Cyber Security Round-up 2020

Port Nicholson Rotary Club
Simon Howard
9 September 2020

Introduction

- Owner and Technical Manager @ ZX Security
- Penetration testing firm based in Wellington
  - “We hack stuff”
- 24 staff with a variety of specialist skills

Presentation overview

- **Risks** with giving increased numbers of staff remote access to the network
- What’s 🔥 in the **cyber crime** world
- Compromised environment **case studies** during lockdown
- Insight into what a **hacker** actually does on your network
- **Security controls** you can put in place

Risks

Risks – Poor Passwords

- Staff member chooses a **poor password** (or reuses passwords), resulting in an **attacker guessing** it and **gaining access** to your systems

Risks – Lack of Two-factor Authentication

- Users **password** is **phished** (or **guessed**) but there is **no two-factor authentication** in place to **stop** a **malicious** user from accessing the **victims account**

Risks – Compromised Home User

- Staff members **home device** is **compromised** due to **poor hygiene**, when they **access** the **network** via remote access the **attacker gains access** too

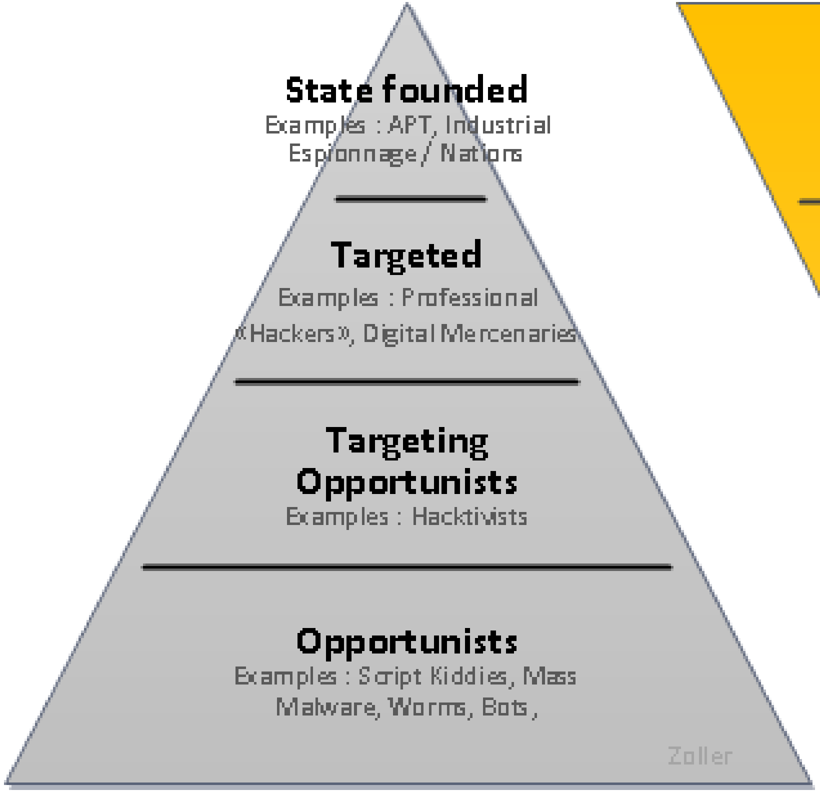
Risks – Unpatched Systems

- You **forgot** to **patch** your **remote access software** and an attacker uses a published **vulnerability** to **gain access** to your network

Risk – Backups Failed / Non-existent

- You aren’t performing **on-site**, and/or **off-site backups**
- **Restoring** from backups **failed**
- You just got ransomwared, went to check your backups and realised they **haven’t been running** for 7 months. 😱

Case Studies & Insight



State founded
Examples : APT, Industrial Espionnage / Nations

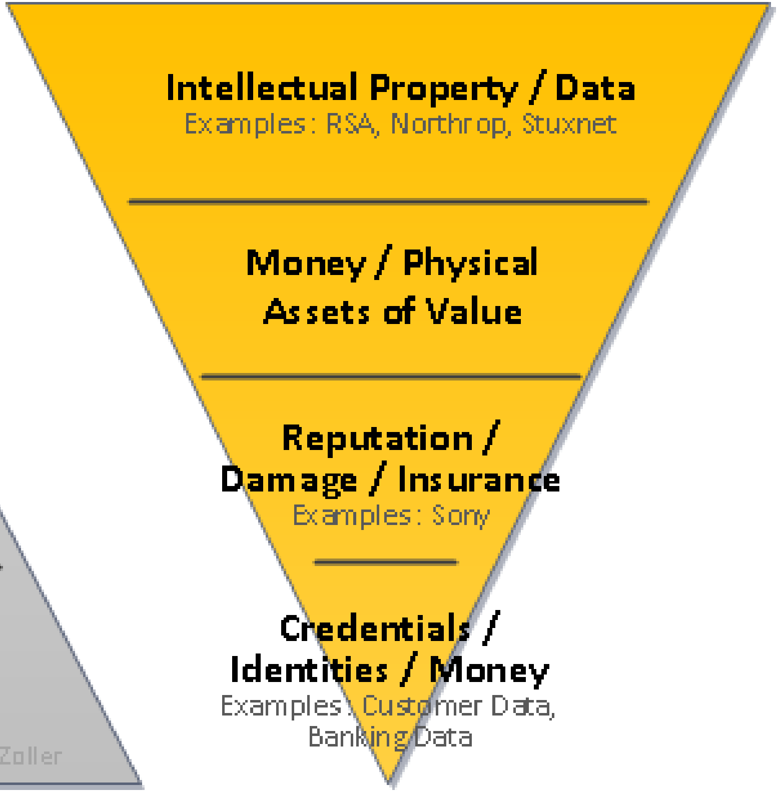
Targeted
Examples : Professional «Hackers», Digital Mercenaries

Targeting Opportunists
Examples : Hacktivists

Opportunists
Examples : Script Kiddies, Mass Malware, Worms, Bots ,

Zoller

Name → Attacker Class
Surface Area → Amount



Intellectual Property / Data
Examples : RSA, Northrop, Stuxnet

Money / Physical Assets of Value

Reputation / Damage / Insurance
Examples : Sony

Credentials / Identities / Money
Examples : Customer Data, Banking Data

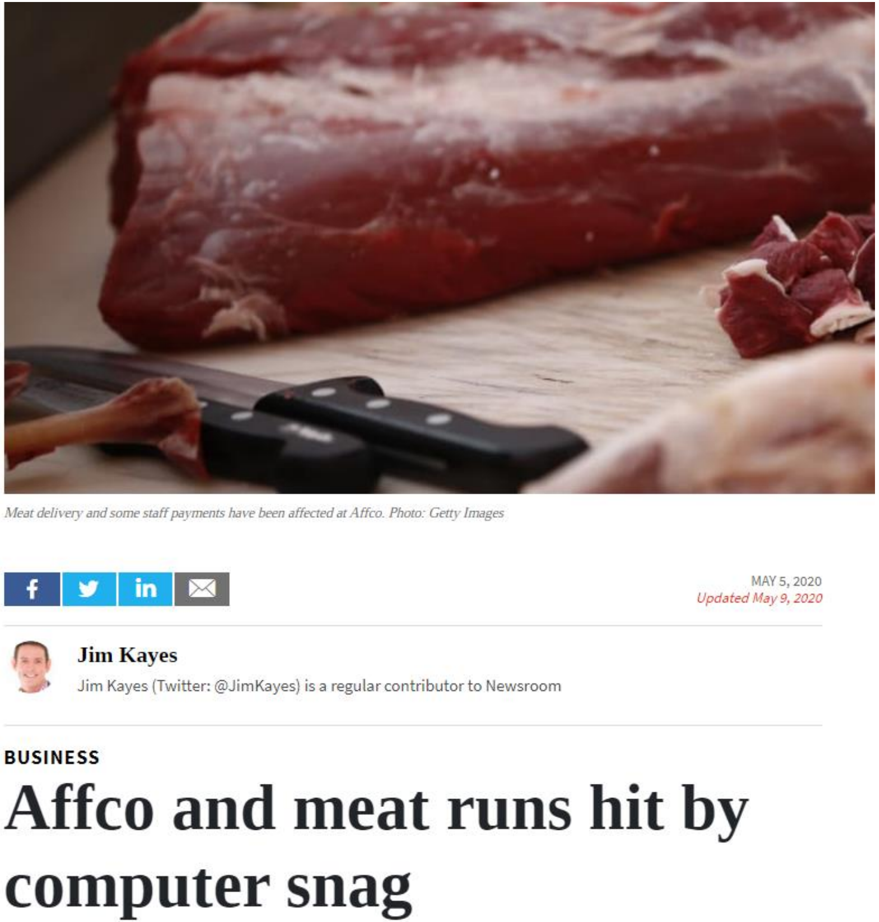
Name -> Typical Targeted Asset
Surface Area -> Value

Targeted – SIM swapping

- CERT NZ received a cluster of reports of **SIM swapping attacks** in Q4 2019, where attackers were able to **gain access** to the victim's **online bank accounts**.
- Around **10 attacks were carried** out
- The average **financial loss** from these attacks was **$30,000**.

What is SIM Swapping?

- SIM swap attacks (also known as SIM porting or SIM hijacking) are where an attacker uses **social engineering techniques** to **manipulate a mobile phone provider** into **porting** a **mobile phone** number from a genuine **customer's SIM** card to the **attacker's SIM** card.
- The attacker can then **receive all SMS messages** and **voice calls** intended for that customer.



Meat delivery and some staff payments have been affected at Affco. Photo: Getty Images

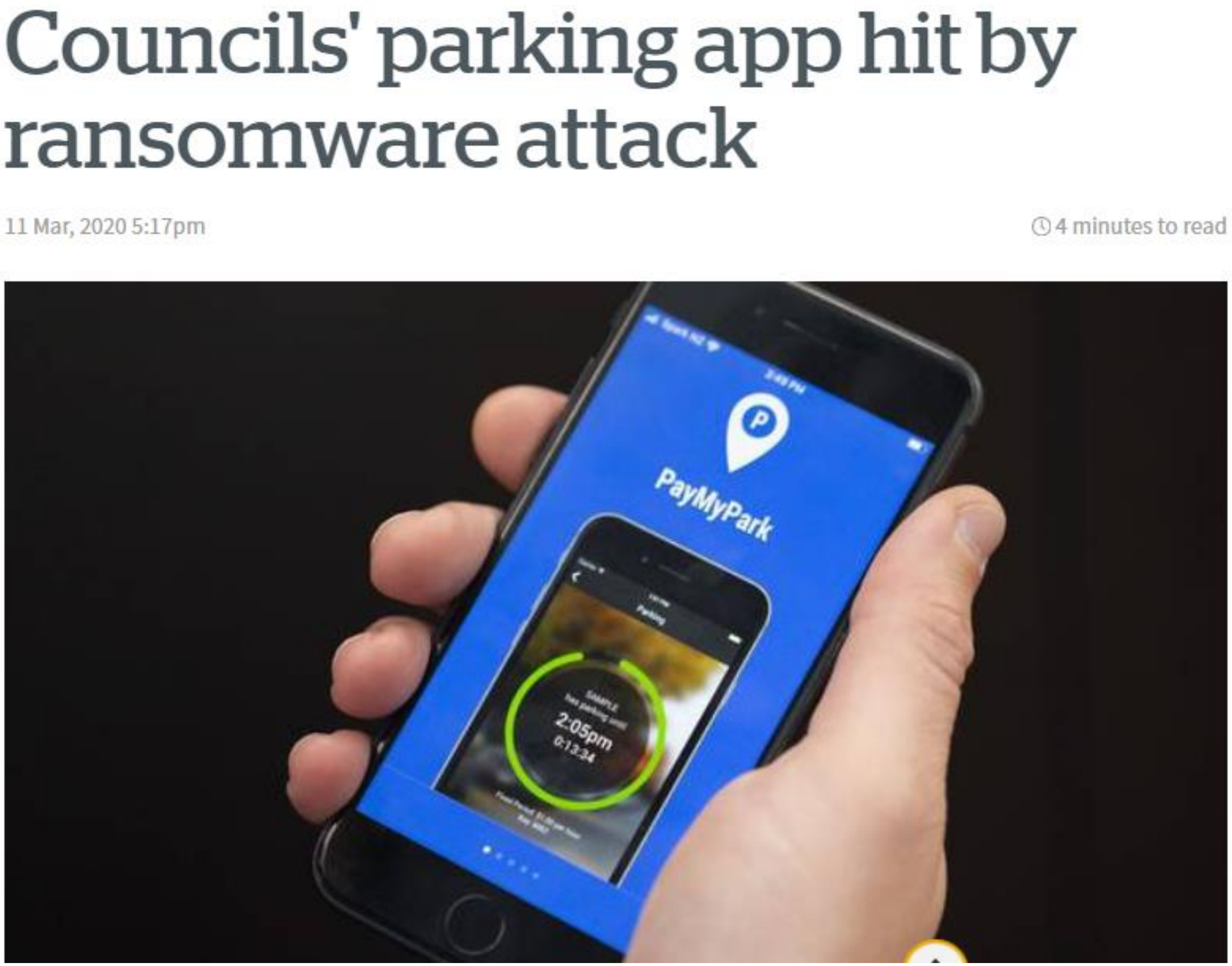
MAY 5, 2020
Updated May 9, 2020

Jim Kayes

Jim Kayes (Twitter: @JimKayes) is a regular contributor to Newsroom

BUSINESS

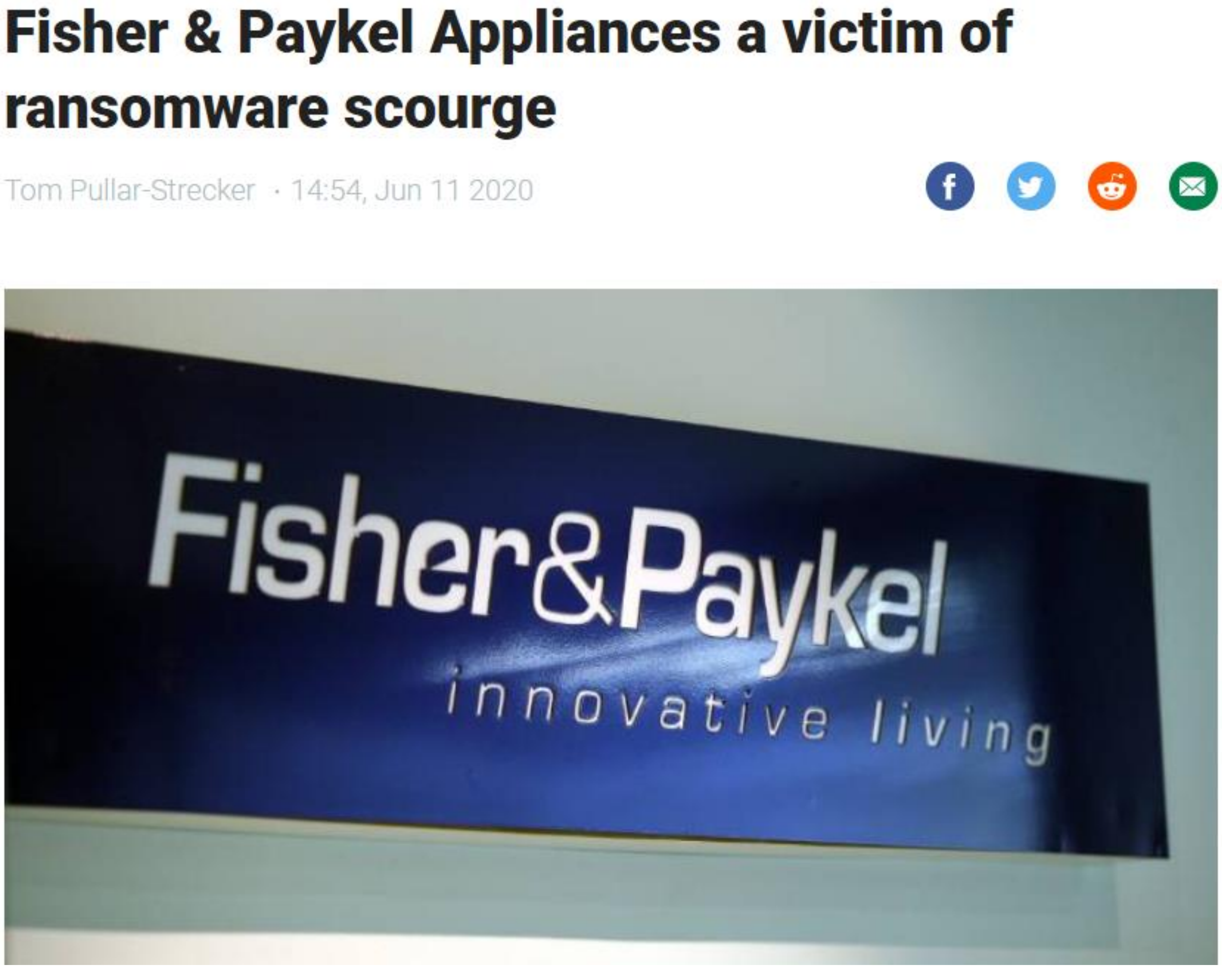
Affco and meat runs hit by computer snag



Councils' parking app hit by ransomware attack

11 Mar, 2020 5:17pm

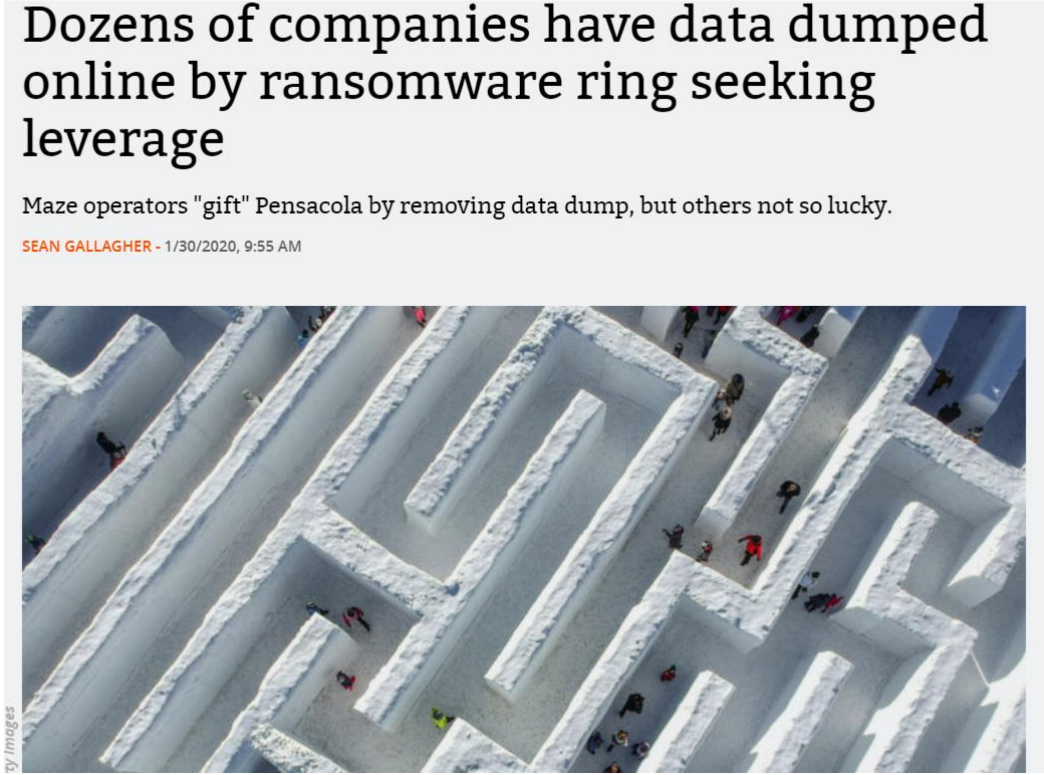
4 minutes to read



Fisher & Paykel Appliances a victim of ransomware scourge

Tom Pullar-Strecker · 14:54, Jun 11 2020

Change in ransomware crew modus operandi



Dozens of companies have data dumped online by ransomware ring seeking leverage

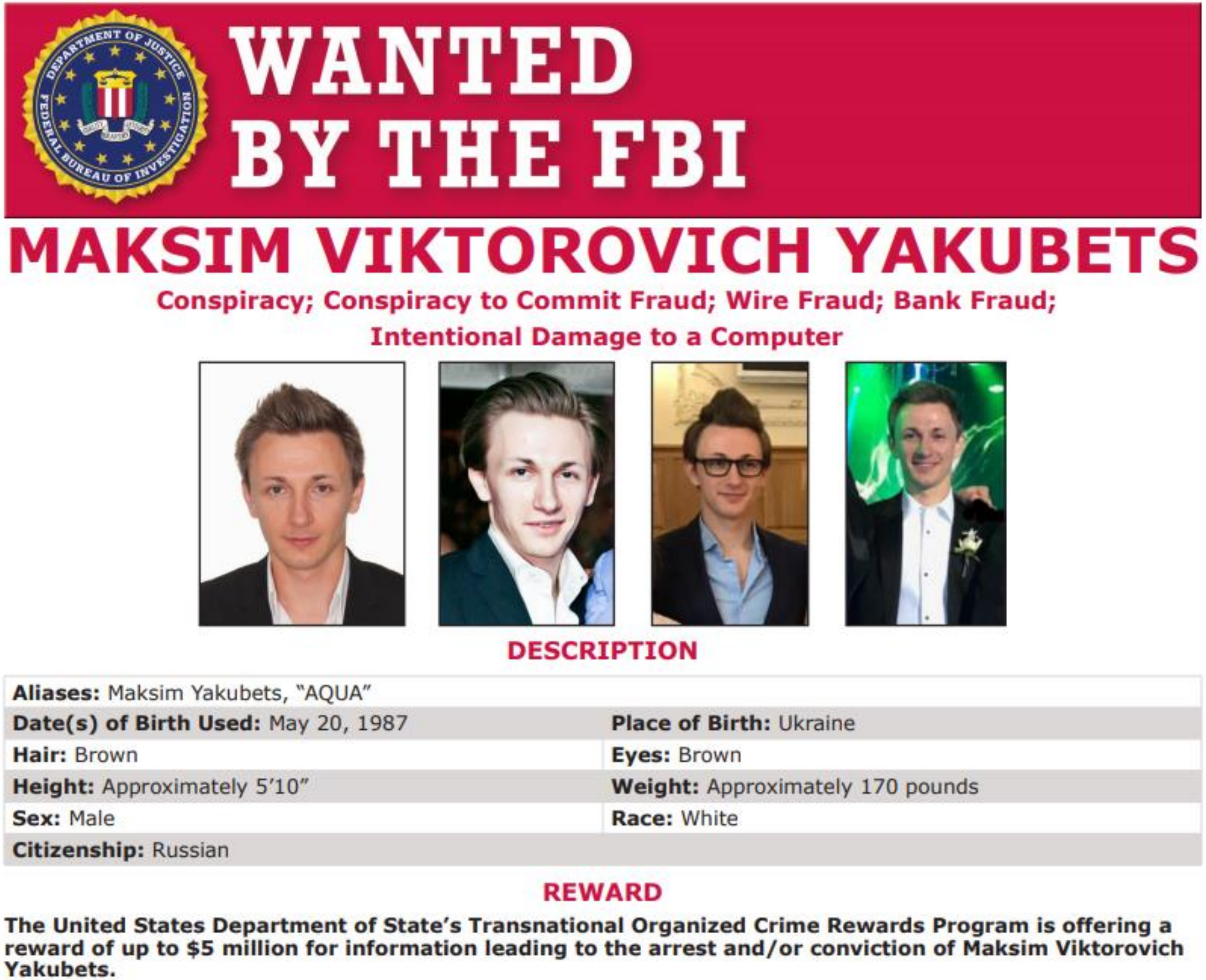
Maze operators "gift" Pensacola by removing data dump, but others not so lucky.

SEAN GALLAGHER - 1/30/2020, 9:55 AM

ty Images

DOJ running a bounty program

- The U.S. Justice Department offered a **$5 million bounty** for information leading to the **arrest** and **conviction** of a **Russian** man indicted for allegedly orchestrating a vast, international cybercrime network that called itself “**Evil Corp**” and **stole** roughly **$100 million** from businesses and consumers.



WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

Legality's of paying ransoms

- The **Treasury Department’s** role in this action is key because it means the **United States** has now imposed **economic sanctions** on **Yukabets** and 16 accused associates, making it a **crime** to **transact with them**

Tues 1
10
10
25
38
LIGHT
UP
DOWN
START
STOP
BACK
GARMIN

Garmin

- Garmin systems were down for days
- No customer communication
- Ransom rumored to be $10 million
- In big trouble with treasury dept. for paying the ransom
- Payment was reportedly made via an intermediary called Arete IR

Arete
Incident Response

Garmin Pays Up to Evil Corp After Ransomware Atta Reports

Case Study - Ransomware

- During lockdown an environment was compromised and a large number of servers had Ransomware installed on them
- The attacker brute-forced a users Citrix (remote access) password, accessed the network and began installing the ransomware

What is a password brute force?

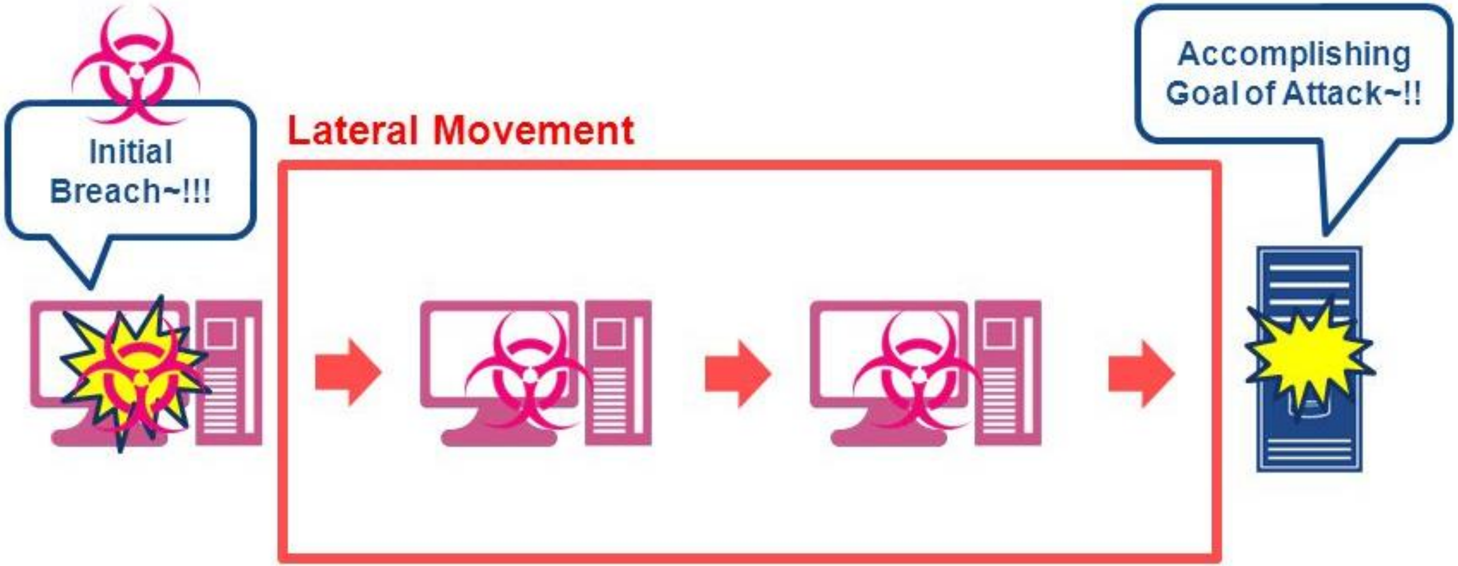
- We find the systems you are running on the internet
  - Outlook Web Access
  - Remote Access
- We find a list of your staff
  - LinkedIn
  - Corporate website
- We try really dumb passwords, slowly, until one works.

During the penetration test it was possible to guess more than **30 users**’ **passwords**, weak examples included ”**Welcome1**” and ”**Password1**”.

What’s next?

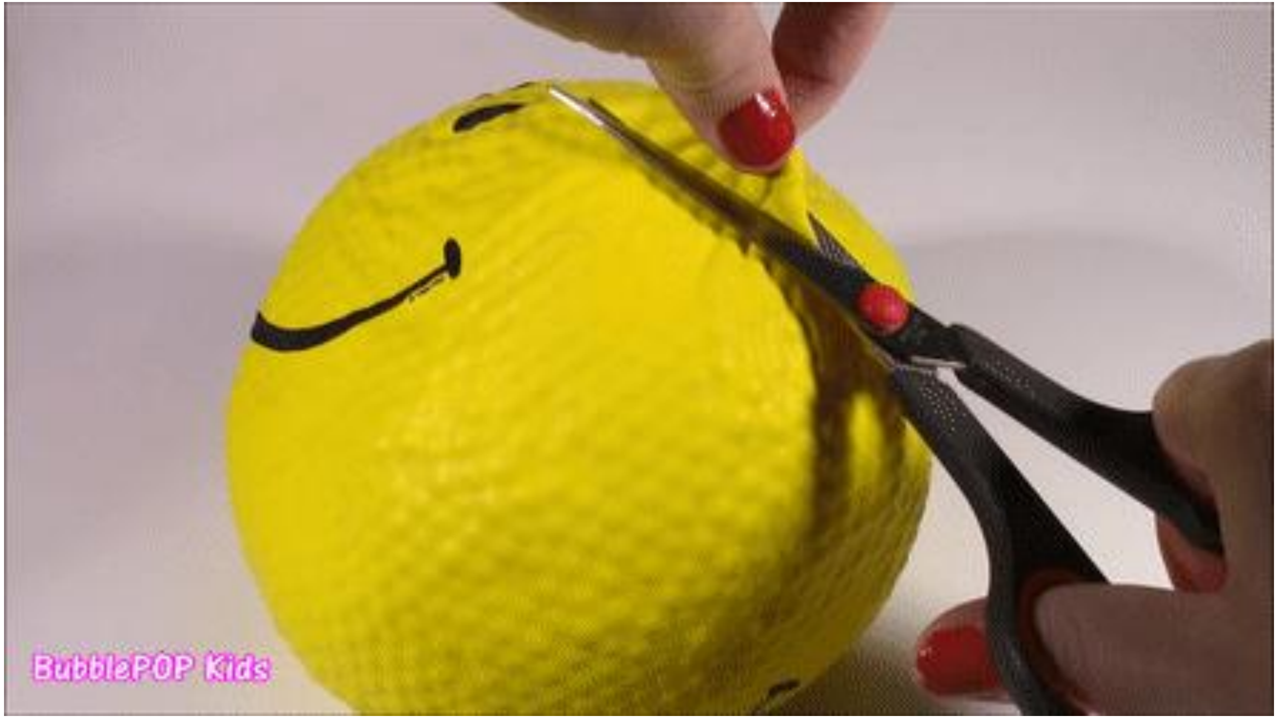
- If we were bad..
  - We might commit some form of fraud based on the account we got access to (email)
  - Or install ransomware (if we have remote)
- If we are smarter, we might go after some data on the network, so we need to start “pivoting” now.

What is pivoting?



Customers network – hard on the outside

Soft’n’squishy on in the inside



Within three hours of the password cracking beginning, ZX Security obtained passwords for

3798 accounts, out of a possible **5843**.

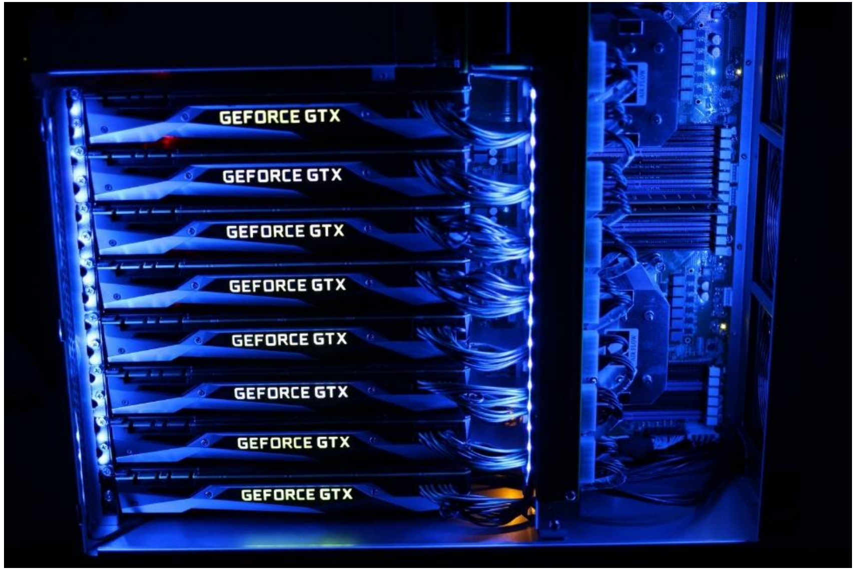
This is **over 65%** of accounts

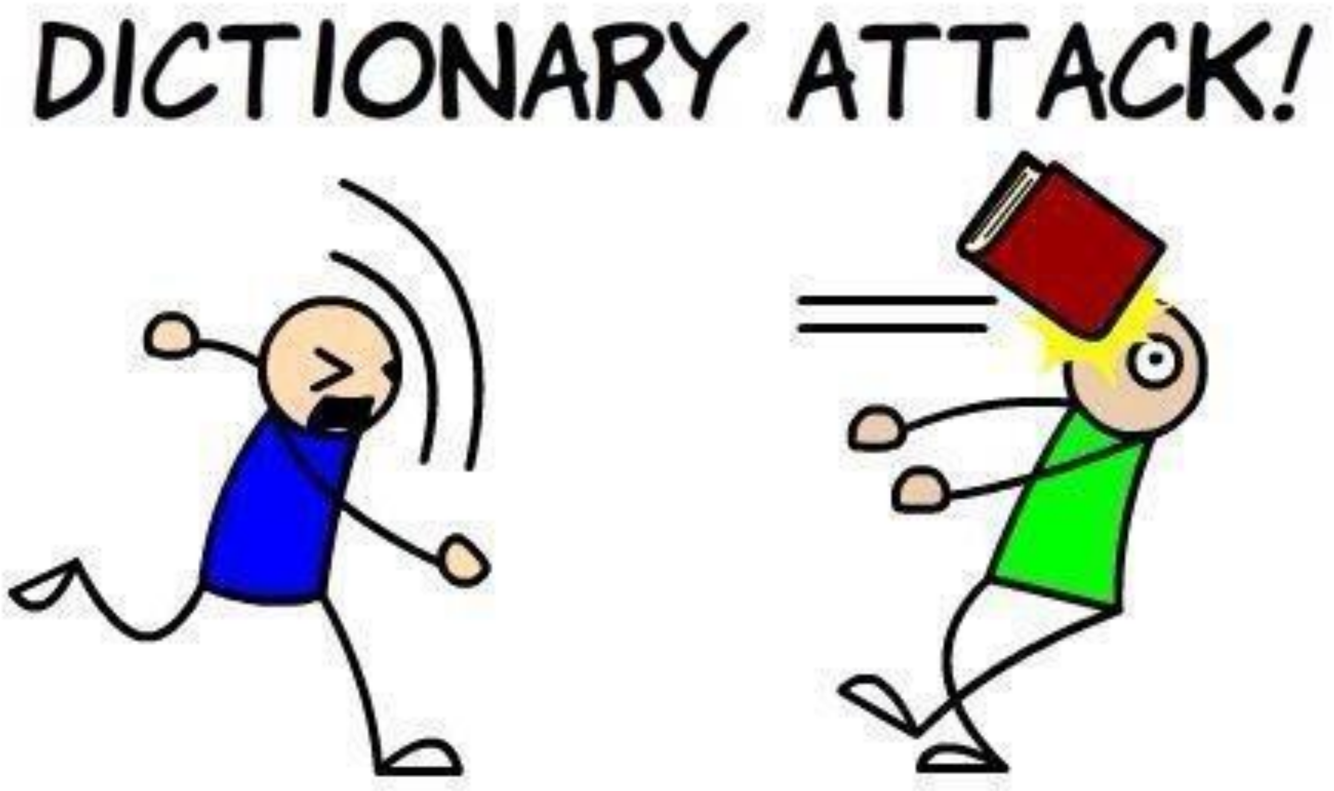
Of the 5843 total password hashes, **two particularly bad cases** of password duplication identified were:

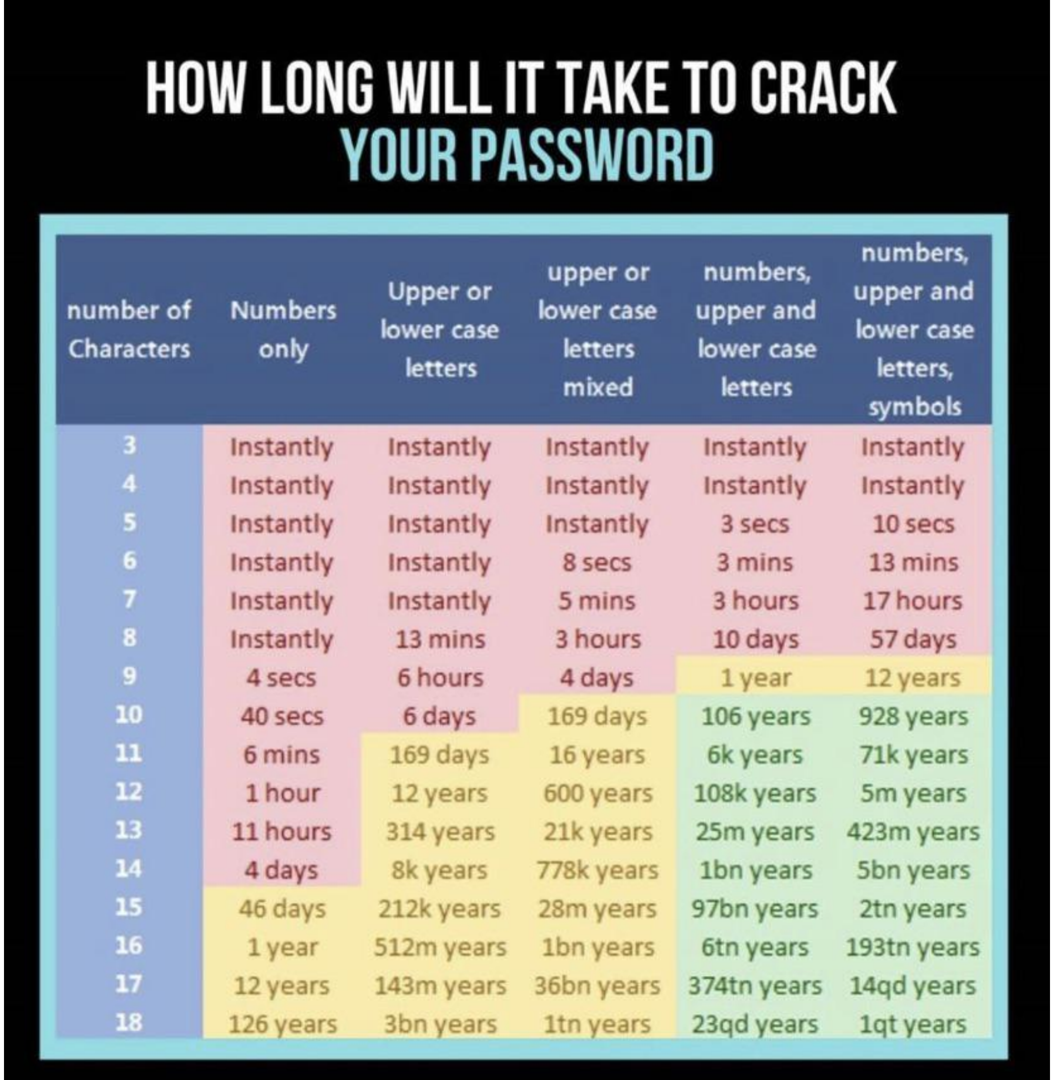
- company_name01 - **used 284** times
- Company_name01 - **used 113** times

What is password cracking

- We obtain a copy of the encrypted passwords
- Using the combined power of multiple CPU’s or graphics cards, we make guesses at the password
- At a rate of 38,000 million guesses a second



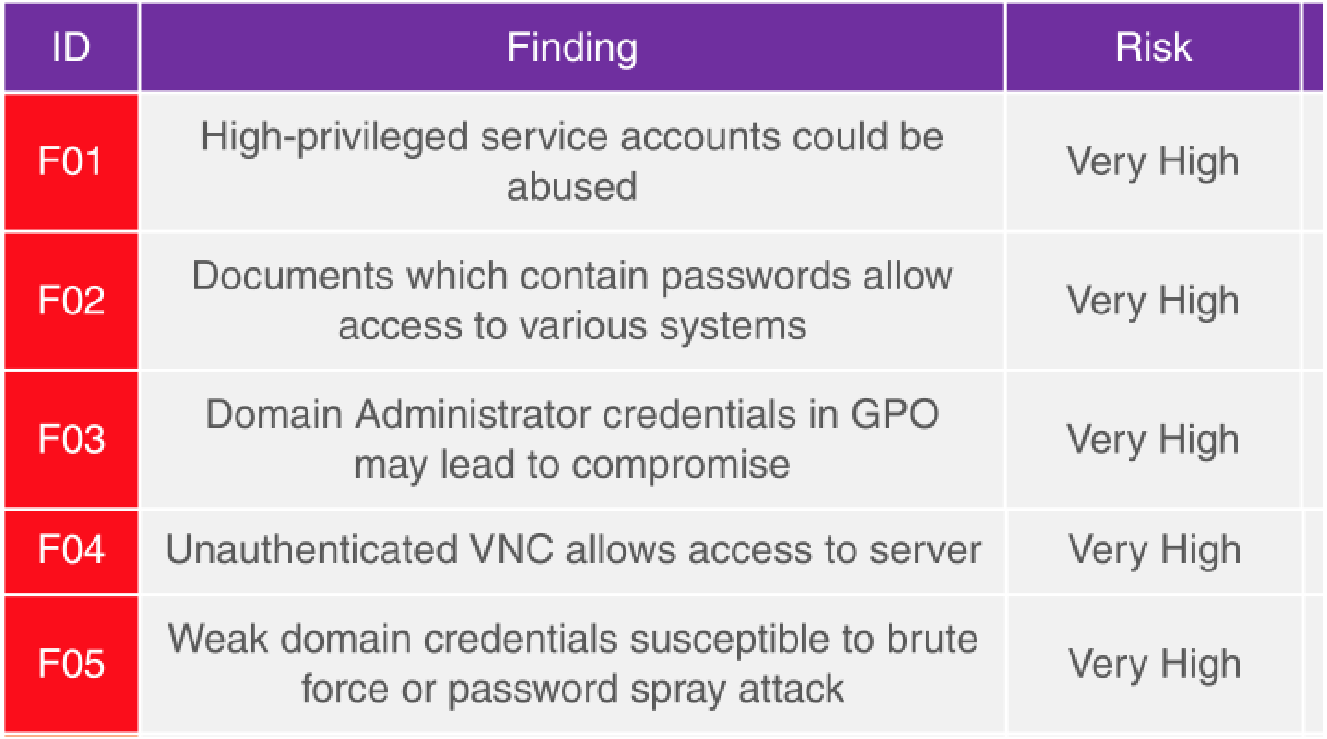

DICTIONARY ATTACK!



HOW LONG WILL IT TAKE TO CRACK YOUR PASSWORD

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

So very squishy



ID	Finding	Risk
F01	High-privileged service accounts could be abused	Very High
F02	Documents which contain passwords allow access to various systems	Very High
F03	Domain Administrator credentials in GPO may lead to compromise	Very High
F04	Unauthenticated VNC allows access to server	Very High
F05	Weak domain credentials susceptible to brute force or password spray attack	Very High

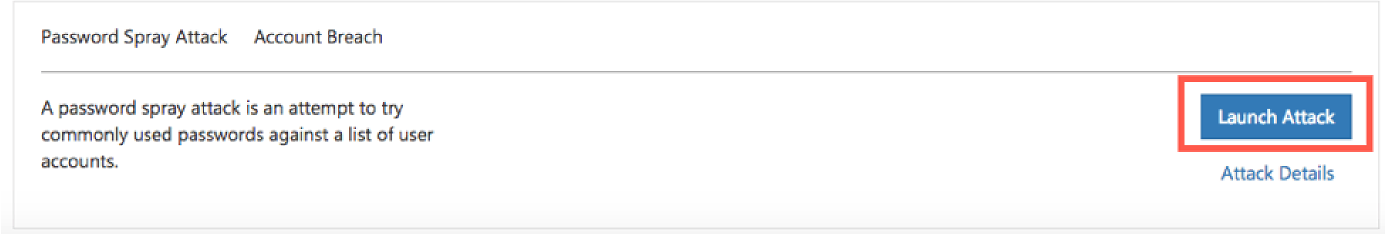
Security Controls

ZXSECURITY.CO.NZ

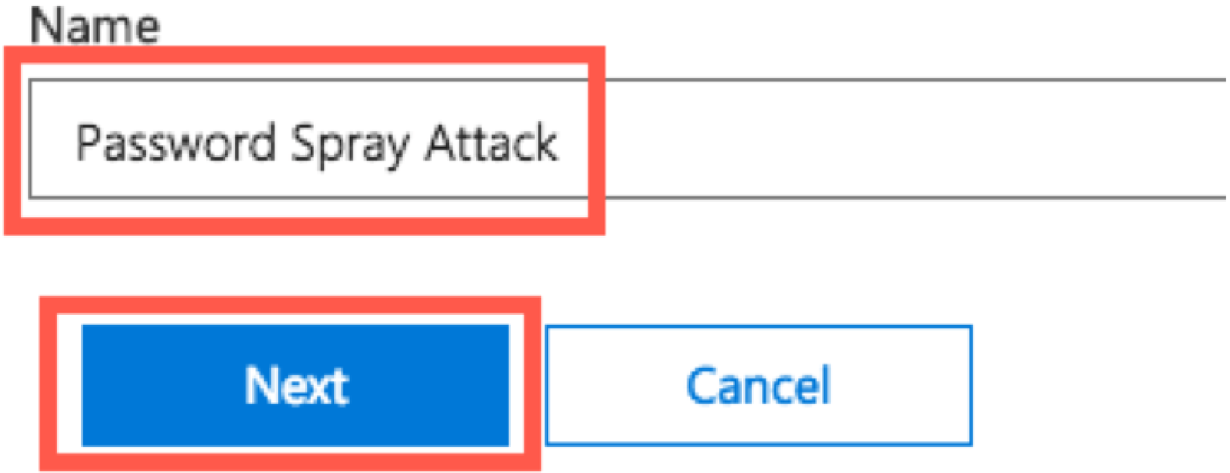
Security Control – Password Policy

- 10 characters minimum
- Force reset all passwords – ensuring all accounts are updated
- Remove aging requirements – these don't make passwords better
- Don't allow users to set easily guessed passwords (that still meet your complexity requirements)
- Test yourself with a password spray!

Microsoft Attack Simulator – Password Spray Attack

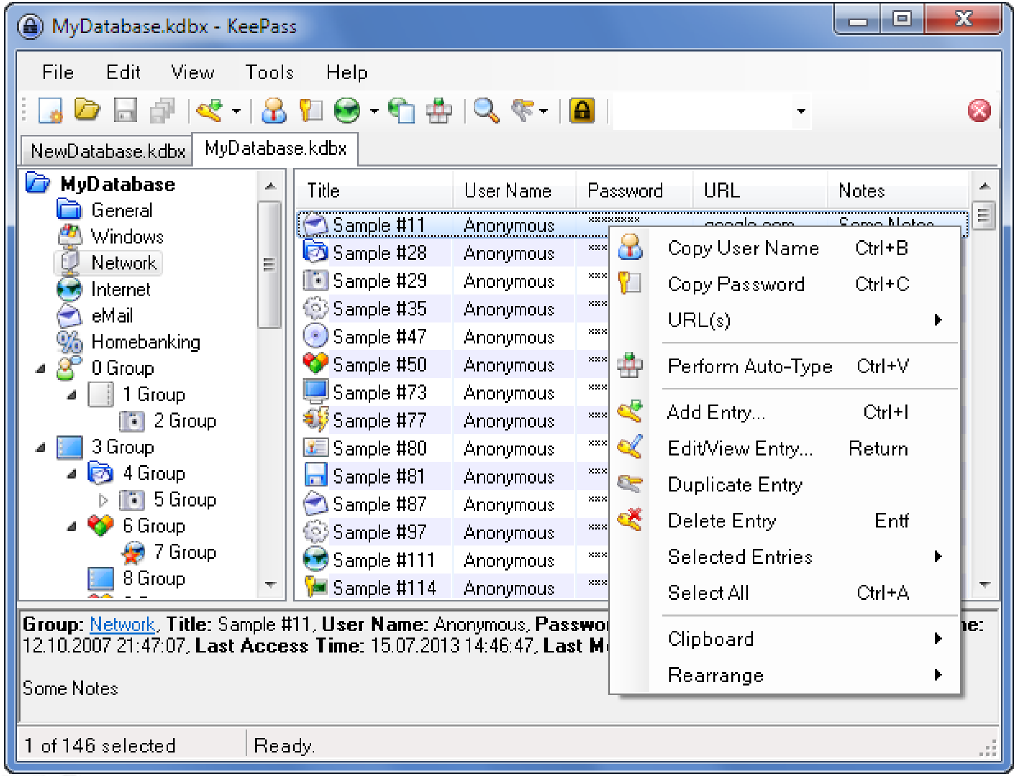


A password spray attack is an attempt to try commonly used passwords against a list of user accounts.



Name: Password Spray Attack

Security Control - Password Manager

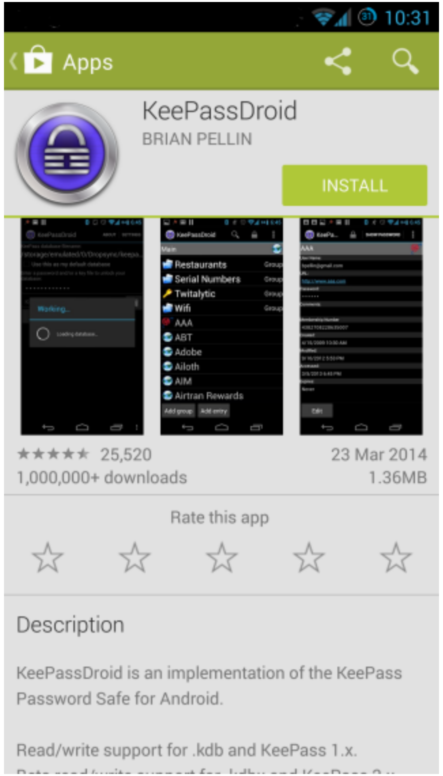


Title	User Name	Password	URL	Notes
Sample #11	Anonymous	********	google.com	Some Notes
Sample #28	Anonymous	***		
Sample #29	Anonymous	***		
Sample #35	Anonymous	***		
Sample #47	Anonymous	***		
Sample #50	Anonymous	***		
Sample #73	Anonymous	***		
Sample #77	Anonymous	***		
Sample #80	Anonymous	***		
Sample #81	Anonymous	***		
Sample #87	Anonymous	***		
Sample #97	Anonymous	***		
Sample #111	Anonymous	***		
Sample #114	Anonymous	***		

Group: Network, **Title:** Sample #11, **User Name:** Anonymous, **Passwo** ... **ne:** 12.10.2007 21:47:07, **Last Access Time:** 15.07.2013 14:46:47, **Last M**

Some Notes

1 of 146 selected | Ready.



KeePassDroid

BRIAN PELLIN

★★★★★ 25,520 | 23 Mar 2014

1,000,000+ downloads | 1.36MB

Description

KeePassDroid is an implementation of the KeePass Password Safe for Android.

Read/write support for .kdb and KeePass 1.x.

Security Control – Poor Hygiene

- Use Microsoft tools (InTune) or Remote Access policy to ensure staff meet a minimum standard before connecting via remote access
  - Windows 10
  - Latest patches installed
  - Microsoft Defender (antivirus) installed + up to date

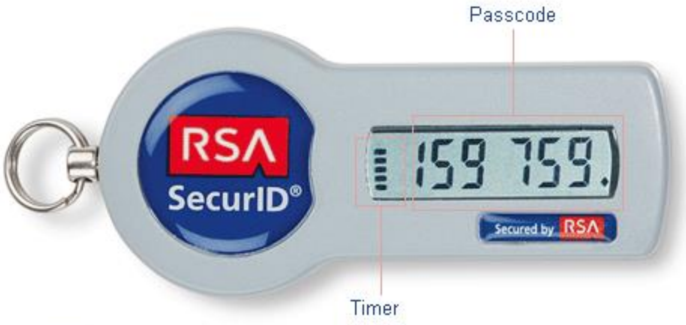
Security Control – Unpatched Systems

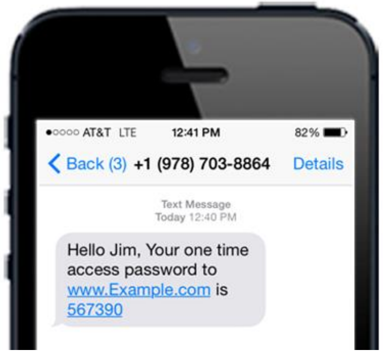
- Ensure someone is receiving security alerts from the vendor any that makes your remote access product
- Any security updates are either installed automatically, or within 48 hours of release (sooner if you can manage it)

Security Control – Browsers

- Use an adblocker like uBlock Origin
- Use private mode in your browser
  - Banking
  - Accounting

Security Control - Two-factor Authentication

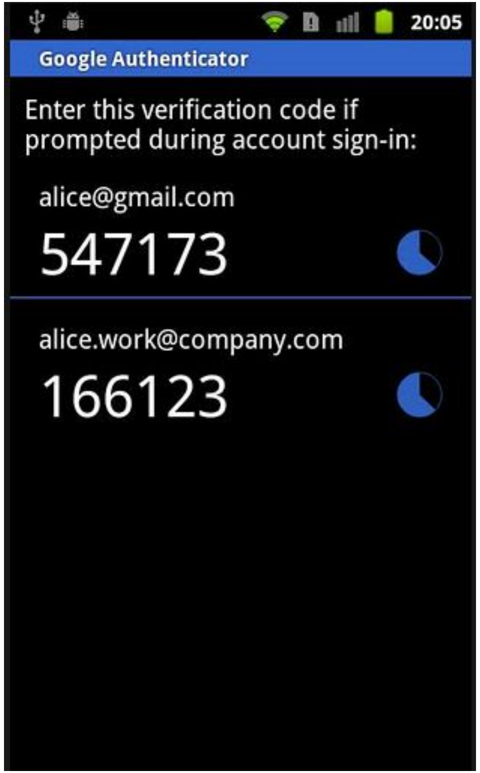



●○○○○ AT&T LTE 12:41 PM 82%

< Back (3) +1 (978) 703-8864 Details

Text Message
Today 12:40 PM

Hello Jim, Your one time access password to www.Example.com is 567390


20:05

Google Authenticator

Enter this verification code if prompted during account sign-in:

alice@gmail.com

547173

alice.work@company.com

166123

Security Control - Two-factor Authentication

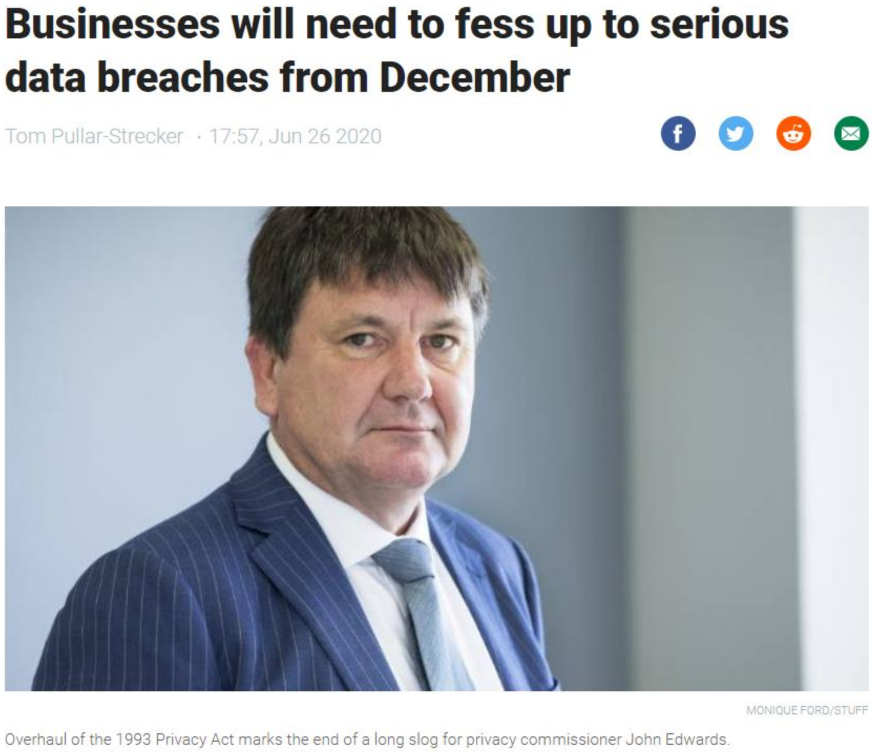
- SMS for 2FA is better than nothing
- But if the option is available, consider using an alternative method (e.g. apps)

Backups

- Backups, backups, backups
  - Dropbox, Onedrive, Google Drive
- Backups

Conclusion

NZ finally has a stick to whack naughty businesses with



Businesses will need to fess up to serious data breaches from December

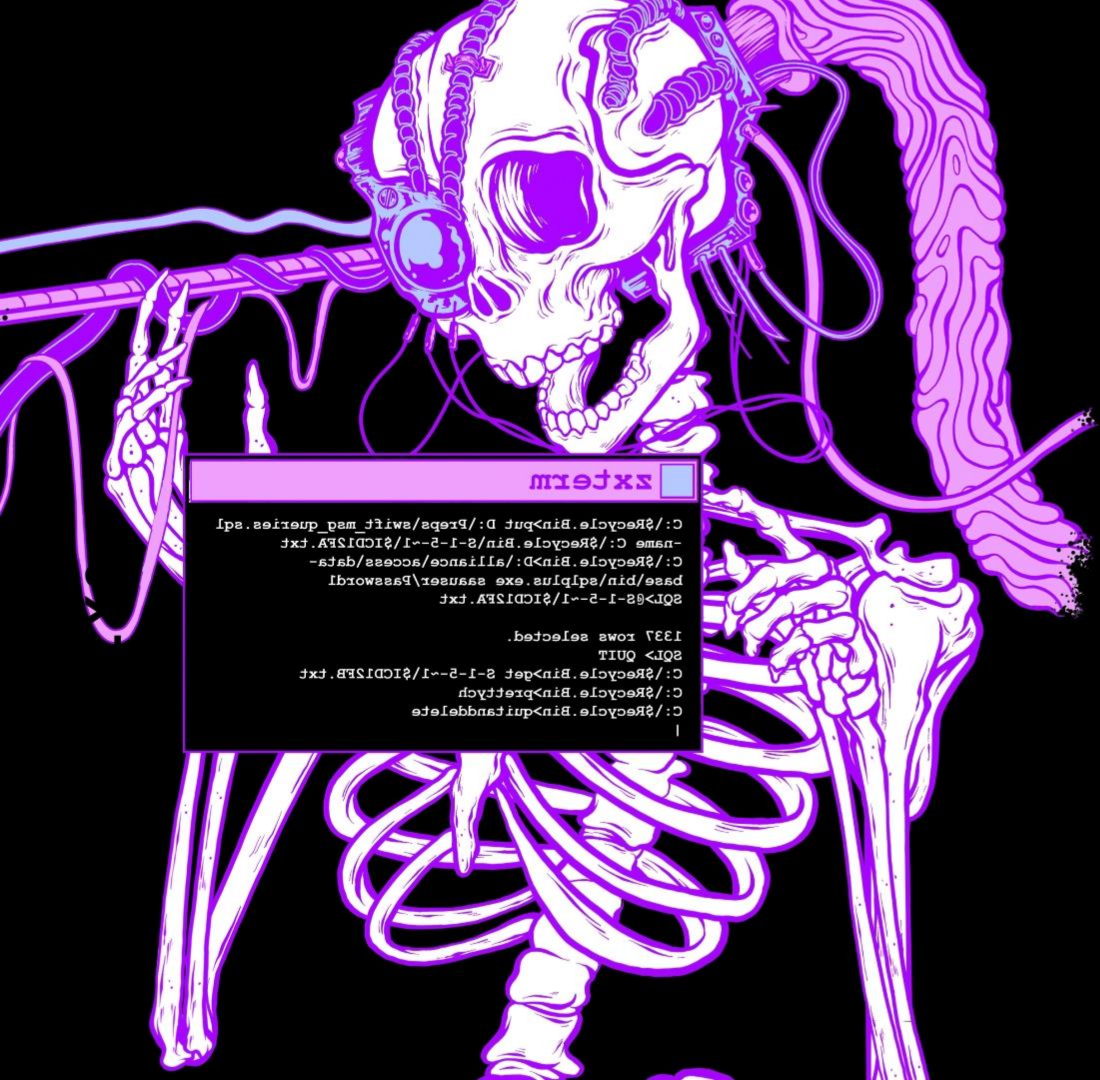
Tom Pullar-Strecker · 17:57, Jun 26 2020

MONIQUE FORD/STUFF

Overhaul of the 1993 Privacy Act marks the end of a long slog for privacy commissioner John Edwards.

Mandatory Data Breach Disclosure

- Even though the fine is moderate - $10,000
- The reputational risk is far worse
- Don’t be the example
- Invest some of that profit in your IT systems
  - Its better to be proactive than reactive
- Cyber security isn’t there to increase your value, its there to retain it.



```
C:/$Recycle.Bin>put D:/Preps/swift_msg_queries.sql
-name C:/$Recycle.Bin/S-1-5-~1/$ICD12FA.txt
C:/$Recycle.Bin>D:/alliance/access/data-
base/bin/sqlplus.exe saauser/Password1
SQL>@S-1-5-~1/$ICD12FA.txt

1337 rows selected.
SQL> QUIT
C:/$Recycle.Bin>get S-1-5-~1/$ICD12FB.txt
C:/$Recycle.Bin>prettych
C:/$Recycle.Bin>quitanddelete
|
```

Thank You

Email: simon@zxsecurity.co.nz
LinkedIn: Simon Howard
Twitter: @bogan

Website: zxsecurity.co.nz