

Threatlandscape

Access: Credentials

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022

This work is licensed under a Creative Commons Attribution 4.0 International License.

Big Question

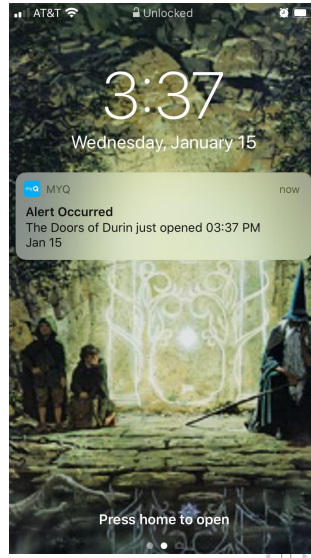
How do they gain access?

All Roads Lead to Information

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

Credentials

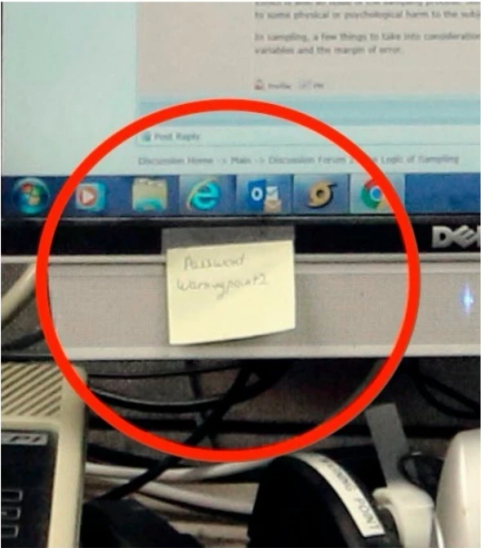
- Legitimate Credentials
- Stolen Credentials
- Bruteforce



Insiders and Legitimate Credentials



Stolen Credentials



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
```

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.