



# Cybersecurity in a broken world

---

Elf Eldridge  
ZX Security  
July 2021  
[elf@zxsecurity.co.nz](mailto:elf@zxsecurity.co.nz)  
[@kaiwhata](#)

# Agenda: *'a security symphony in six parts'*

1. Introduction, Context & Data Sources
2. Biggest 2021 cybersecurity stories
3. What to do about it?
4. ZX Greatest Hits 2021
5. Azure and AWS
6. FAQs: bug bounties, culture, OSINT, NZISM, awareness



# Part 1: Introduction, Context and Data Sources

---

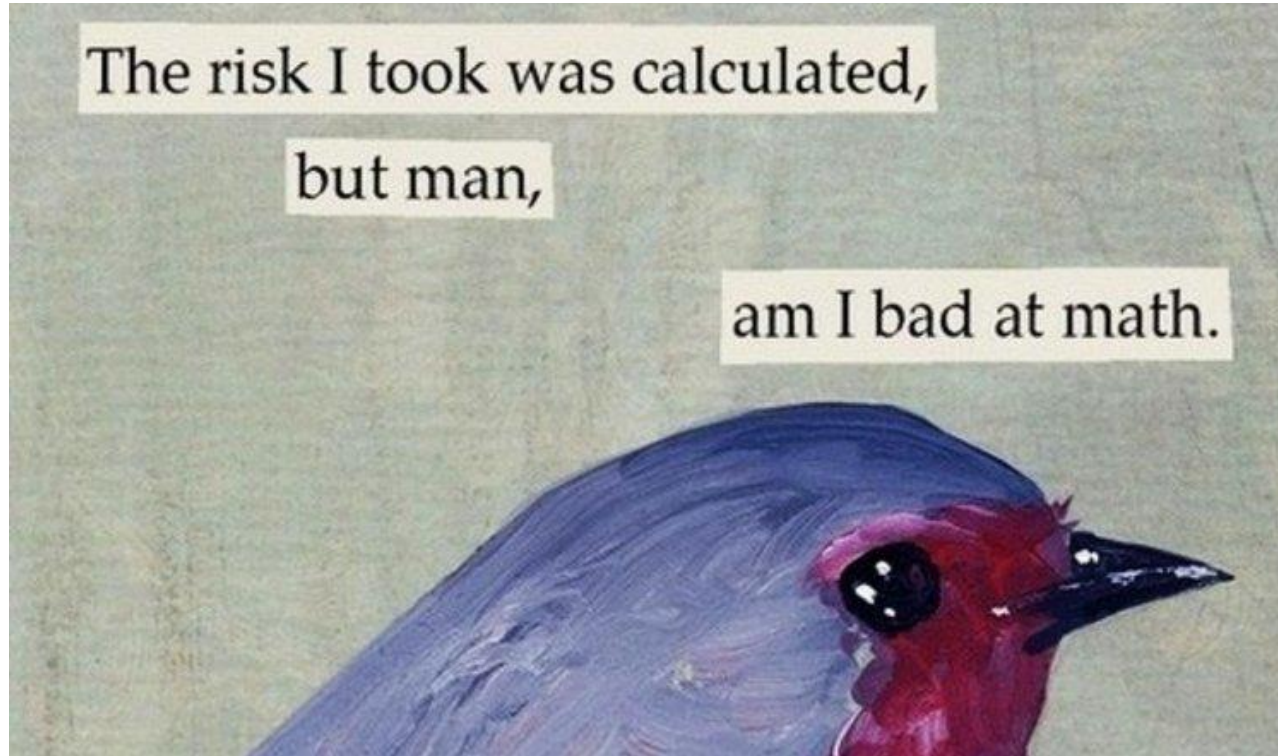
Elf Eldridge  
ZX Security  
July 2021  
[elf@zxsecurity.co.nz](mailto:elf@zxsecurity.co.nz)

# About Me / ZX Security

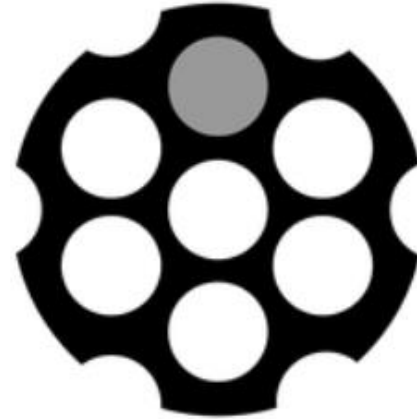
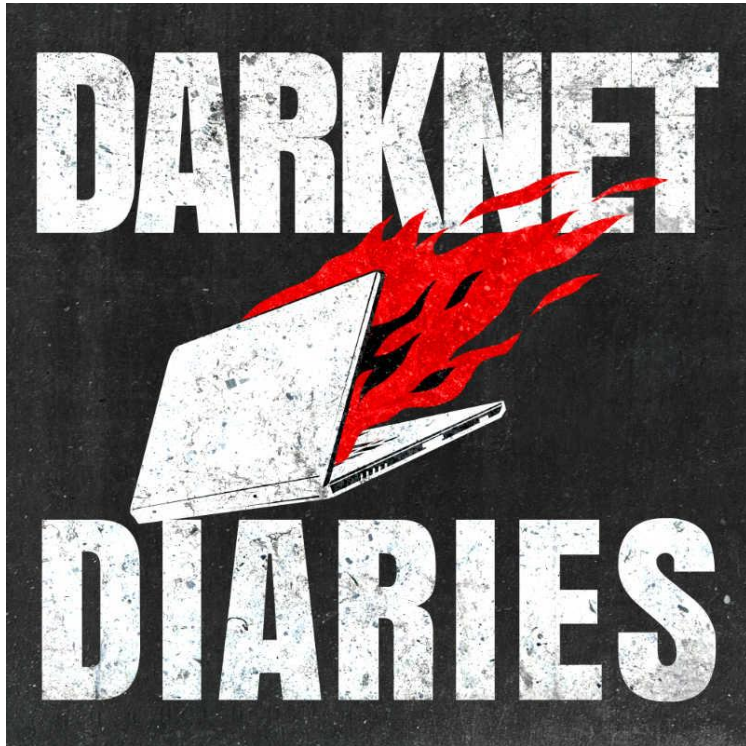
- Security Consultant @ ZX Security
  - Penetration Tester/Process Review
- Penetration testing firm
  - “We hack stuff”
  - Red team engagements - external / internal assessment
  - Cloud reviews (Office365, Azure, AWS)
  - Web application testing
  - Mobile application testing



# Humans vs Risk



# Keeping Up to Date



**RISKY.BIZ**  
It's a jungle out there

(sitemap)~\$ type to search



# Part 2: Biggest Cybersecurity Stories of 2021

---

Elf Eldridge

ZX Security

July 2021

[elf@zxsecurity.co.nz](mailto:elf@zxsecurity.co.nz)



ONLINE SECURITY ●

## Colonial Pipeline hackers only needed one password, CEO tells senators

09/06/2021

Reuters





**FINANCIAL**

# Ransomware strikes AXA shortly after insurer announces it will stop covering extortion fees



**HEALTHCARE**

# Irish Prime Minister says government won't pay ransom after hack forces hospitals to alter services





## Microsoft IOC Detection Tool for Exchange Server Vulnerabilities

Original release date: March 06, 2021



Microsoft has released an [updated script](#) that scans Exchange log files for indicators of compromise (IOCs) associated with the [vulnerabilities](#) disclosed on March 2, 2021.

CISA is aware of widespread domestic and international exploitation of these vulnerabilities and strongly recommends organizations run the [Test-ProxyLogon.ps1 script](#) —as soon as possible—to help determine whether their systems are compromised. For additional information on the script, see Microsoft's blog [HAFNIUM targeting Exchange Servers with 0-day exploits](#).

For more information about these vulnerabilities and how to defend against their exploitation, see:

- Microsoft Advisory: [Multiple Security Updates Released for Exchange Server](#)
- Microsoft Blog: [HAFNIUM targeting Exchange Servers with 0-day exploits](#)
- Microsoft GitHub Repository: [CSS-Exchange](#)
- CISA Alert: [Mitigate Microsoft Exchange Server Vulnerabilities](#)
- CISA Emergency Directive 21-02: [Mitigate Microsoft Exchange On-Premises Product Vulnerabilities](#)

# RBNZ cyber breach: Accellion remains tight-lipped on timing of comms

11:53 am on 10 February 2021

Share this



**Nicholas Pointon**, Business journalist

[@nichpointon](#) [✉ nicholas.pointon@rnz.co.nz](mailto:nicholas.pointon@rnz.co.nz)

The software firm at the centre of a cyber breach won't be drawn on whether it kept the Reserve Bank in the dark about a fault in its systems.



# Acer reportedly hit with \$50 million ransomware demand

*The attack looks to be the work of the REvil group that hit Travelex last year*

By [Kim Lyons](#) | Mar 20, 2021, 9:10am EDT

f   SHARE



Sam Yeh/AFP via Getty Images



**verge  
deals**

Subscribe to get the best Verge-approved tech deals of the week.

Email (required)

ZXSECURITY.CO.NZ

FINANCIAL

# How REvil evolved into a ransomware collective capable of extorting Kaseya, JBS



# Hackers release personal info of 22 D.C. police officers

The hack is entirely distinct from the attack on the Colonial Pipeline and conducted by a different group, though both are Russian-speaking outfits.



“We care deeply about security...”



Do you though?

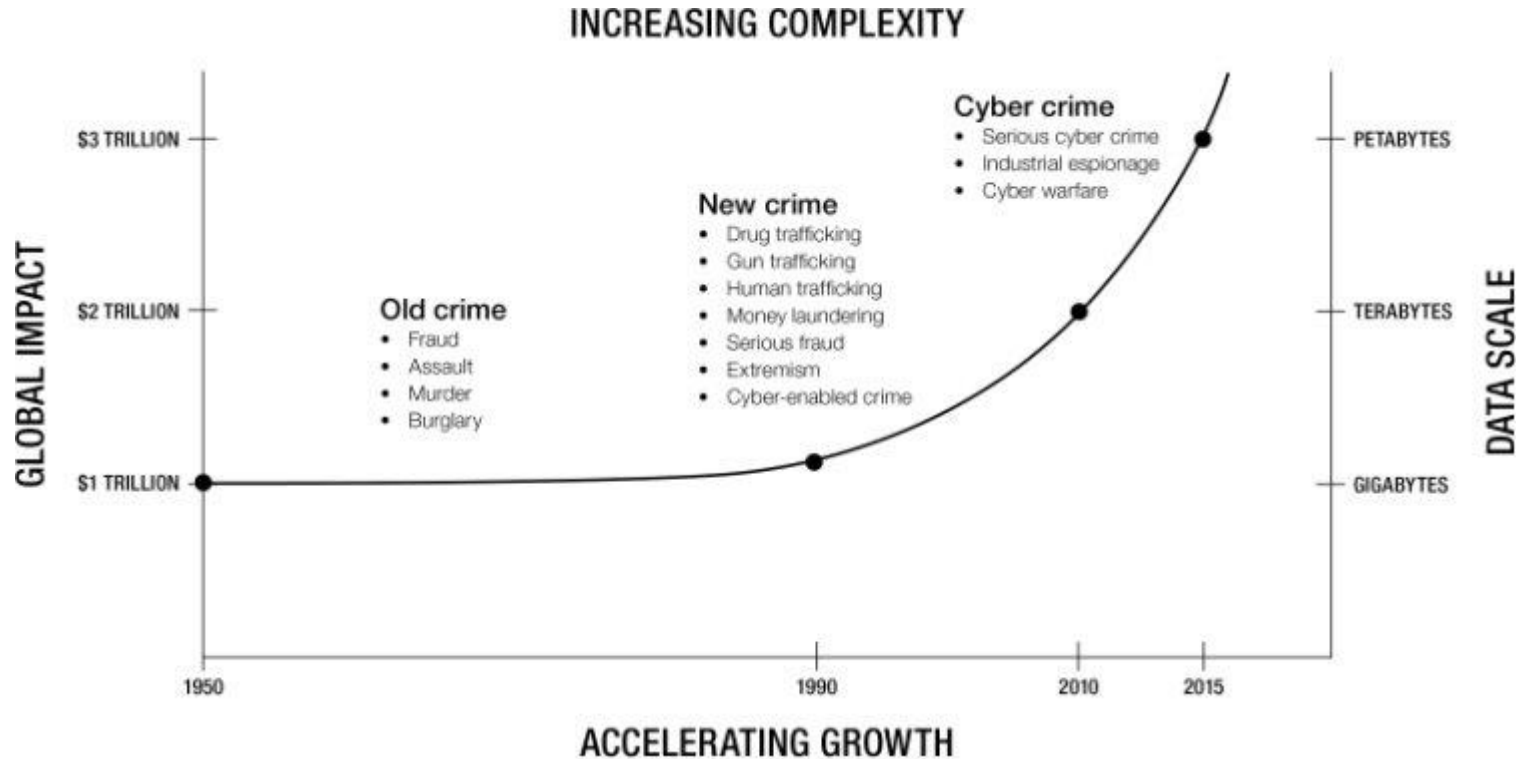




**KNOWING**    
*IS HALF THE BATTLE*

What can we learn from these?

# Increasing Complexity of Crime



# These are Ransomware businesses

- Business model has changed to gain money even from people who have backups.
- Will also seek ransom to not publicly disclose the files and other private data, which they exfiltrated before performing the encryption.
- Some Ransomware organisations are doing a third-tier ransom where they go to each affected party (customers) and seek payment not to release their individual data.
- These are not a group of malicious individuals in a basement - these are companies with:
  - Teams specialised in each stage of the attack pipeline:
    - Initial Infiltration.
    - Lateral Movement and Privilege Escalation.
    - Exfiltration of data.
    - Deployment and Execution of Ransomware
    - Customer Support to aid in the paying of ransoms and the decryption of files.
  - Monthly KPIs to achieve.
  - Stakeholders who need a return on their investments.

# Ransomware Preparation - Maturity Model

2021-06-22 • David Robinson

## Background

ZX Security has prepared this maturity model to help organisations evaluate their preparedness for a Ransomware attack . The preparations presented here are part of an ongoing process, not just something you review once. As each level is reached, the items on the lower levels should be revisited, as things are continuously changing (both your organisation's IT systems and the risks posed by Ransomware).

Most of the content and the recommendations in this model should not be new or novel. The protections and mitigations for Ransomware are common security advice, so where possible these have been presented with a justification that ties back to mitigating Ransomware.

This is a large task if everything is completed, but doing some of what is outlined here will be better than nothing. Likewise, this document is not exhaustive, there is also more work that can be done on top of what is discussed here. The information gained in the first three maturity levels should help the organisation understand the risk which they are facing from Ransomware and then decide what tasks are approached next based on the organisation's risk appetite.

This blog focuses mainly on the business operation side of a Ransomware attack. The NCSC in the UK has put together a document on [what board members should know about Ransomware and what questions to ask the organisation's staff](#). Additionally, each country will have privacy laws which may mean they have to report these attacks or suffer legal consequences. For instance in Aotearoa failing to notify the Privacy Commissioner of a notifiable privacy breach could result in a fine of up to NZD\$10,000.

## Anatomy of a Ransomware Attack

Over the last few years, we have seen Ransomware change from spreading automatically like a worm, to a large coordinated process run by real humans in a business relationship. Recent Ransomware attacks are multiple step processes, often being split between different teams. A Ransomware attack chain may look something like this:

## Most recent posts

[Ransomware Preparation - Maturity Model](#)  
[CVE-2021-31585: Accellion kiteworks - Web administrator to remote code execution](#)  
[CVE-2021-33564 Argument Injection in Ruby Dragonfly](#)  
[CVE-2021-27938 XSS in Silverstripe](#)  
[CreateQueuedJobTask](#)  
[All my Intune users could become Local Administrators and it's a Feature?](#)

## Posts by tag

[Service Workers](#) ▾

[XSS](#) ▾

[AWS](#) ▾

[Presentation](#) ▾

[DoS](#) ▾

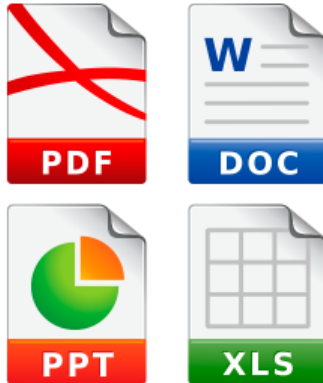
[Maturity Model](#) ▾

[Azure](#) ▾

[Intune](#) ▾

# Ransomware – Delivery Mechanism

- Tools, Techniques and Procedures
  - Email with attachment (XLS, DOC, PPT, PDF)
  - Social engineering
  - Watering hole (compromised website)
  - Compromise your company web site (CMS – i.e. WordPress)



# Ransomware – Email Delivery



Wed 10/08/2016 8:26 AM

NZPost

A delivery man has not bring the parcel

To simon@zxsecurity.co.nz



If there are problems with how this message is displayed, click here to view it in a web browser.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



**CHECK THE PACKAGE**

A delivery man was unable to redeem your package to recipient was absent. Print information label and then a <http://catgrupo.com/fcepz9ia/qbzauwnc2jlicl.php?id=simon@zxsecurity.co.nz> reason: packing.

Click to follow link

**Print out info**

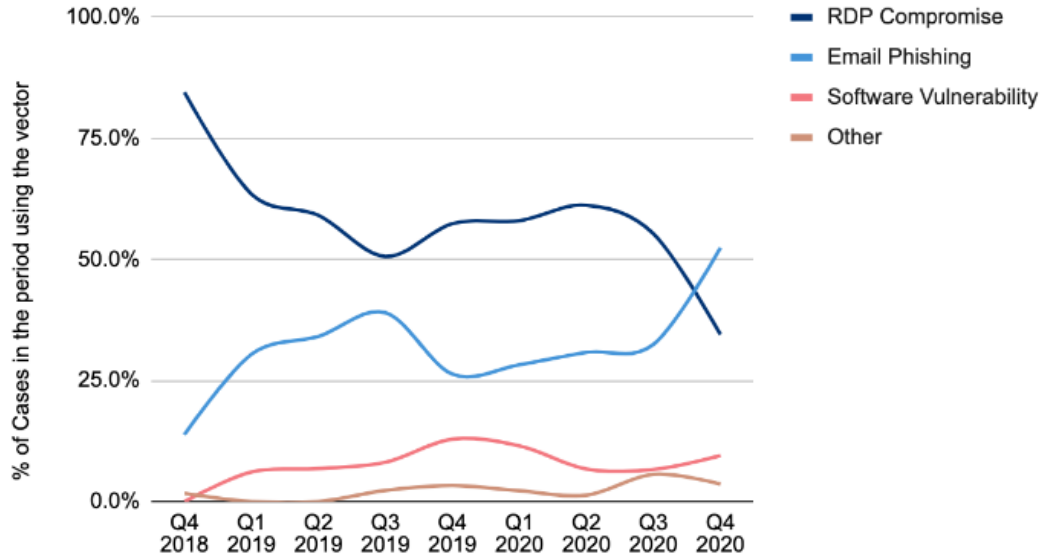
In the event the packet isn't picked up within 30 working days NZPost could have the right to take commission from you for it's storing in the amount of 1.34 NZ\$ through each hour of keeping.

© New Zealand Post 2016

# Ransomware as a Service

## Email Phishing Is the Top Attack Vector

Ransomware Attack Vectors



# Ransomware as a Service

- Mean Ransomware Payment is ~USD\$170,000
- Median Ransomware payment is ~USD\$45,000
- Mode Ransomware payment is ~USD\$10,000

**“The number of organizations that paid the ransom increased from 26% in 2020 to 32% in 2021, although fewer than one in 10 (8%) managed to get back all of their data”**

Source: Coveware /Sophos



# Waikato DHB

NEW ZEALAND / HEALTH

## Waikato DHB ransomware attack: Half of servers restored in past four days

8:29 pm on 2 June 2021

Share this     

 **Andrew McRae**, Reporter  
 [andrew.mcrae@rnz.co.nz](mailto:andrew.mcrae@rnz.co.nz)

 **Kate Gregan**, reporter  
 [kate.gregan@rnz.co.nz](mailto:kate.gregan@rnz.co.nz)

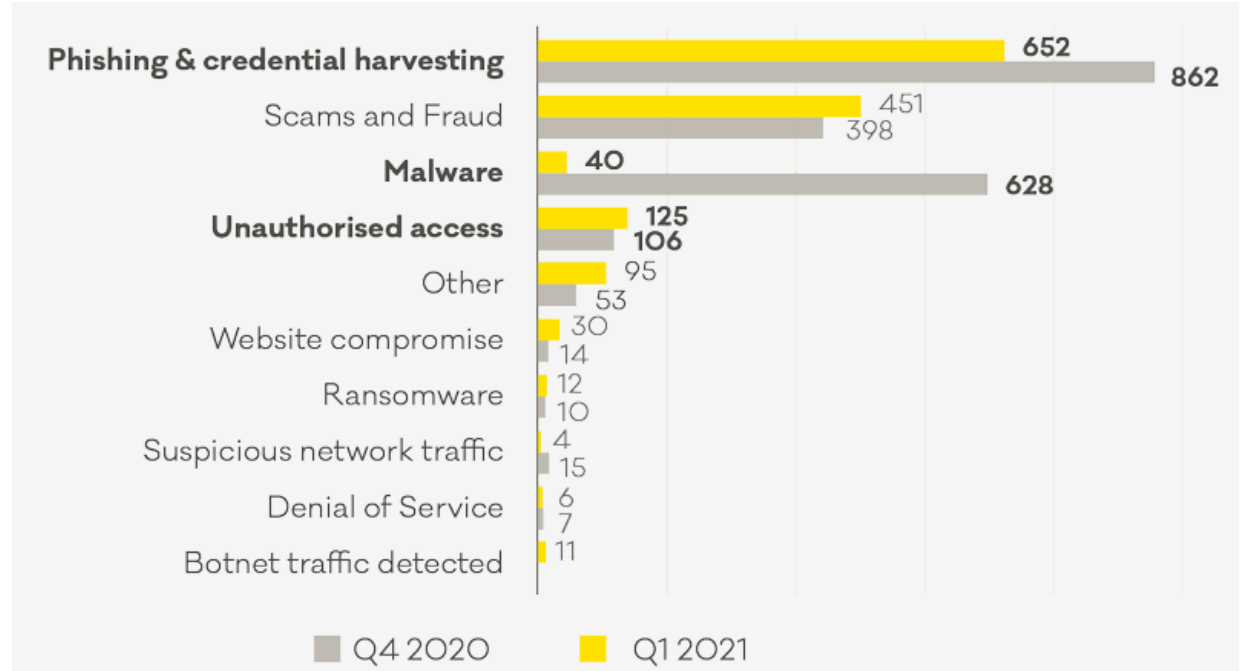
Waikato DHB has dismissed the idea that paying a ransom after its cyber attack would have been easier than having its entire computer system put out of action for such a long time.



**The average number of incident reports per quarter is 1,569 and average direct financial loss is \$4.2 million.**

<https://www.cert.govt.nz/about/quarterly-report/quarter-one-report-2021/>

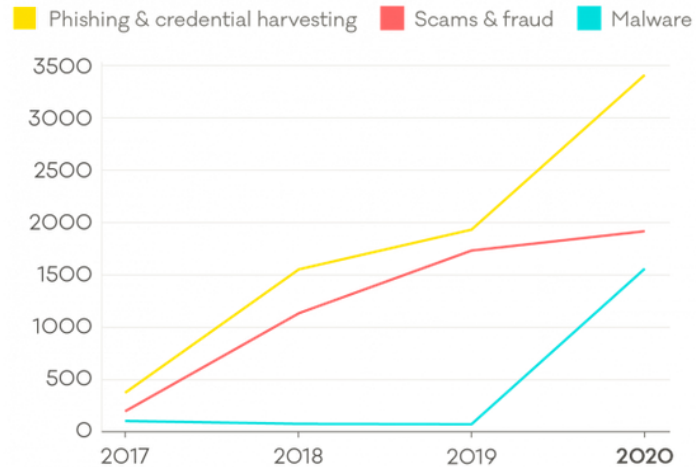
# Phishing



[Show full data](#)

# NZ CERT Statistics – FY 2020 Report

## Top incident categories



The top three incident categories in 2020 are:

- 3,410 phishing and credential harvesting reports, up 76% on 2019
- 1,920 scams and fraud reports, up 11% on 2019
- 1,560 malware reports, up 2008% on 2019

# 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



If you purchase via links on our site, we may receive [affiliate commissions](#).

Home » Security » RockYou2021: largest password compilation of all time leaked online with 8.4 billion entries

# RockYou2021: largest password compilation of all time leaked online with 8.4 billion entries

by Edvardas Mikalaukas — 7 June 2021 in Security 17



137  
SHARES



What seems to be the largest password collection of all time has been leaked on a popular hacker forum.

## Editor's choice



### \$280 million stolen per month from crypto transactions

by Edvardas Mikalaukas 2 JUNE 2021 1

Front-runners are abusing decentralized cryptocurrency exchanges by draining hundreds of millions in crypto from trader transactions on the Ethereum network.

[READ MORE](#)



## Part 3: What to do about it?

---

Elf Eldridge  
ZX Security  
July 2021  
[elf@zxsecurity.co.nz](mailto:elf@zxsecurity.co.nz)

# Who to Call?

certnz >

About us

> / About / Contact us

## Contact us

Contact CERT NZ if you have feedback or a general enquiry.

If you or someone else is in immediate danger or a crime is being committed, call 111 now.

## Report an incident

If you'd like to report a cyber security issue, use our online tool rather than sending us an email.

[Report an issue — businesses and individuals](#)

[Report an issue — IT specialists](#)

If you'd like assistance completing the form, call us:

- in New Zealand, call us on 0800 CERT NZ (0800 2378 69)



# Phishing

- Don't accept sweets from strangers
  - Or open emails from someone you don't know
  - Don't click on links you are unsure about
  - Don't open attachments you are unsure about
  - Don't plug in unauthorised USB keys and other peripherals (goodie bags)
- Comes in many shapes and sizes
  - LinkedIn
  - Facebook, Whatsapp
  - Skype/Phone (vishing)
  - SMS
- Verify via a DIFFERENT channel



# Ransomware - Prevention

- Perform regular backups
  - On-site
  - Off-site, cold backups
  - Practice Restoring and regular checks
- Apply software updates
  - Operating systems
  - Desktop applications
- Use Antivirus
  - But don't rely on it
  - You don't need to pay for it either

<https://zxsecurity.co.nz/research/ransomware-preparation-maturity-model/>

# Ransomware – If you are infected

- Seek expert help, report the attack to CERT NZ
  - They have an awesome reporting tool and great staff
  - If it happens at work, contact your IT team
- Search for 3<sup>rd</sup> party decryption tools
  - If confident, try cleaning the infection yourself
- Be prepared to restore from backup

<https://zxsecurity.co.nz/research/ransomware-preparation-maturity-model/>

# Ransomware – Paying Ransoms

- Paying the ransom should be a last resort
  - Perform a cost analysis of incident response vs payment
  - Possibility for re-infection
  - Files may not be decrypted at all
- Always rebuild the infected machine after an infection

# Security controls



**DON'T  
PANIC**



CRITICAL CONTROLS

## CERT NZ's Critical Controls 2021

Each year, we review our critical controls against the incidents we have seen over the past 12 months. When correctly im



CRITICAL CONTROLS

## Password manager

Providing a password manager for your staff to store their passwords, or other secrets like...



CRITICAL CONTROLS

## Securing internet-exposed services

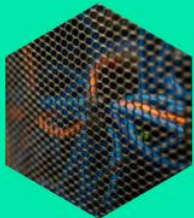
Limiting and securing your internet-exposed services will help you prevent unauthorised...



CRITICAL CONTROLS

## Secure defaults for macros

While macros have a valid business function, they are often used by attackers too. Using...



CRITICAL CONTROLS

## Network segmentation and separation

When paired together, segmentation and separation can add an additional level of acces...



CRITICAL CONTROLS

## Centralised logging

Storing and securing your logs in a central place makes log analysis and alerting easier.



CRITICAL CONTROLS

## Implement and test backups

After an incident, restoring your data from backups is often the best way to return to business a...

# NZ CERT Critical Controls 2021

1. Patch your software and systems
2. Implement multi-factor authentication and verification
3. Provide and use a password manager
4. Configure logging and alerting
5. Secure internet-exposed services
6. Implement and test backups
7. Implement application allowlisting
8. Enforce the principle of least privilege
9. Implement network segmentation
10. Set secure defaults for macros



# NZ CERT Critical Controls 2020

1. Patch your software and systems
2. Disable unused services
3. Implement and test backups
4. Implement application allowlisting
5. Enforce the principle of least privilege
6. Configure centralised logging and analysis
7. Implement network segmentation
8. Manage authentication
9. Follow an asset management lifecycle
10. Set secure defaults for macros





# ASD Essential Eight

1. Application whitelisting
2. Patching applications
3. Configuring Microsoft Office macro settings
4. Application hardening
5. Restricting administrative privileges
6. Patching operating systems
7. Multi-factor authentication
8. Daily backups



Home / Publications / Essential Eight Maturity Model

## Essential Eight Maturity Model

# Summary

- Don't reuse passwords
- NZ CERT
- Be careful of phishing
- Be realistic about your privacy
- Automatic Updates
- Backups



# Part 4: ZX Greatest Hits

---

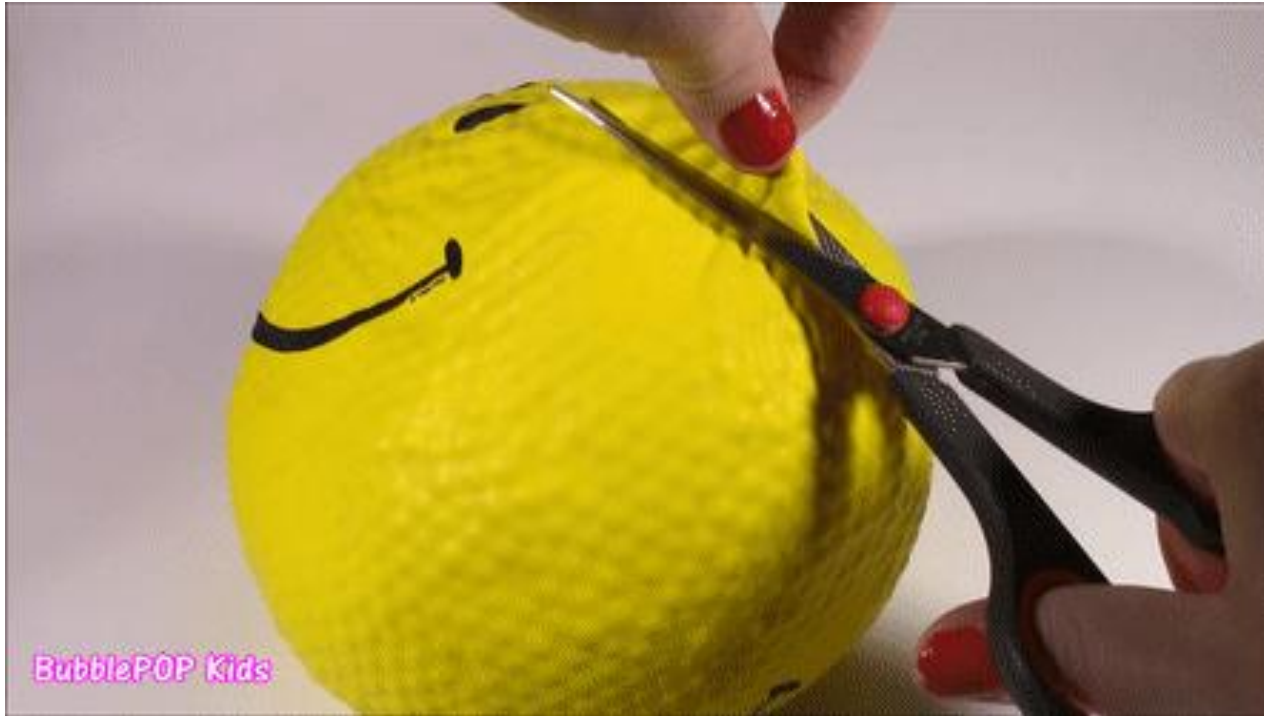
Elf Eldridge  
ZX Security  
July 2021  
[elf@zxsecurity.co.nz](mailto:elf@zxsecurity.co.nz)

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

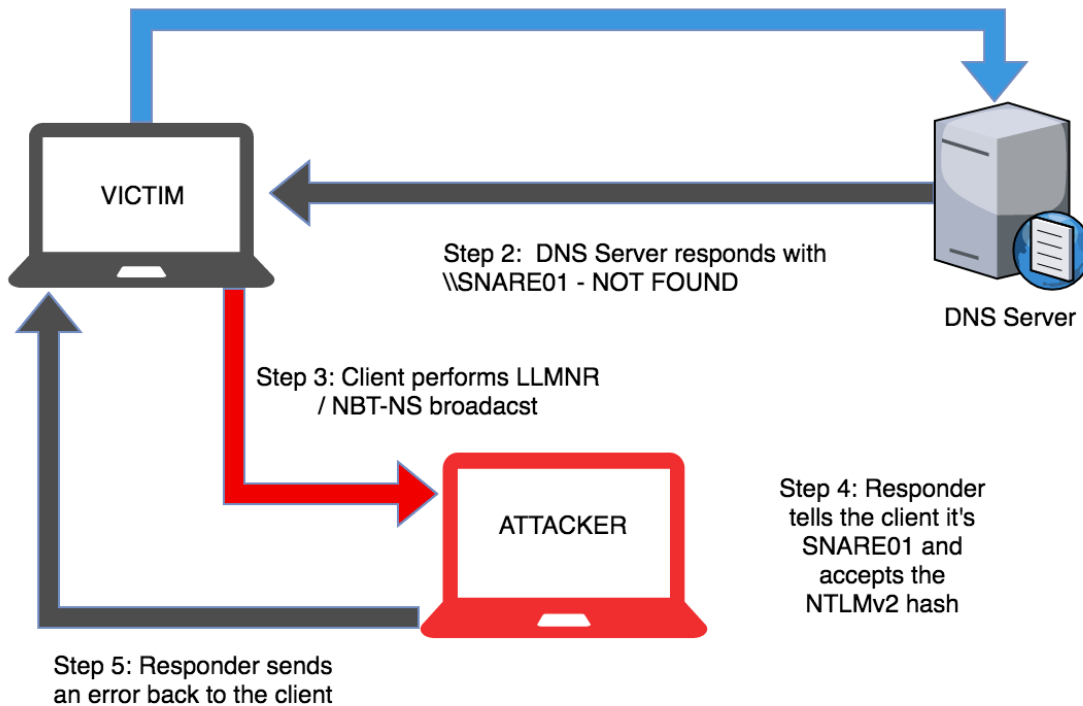
# Customers network – hard on the outside



Soft'n'squishy on in the inside



Step 1: User sends incorrect SMB share address \\SNARE01



## Sniffing



...or just looking around..



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

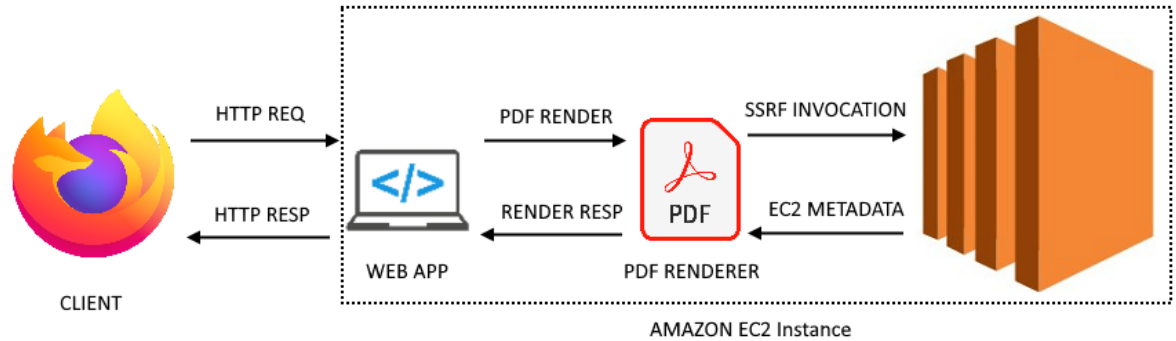


## MFA Bypass



## Securing Your GraphQL API from Malicious Queries

SQL Injection in 2021: GraphQL Edition



## Server Side Request Forgery

# Other tools

- OWASP Security Knowledge Framework  
(<https://owasp.org/www-project-security-knowledge-framework/>)
- OWASP Application Security Verification Standard  
(<https://owasp.org/www-project-application-security-verification-standard/> )
- OWASP Software Assurance Maturity Model  
(<https://owasp.org/www-project-samm/> )

# OWASP ASVS Example

## V3.2 Session Binding Requirements

#	Description	L1	L2	L3	CWE	NIST §
<b>3.2.1</b>	Verify the application generates a new session token on user authentication. ( <a href="#">C6</a> )	✓	✓	✓	384	7.1
<b>3.2.2</b>	Verify that session tokens possess at least 64 bits of entropy. ( <a href="#">C6</a> )	✓	✓	✓	331	7.1
<b>3.2.3</b>	Verify the application only stores session tokens in the browser using secure methods such as appropriately secured cookies (see section 3.4) or HTML 5 session storage.	✓	✓	✓	539	7.1
<b>3.2.4</b>	Verify that session token are generated using approved cryptographic algorithms. ( <a href="#">C6</a> )		✓	✓	331	7.1

TLS or another secure transport channel is mandatory for session management. This is covered off in the Communications Security chapter.

# Summary

- Have and enforce strong passwords
- Check internal AND external security
- Get a technical evaluation of any critical software
- OWASP ASVS





# Part 5: Azure and AWS

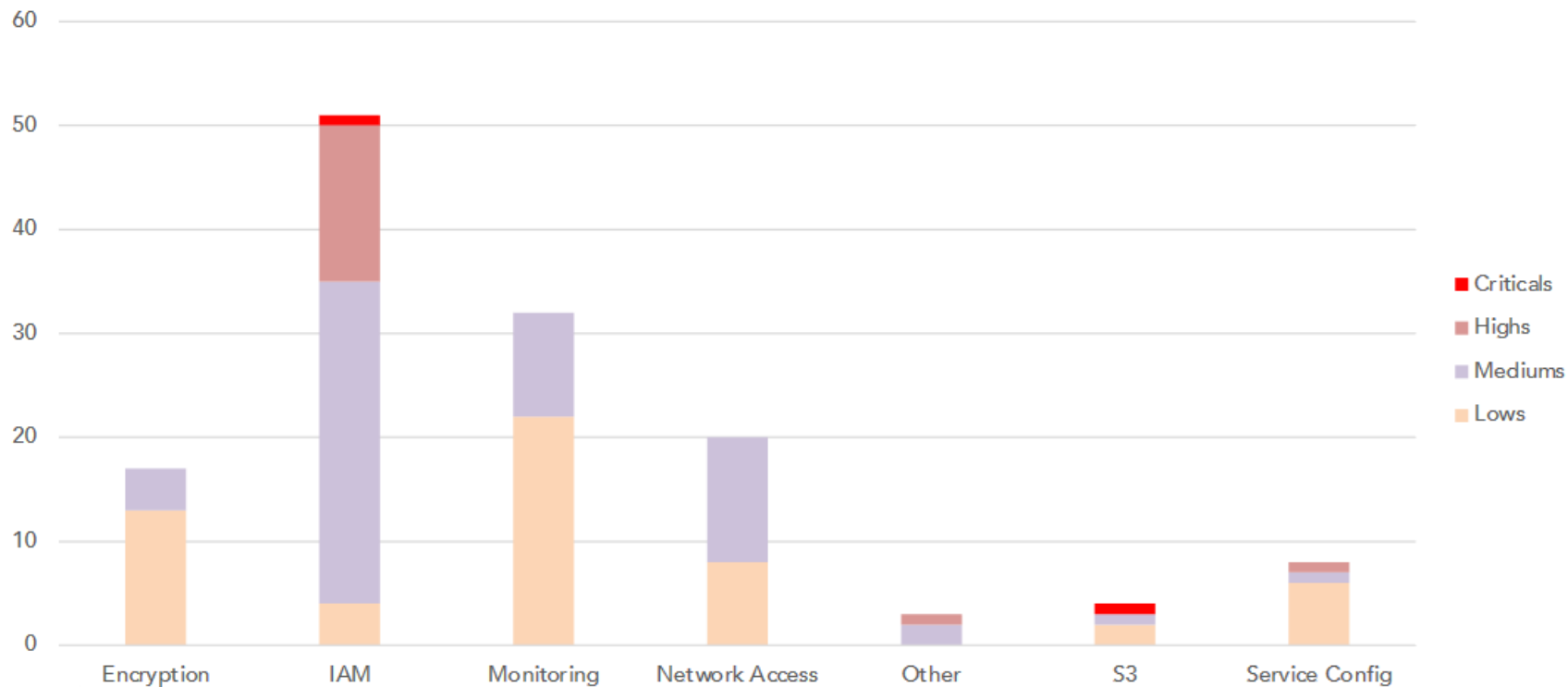
---

Elf Eldridge  
ZX Security  
July 2021  
[elf@zxsecurity.co.nz](mailto:elf@zxsecurity.co.nz)

Paraphrasing:  
[blaise@zxsecurity.co.nz](mailto:blaise@zxsecurity.co.nz)



# Broad Trends



# Summary of Critical and High Findings

- Critical: World writeable bucket
  - Better: it had root creds stored in a file
- Critical: SSRF leads to metadata server in EC2
- Lack of key rotation (especially important on CI/CD)
  - Keys copied into github
- SNS Publishing open to public

# Other Important Findings

- Administrator role use abused
  - Spinning up resources unapproved for company use
- No MFA (admins and root)
- Password policy
- PassRole use – iam:\* is a terrible idea
- Inspector findings ignored – why have it?
- Logging absent or ignored



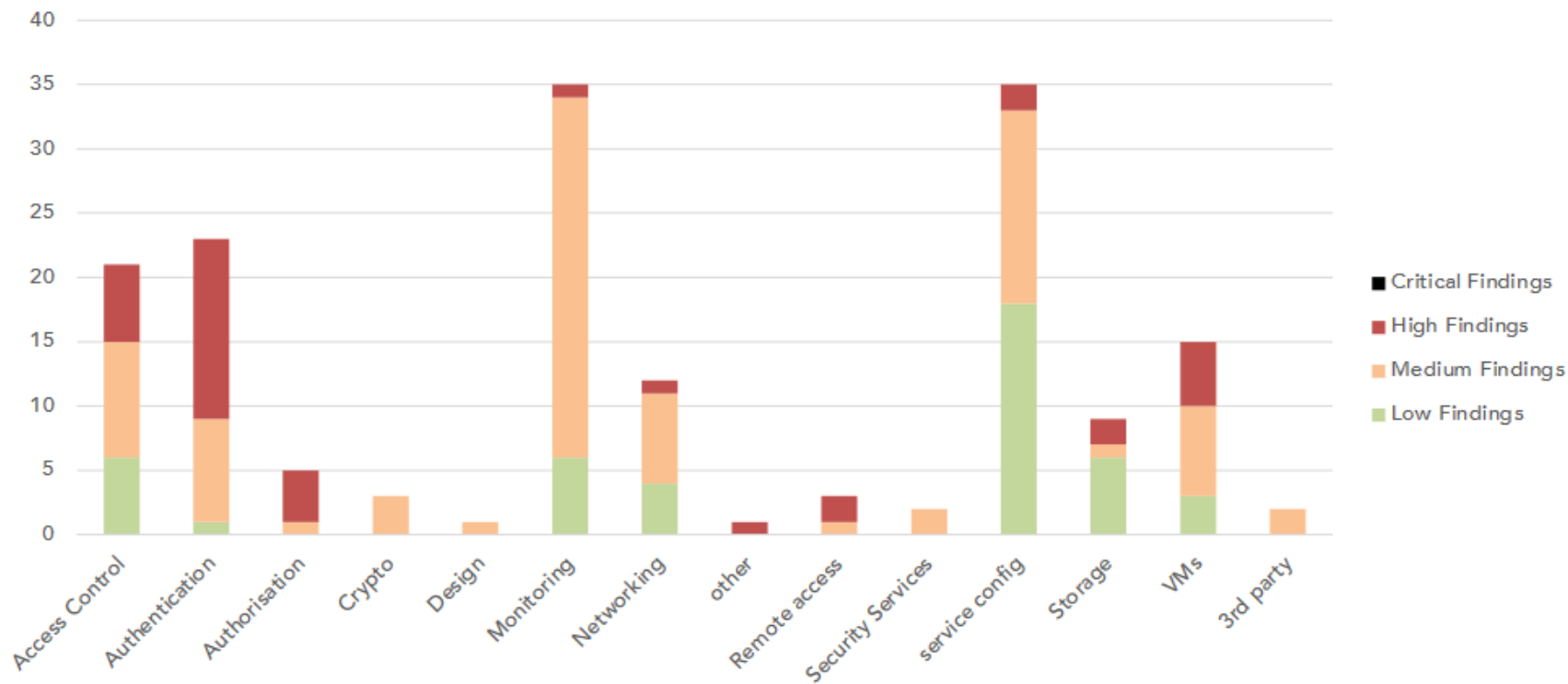
What does good AWS look like?

[https://zxsecurity.co.nz/assets/files/attachments/AWS\\_Security\\_Faux\\_Pas\\_11-2020.pdf](https://zxsecurity.co.nz/assets/files/attachments/AWS_Security_Faux_Pas_11-2020.pdf)



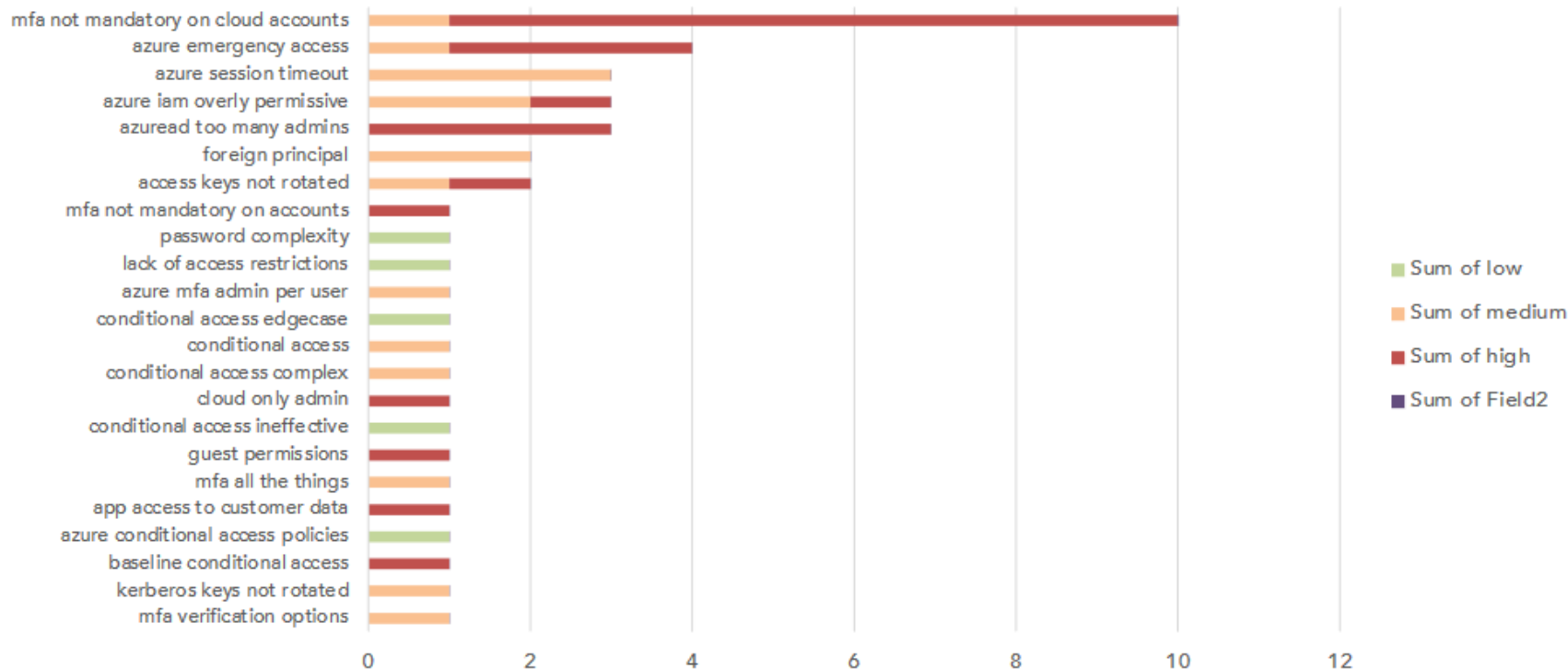
# Microsoft Azure

# Broad trends





# AAA major issues



# Why is this so important?

Customers' biggest weakness is often their On-Premises Active Directory, which is happily syncing into Azure.

- Getting Domain Administrator access on-prem is a very common occurrence for our Internal Pen Test team
- Pivoting from on-prem to Azure once you've got DA is simple if there are no additional verifications (such as MFA)
- Often customers will exclude their on-prem from Conditional Access

# Monitoring takeaways

- Default is to not log security events (no diagnostic logs)
- Retention is 30 days unless steps are taken to increase this (comes at a cost)
- Alerting must be thought through and configured
- Many services have additional security logging not enabled using the Subscription-level Diagnostic Settings



# Microsoft Azure

[https://zxsecurity.co.nz/assets/files/attachments/Azure\\_Security\\_Faux\\_Pas\\_03-2021\\_v1.0.pdf](https://zxsecurity.co.nz/assets/files/attachments/Azure_Security_Faux_Pas_03-2021_v1.0.pdf)



## Part 6 FAQs

---

Elf Eldridge  
ZX Security  
July 2021  
[elf@zxsecurity.co.nz](mailto:elf@zxsecurity.co.nz)




*“Yo! You didn’t mention DoS!”*

<https://zxsecurity.co.nz/research/dos-preparation-maturity-model/>




*“Password changes every 90 days:  
Devil or Angel?”*

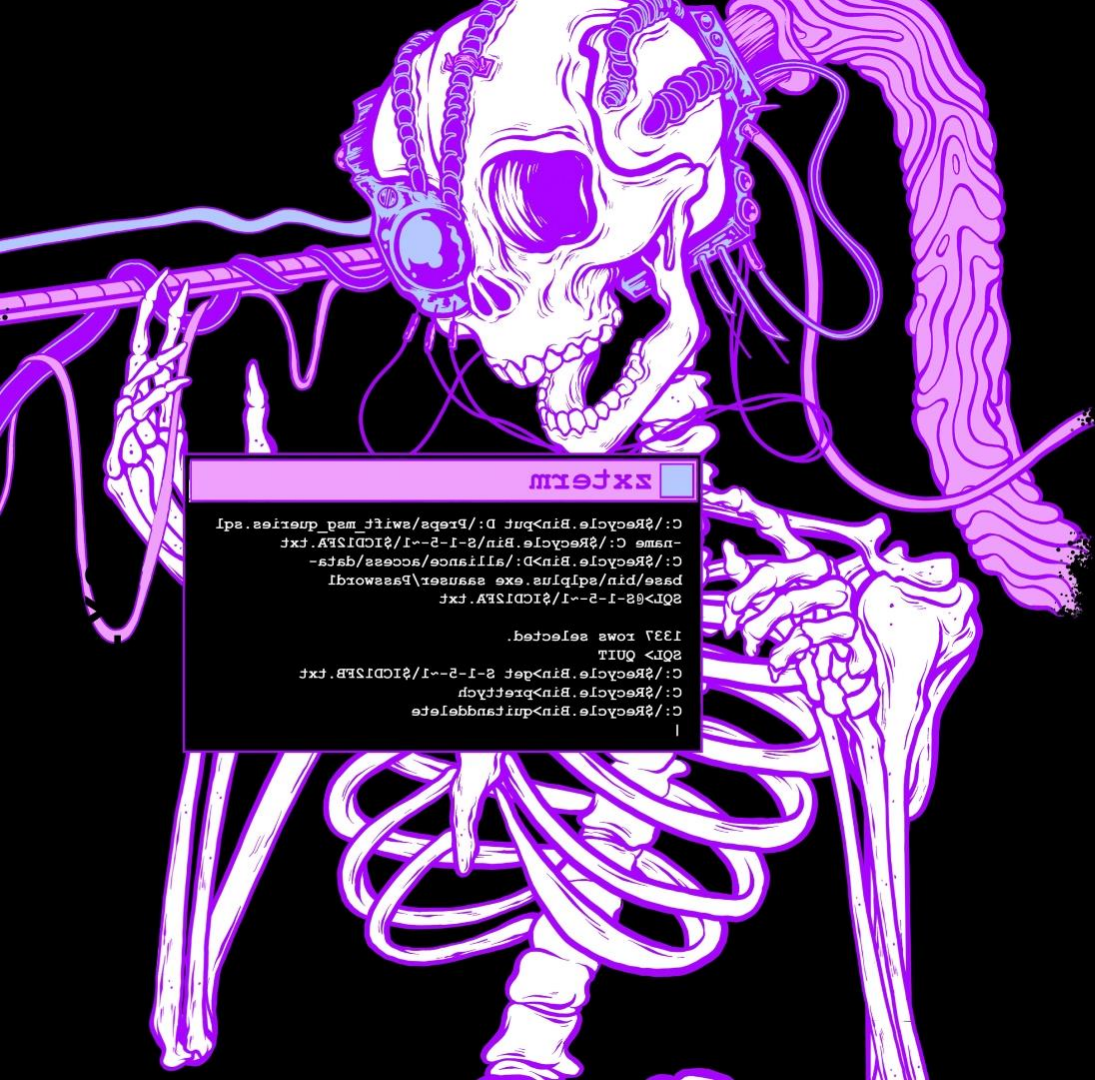


*“How effective are bug bounty programs?”*





*“Are there any major issues in cybersecurity that aren’t talked about much?”*



```
zxterm
C:\$Recycle.Bin>cd D:\Prags\wifi_mad_queries.spd
-name C:\$Recycle.Bin\8-1-2--1\%CD12FB.txt
C:\$Recycle.Bin>dir /s /b /a:*.txt /ad /o: /x: /l /w: /c: /d: /e: /f: /g: /i: /j: /k: /l: /m: /n: /o: /p: /q: /r: /s: /t: /u: /v: /w: /x: /y: /z: /?
base/bin/edp1us.exe sasuser\Password1
SQL>8-1-2--1\%CD12FB.txt

1337 rows selected.
SQL>QUIT
C:\$Recycle.Bin>def 8-1-2--1\%CD12FB.txt
C:\$Recycle.Bin>prectyph
C:\$Recycle.Bin>quitfanddeletere
|
```


# Questions

Email: [elf@zxsecurity.co.nz](mailto:elf@zxsecurity.co.nz)

LinkedIn: Elf Eldridge

Twitter: @kaiwhata

Website: [zxsecurity.co.nz](http://zxsecurity.co.nz)



*“No-one on our board has a good understanding of IT, so we cant get investment to improve things...”*



*“Should we be using cloud services to improve security?”*