“THEY’RE JUST TAKING HOME ANY LAPTOP THEY COULD FIND!”

2020 Stories from the SOC
@GyledC
Cyber Research NZ
whoami

- Melbourne-based Cyber Threat Analyst
- Works in a MSSP (Managed Security Service Provider) SOC (Security Operations Centre)
- Has an unconventional path to tech and infosec
- Graduate Certificate in Incident Response, SANS Institute; Master in Cyber Security – Digital Forensics, UNSW Canberra ADFA
- Volunteers for different organisations: various causes from mental health, KidSecuriDay to OSINT
Q1 2020 Timeline

- Late December 2019 to early January 2020: Various social media posts on a new virus
- 23 January 2020: Lockdown imposed in Wuhan & other cities in Hubei
- 11 March 2020: WHO declared COVID-19 outbreak as a pandemic
March 2020

- Increase in traffic involving pandemic and COVID themes
- High potential for spear phishing attacks
  - *Action taken: Release of advisory for both technical and non-technical audience*
- Gathering of info regarding pandemic plans
  - *Identification of essential services, plans for remote work*
- Lockdown announcement: “They’re just taking home any laptop they could find.”
DURING THE LOCKDOWNS
BE VEWDY VEWDY QWIIET.

I'M HUNTING WABBITS!
## Challenges

### Issues
- On-prem vs cloud
- Exposed RDP
- New cloud resources deployed
- No BYOD policies
- No clear acceptable use policies

### Solutions/workarounds
- Detection tools – connectors to the cloud environment
- Application of red team techniques to show impact
- More frequent communication
- Custom rules/models/signatures
- Explanations involving potential legal issues
Lessons learned

- Secure remote access
- BYOD policies
- Updated documentation
- User communication
Questions?

- Feel free to reach out to me in Twitter: https://twitter.com/GyledC
- @GyledC

- Image sources:
  - Microscope and tech company logos: https://unsplash.com/photos/GL689nIE1Xg
  - Person in mask and hoodie: https://unsplash.com/photos/F7DAQIDSk98
  - Elmer Fudd meme: http://www.quickmeme.com/meme/3q06ch
  - Laptop with Netflix in a dark room: https://unsplash.com/photos/Nn0Ap_GCzw4