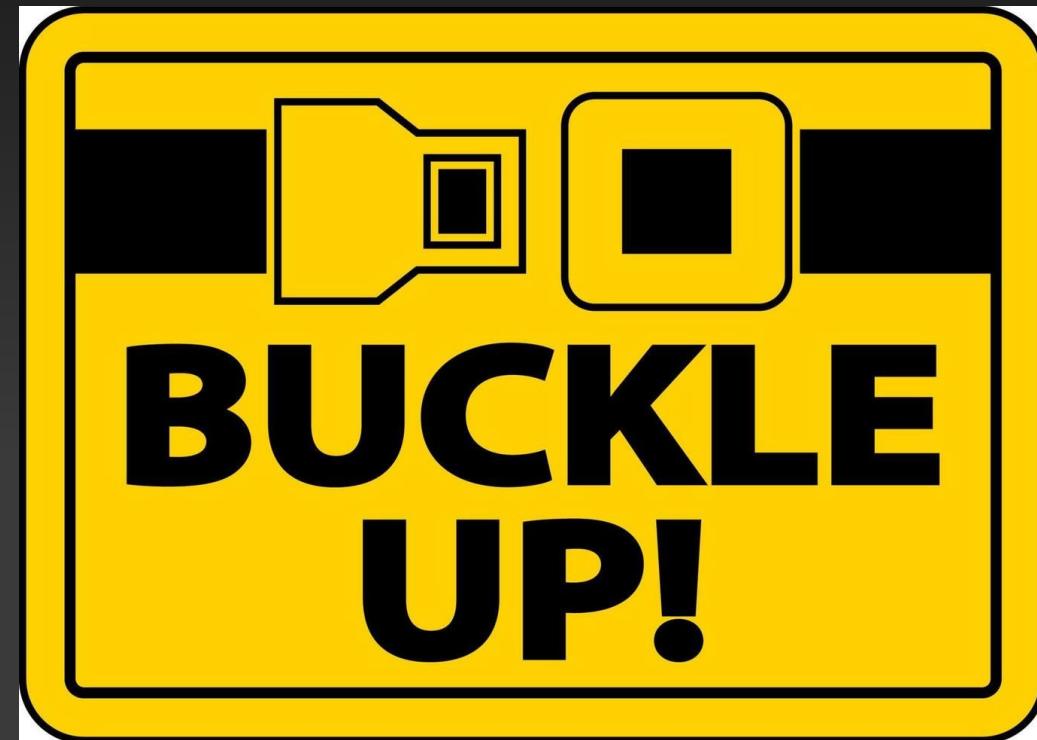




Announcements



Karaoke

- Thank you all for coming!



Karaoke



DMU eSports Karaoke

This Monday (19th Feb)

8.00pm to 11.30pm

Upstairs firebug



Merchandise

Front



Back



Front



Back



1 WEEK REMAINING!!!!
Make sure you PAY

£15

£28



CEM Careers Programming Sessions

- Wednesday 21st February (next week)
- All sessions are *free!*
- Lead by industry professionals

Data & Analytics
11am-12pm
(MS Teams)

Python Programming
12pm-1pm
(Gateway House)

Software Development
2pm-4pm
(MS Teams)



TrendMicro CTF - Friday 15th March



Limited to 20 spaces

In-person at Gateway House

Sign up link in Discord later



Mini-talks session (21st March)

Some previous titles:

Tools I Have in my Arse(nal)
AI in Cyber Security
Hijacking Cars
Flipper Zero
Buffer Overflow
CTF/OSINT Writeups

Examples can be made available

Please speak to us!

Start having a think



Finally...



Back2Hack... returns!

***Not the
real logo I was
pissing about
with ChatGPT



Saturday 25th May 2024





APTs (Advanced persistent threats)



Don't do illegal shit



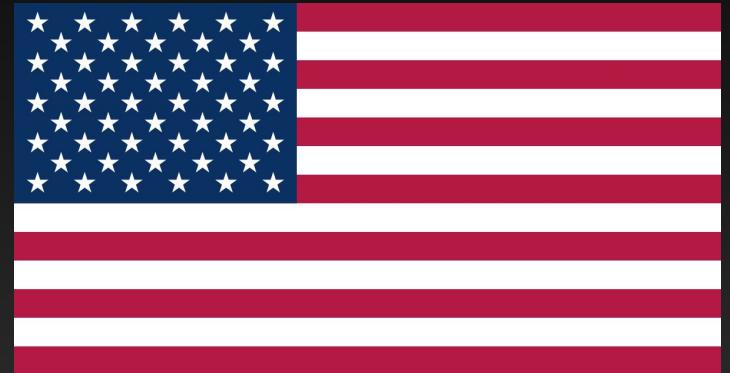
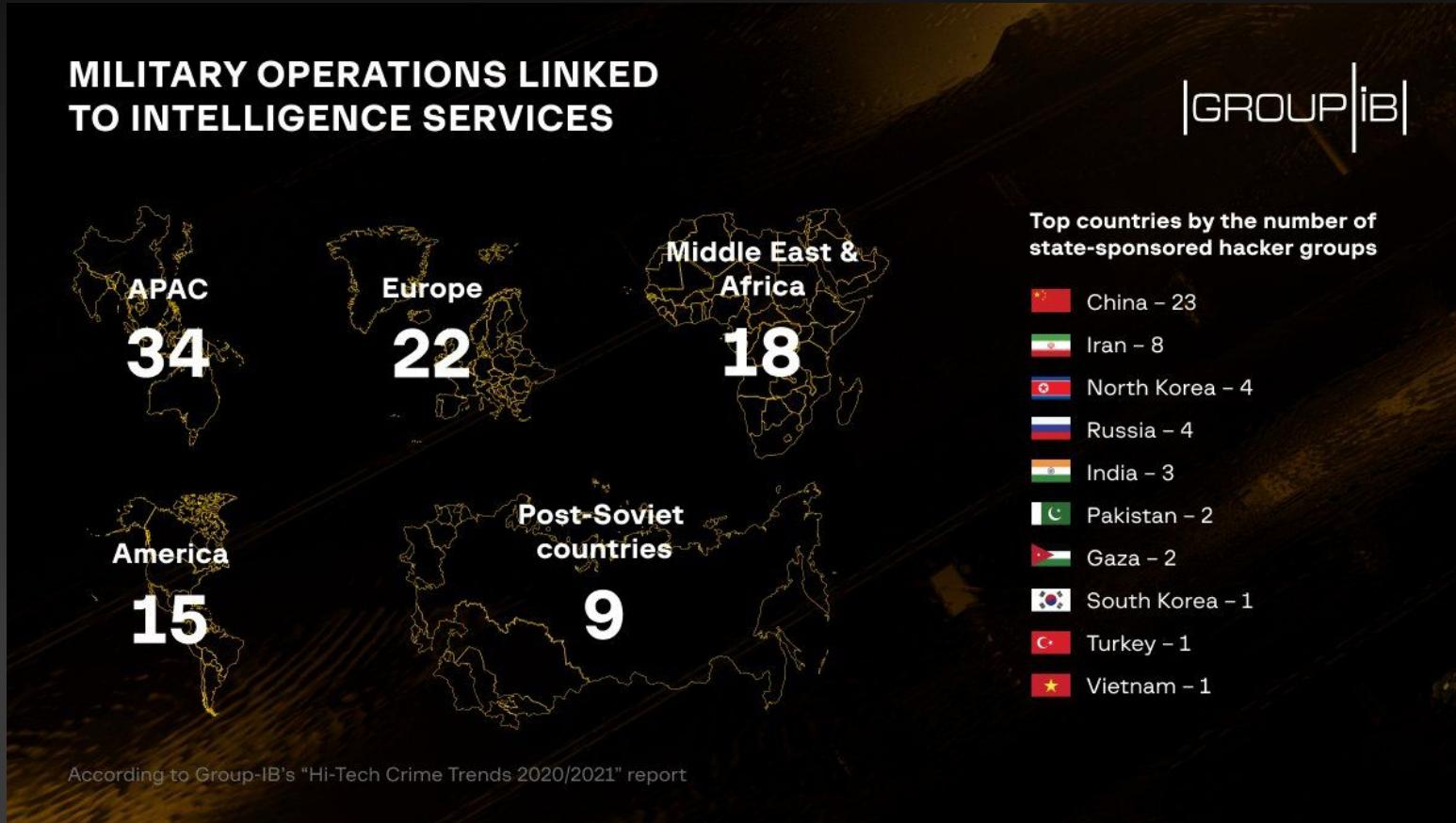
What's an APT?

- Team of malicious hackers with very advanced capabilities



What's an APT?

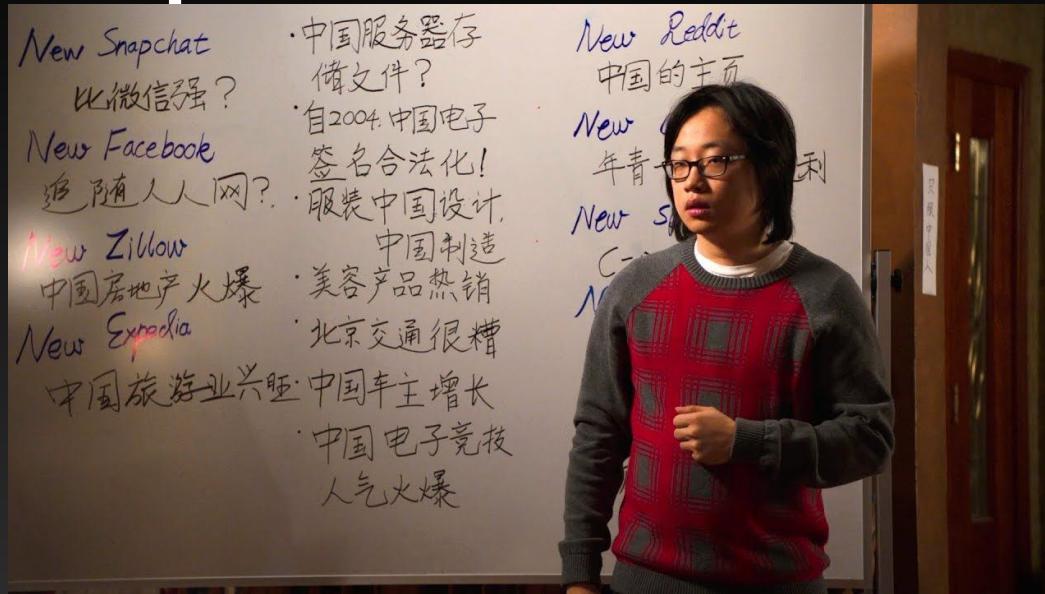
- Most groups are “state sponsored”



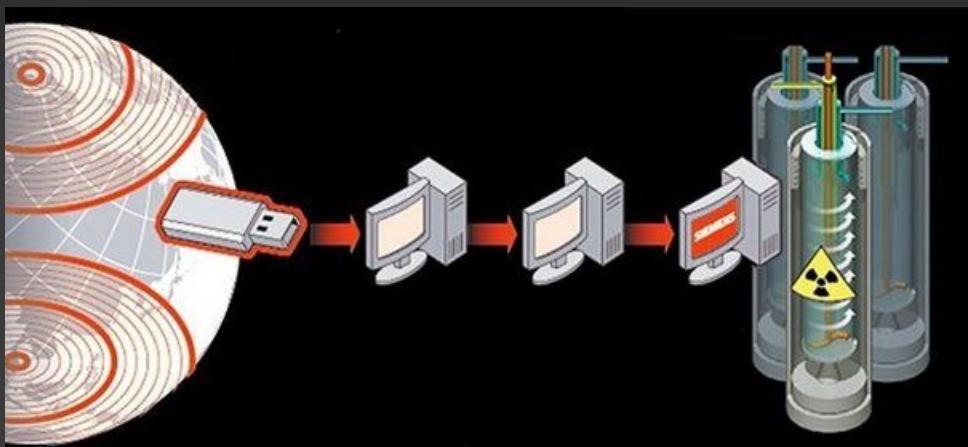
Purposes of APTs



Espionage



Money



Physical damage & disruption

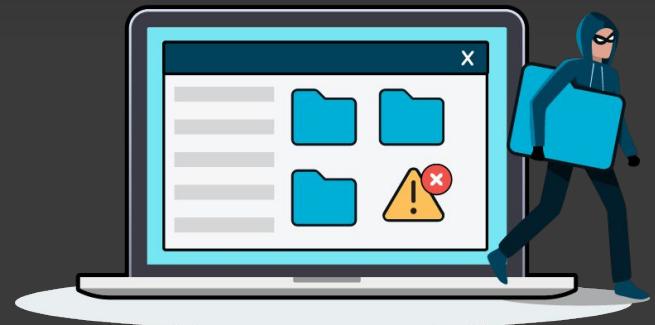


How do they do it?

- Advanced, prolonged campaigns spanning a wide time period



- Establish a foothold
 - Create backdoors
- Exfiltrate all the data away



How do they do it?

- They often use zero-days



Can anybody name any Zero-Days
currently being exploited?

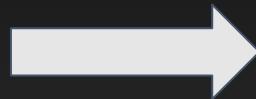
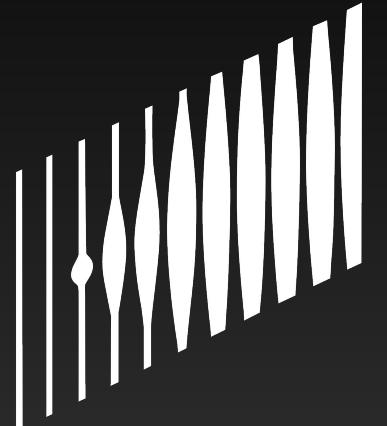


APT Spotlight



Lazarus

- North Korean government-run group
- Commits
 - Cyber espionage
 - Cyber warfare
- Some notable targets:



Great podcast about their exploits



Leaked lots of PII and IP



Lazarus

- Many, many, many banks



Bangladesh
Bank



Polish Financial
Supervision
Authority



遠東國際商業銀行
Far Eastern Int'l Bank
(Taiwan-based)



(Ecuador)



Bank of Chile



Vì chúng tôi hiểu bạn
(Vietnam)



(India)

And others
in
South Korea
Mexico
Pakistan
Philippines
Turkey



Lazarus



Allegedly...



Lazarus

Motivations?





always has been

wait, this is a film night?



imgflip.com







An error has occurred

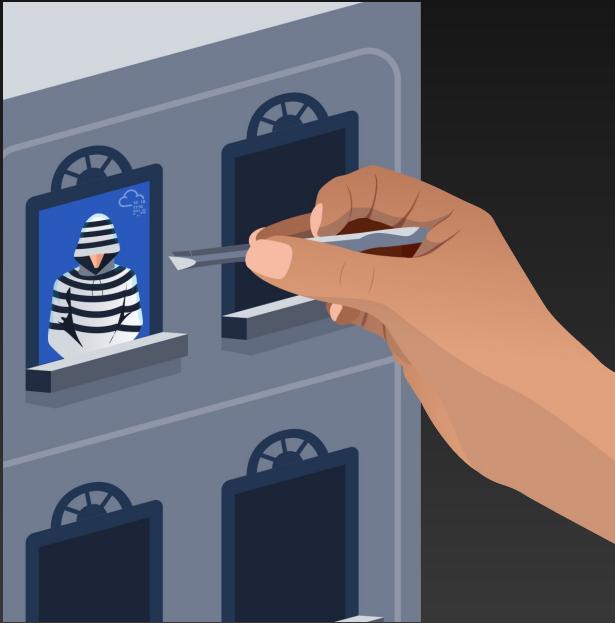
Press Enter to ret

Press CTRL+ALT+D
you will lose all

Error: 0E : 016F : BPF

If you do this,
open applications.

Today's Task...



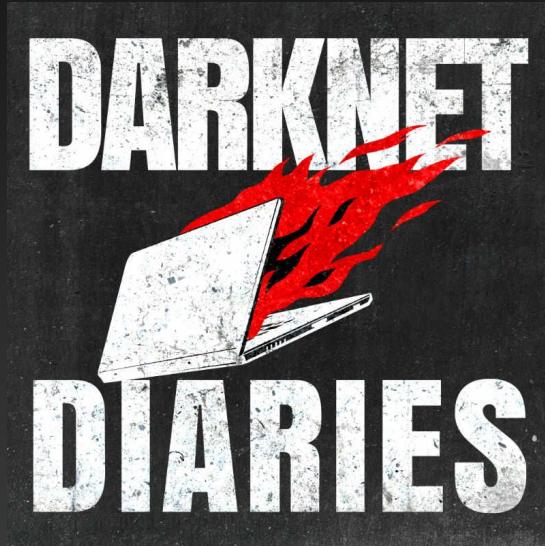
Eviction

<https://tryhackme.com/room/eviction>



Resources

- Lots of cool podcast episodes



[Jack Rhysider - YouTube](#)



[BBC World Service - The Lazarus Heist - Downloads](#)

- Go down some YouTube rabbit holes!
- A list of APTs on Wikipedia:

[Advanced persistent threat - Wikipedia](#)





JESUS, I NEED A DRINK. YEAH?

