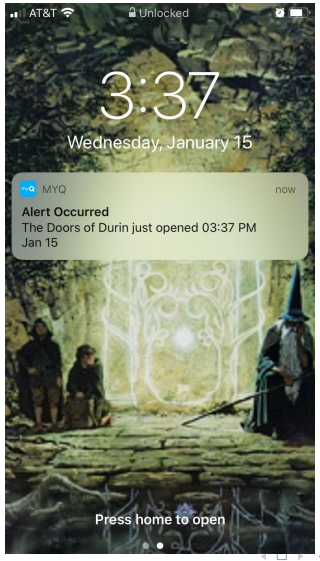
All Roads Lead to Information
Credentials
Legitimate Credentials
Stolen Credentials
Bruteforce
Vulnerabilities
Configuration
Bugs
Human Element
Social Engineering
Insiders

There are many ways to access information stored on our computing devices. Too many to cover with any real accuracy.

We will nevertheless cover the broad outlines of the most common ways of gaining access and ways of making these attacks less likely.

Credentials

- Legitimate Credentials
- Stolen Credentials
- Bruteforce



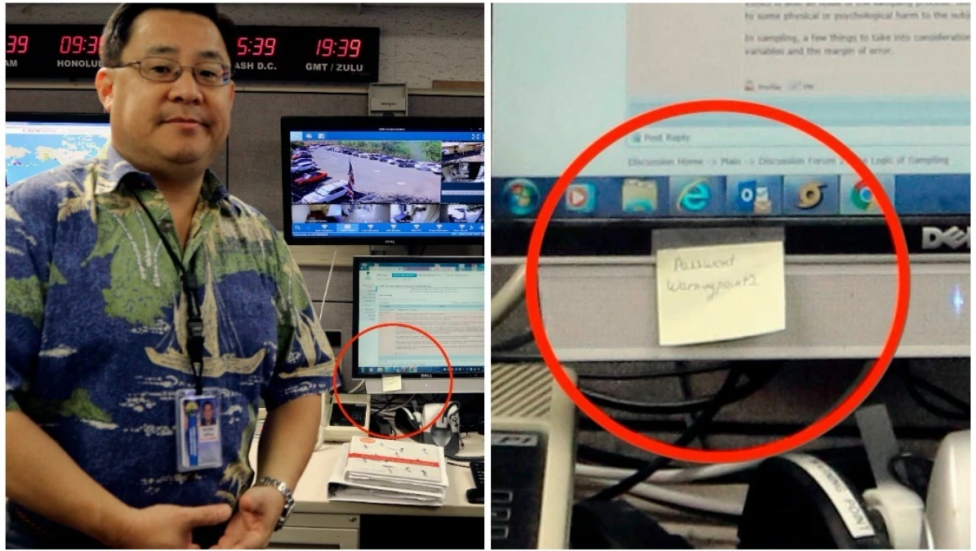
Our systems determine who has how much access based on the credentials presented.
Easiest way to gain access would be to have these credentials. Which is why Phishing attacks are always popular.

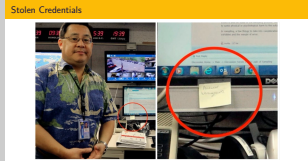
Insiders and Legitimate Credentials

Insiders and Legitimate Credentials

Organizations need people to carry out their business. This requires a certain level of trust, which is reflected in the access one is granted.
We trust that the employee will act with the organizations' best interest in mind with the access they are given. This is part of the employment contract afterall.
Problems arise when the employees are disgruntled, or conflicts with other interests arise.
For example in 2014, a contractor for NSA felt that public interest overrode the interests of the intelligence agency that employed him. He obtained thousands of classfied documents and revealed them to the press. The rest is history.
No matter what we may think of Edward Snowden and his actions, it is obvious that the process to grant and revoke credentials needs some consideration.

Stolen Credentials





When legitimate access is not an option, the next best thing is to borrow the credentials of someone who has access.

It can be a simple matter of reading what is written on the post-it notes. At this point there have been too many emergency agencies, police stations, and military units embarassed by revealing their passwords on live TV.

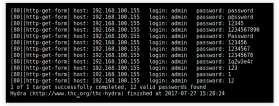
More often though, malicious actors will steal the passwords through phishing or cross site scripting.

Phishing is the practice of sending misleading e-mails to legitimate users. The e-mail may include a malware infected file, or a link to a phishing website. Very often when the user clicks the link they are redirected to a legitimate looking website, if they enter their password in this website the password will be passed onto the malicious actors. Similarly, the malware downloaded from phishing e-mails can establish backdoors on users' systems, or steal passwords stored on the system.

Brute Force

```
[80][http-get-form] host: 192.168.100.155   login: admin   password: password
[80][http-get-form] host: 192.168.100.155   login: admin   password: p@ssword
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567890
[80][http-get-form] host: 192.168.100.155   login: admin   password: Password
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123456
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345678
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```


Brute Force



Brute forcing a password is to throw computational power at the problem. You would try possible passwords until you find one that works.

Most systems that have remote access would have some mechanisms to make brute forcing a password difficult. System may time out or disable user account after certain number of tries for example.

Still, there are ways of brute forcing passwords such as password spraying, attacking a vulnerable protocol (SMB v1 and v2 are notorious), or brute forcing the passwords offline on stolen shadow files for example.

Some Ways to Keep Credentials Safe

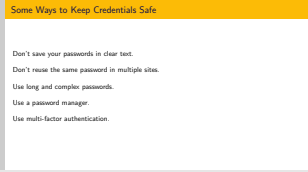
Don't save your passwords in clear text.

Don't reuse the same password in multiple sites.

Use long and complex passwords.

Use a password manager.

Use multi-factor authentication.



The proper action depends on the context. Correct control for a bank will not be the same as the corner pizzeria, which will not be the same for a high-school student. Generally though, these tips apply to almost everyone.

To make it harder to steal your credentials, don't store your passwords in clear text. Don't write them down on paper...

Sometimes a website will get hacked and the passwords for the users will be leaked. Then malicious actors may use the same password for the users' accounts on other web sites. You wouldn't want the bad guys to gain access to your bank account because some fan-fiction forum you subscribed to got hacked. So don't reuse the passwords across multiple sites.

To prevent brute forcing your passwords, use long and complex passwords that are a combination of lower, upper case letters, numbers, and symbols. You have these complex passwords that are hard to remember, and you also use a different one for each web site... This is getting hard to remember...

So use a password manager with a really good master-password to keep all those hard to remember passwords safe.

Also use multifactor authentication so that even if your password is stolen, or brute-forced you