Cyber Security

The threat landscape

Chris G. Willcocks
Durham University

Lecture content

Crossover with
Sun Tzu “The Art of War”

- Know your enemy
- Know your terrain
- Know your economy (waging warfare)
- What are the common tactics?
- Planning strategies
- Spies: Can “we” (or they) truly be anonymous?
- Intelligent threat analysis
- Case study: typical medium-sized corporate spending

Who really are the adversaries? "Know your enemy"

Professional Criminal Gangs £££

- Make it so hacks are not cost-effective

Lone Hackers, Cyber Criminals, Script Kiddies

- Lone hackers are often not worth worrying about, script kiddies are more numerous

Governments
Political Activists
Insiders
Competitors
ISPs? Companies? The University?

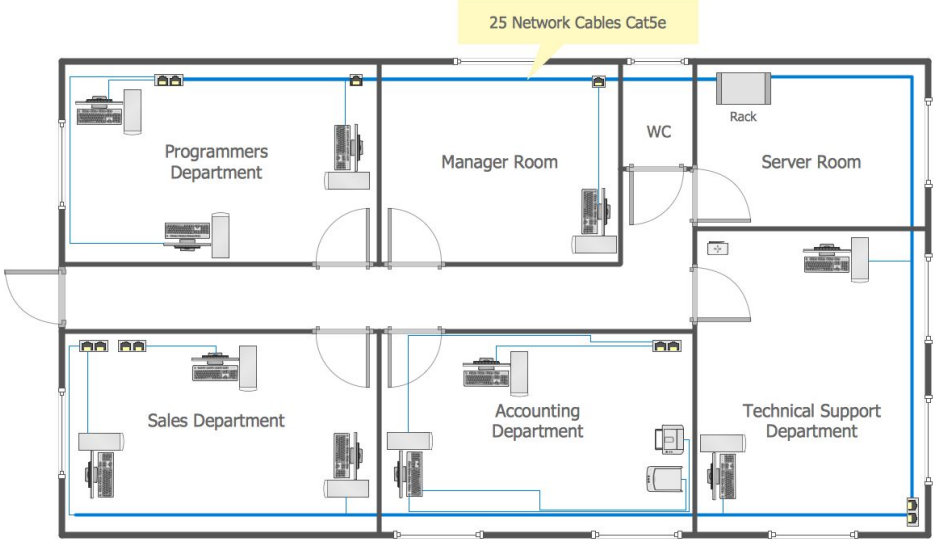
- May or may not be attackers
- Humans default to a position of trust (helps us survive in complex environments)

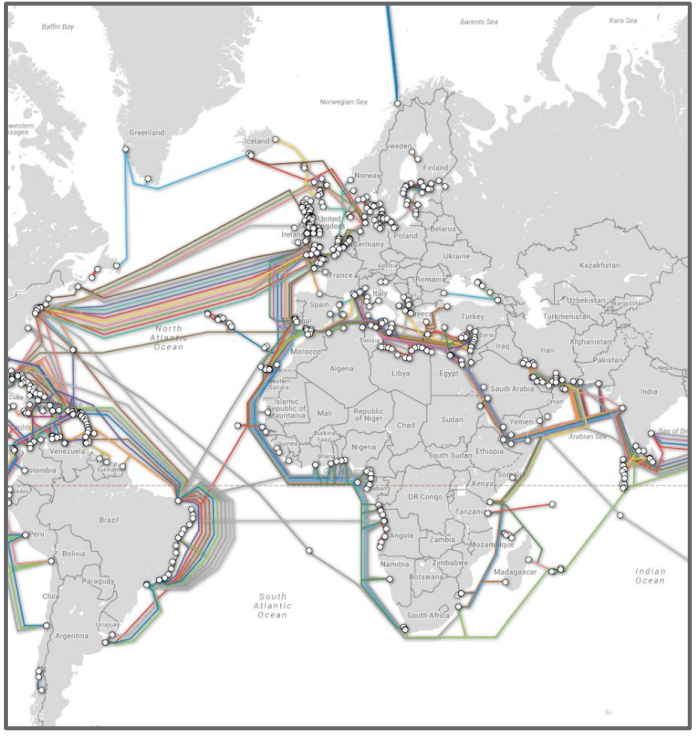
...depending on who the enemy is, different skills are required

Know the battlefield

With the internet, the battlefield is much larger and more complex than in traditional warfare.

- Think hierarchically



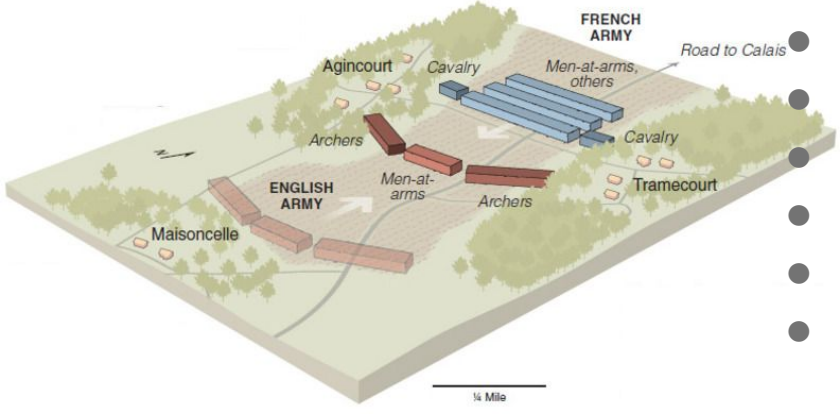


https://www.submarinecablemap.com

Know the most common tactics

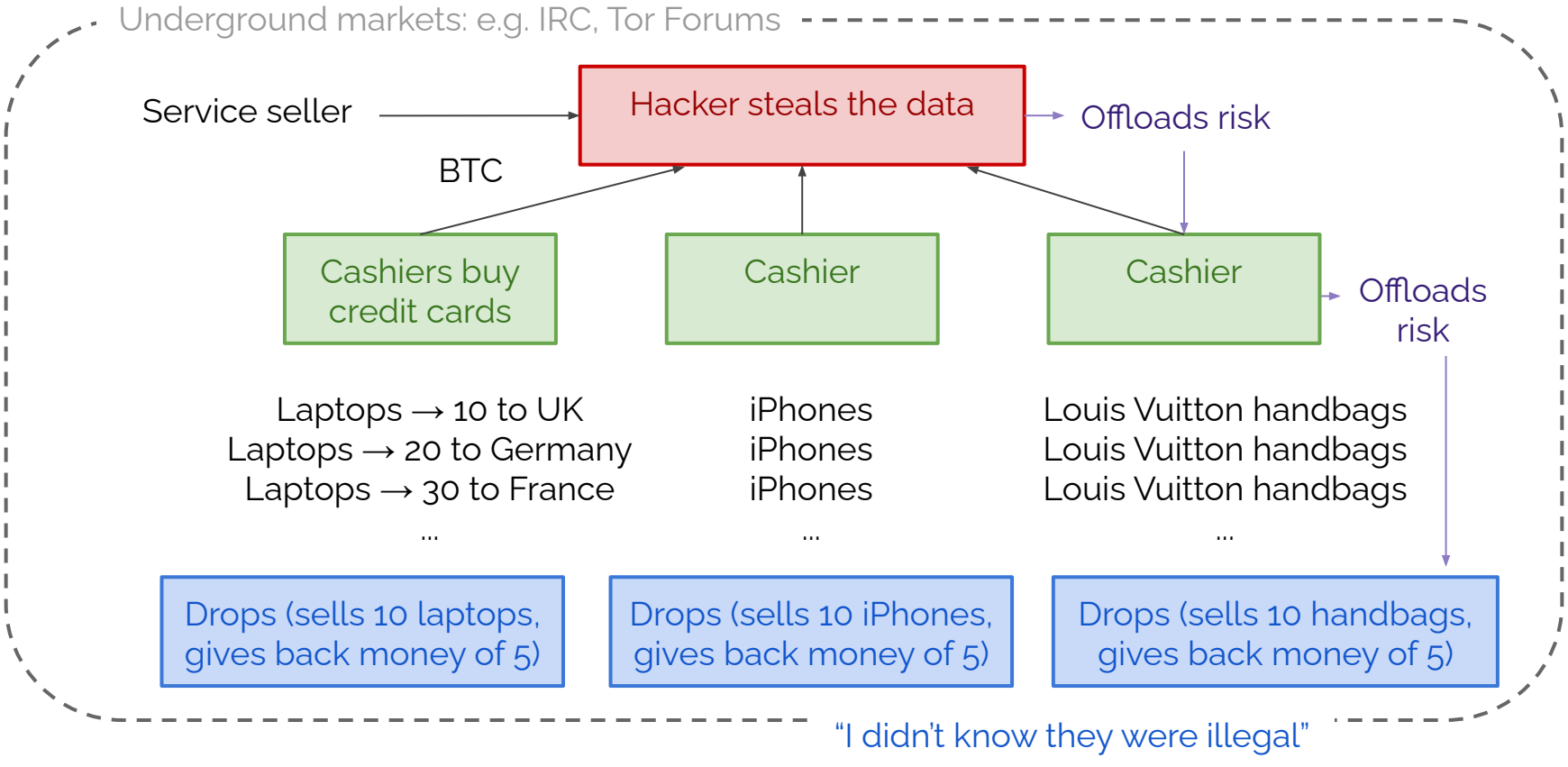
What is the motivation of most hackers? **£££** +

- Steal credit cards, paypal logins, …
- Ransomware
- Industrial espionage (steal some sensitive information to sell to someone else)



- Database breach, DoS attacks (use worms)
- Botnets, Fast flux, Domain flux
- Spam
- Keyloggers
- Rootkits
- Man-in-the-browser

Tactics What do hackers do with 1,000,000 credit card numbers?

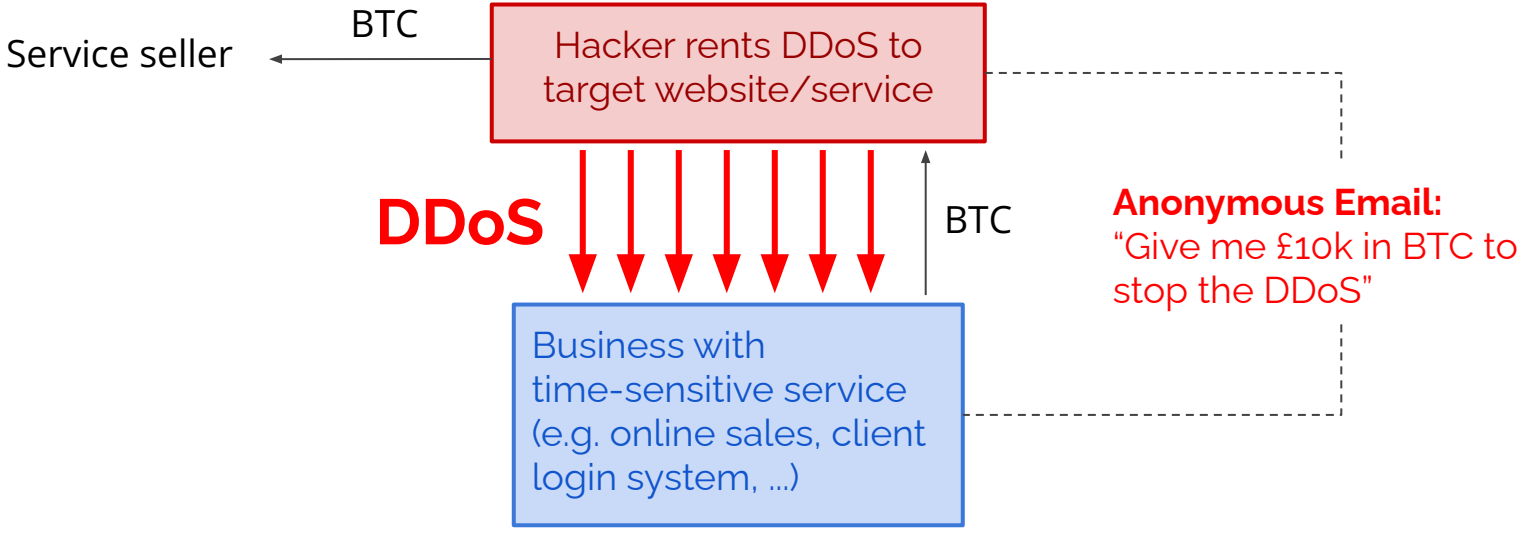


Tactics

What do hackers do with 1,000,000 credit card numbers?

Recording of underground market I captured recently

...more common tactics



Know the economy

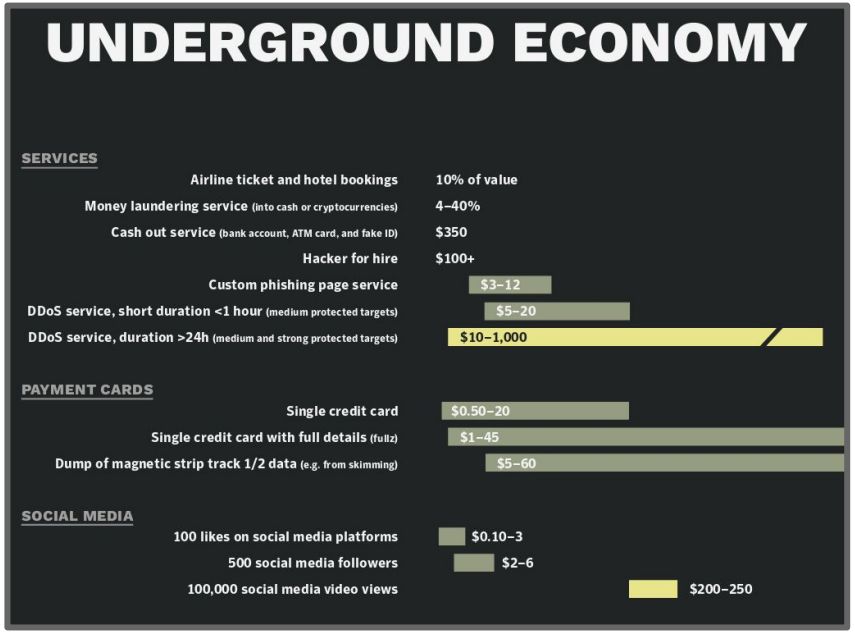
- Bitcoin transactions changes cyber landscape by enabling anonymous transactions

Economy can have fairly deep Hierarchies, for example:

- Hacker steals 1000 *Fullz* (credit card & CCV & name & address)
- Sells on Tor forum for 0.5 BTC (~£5k)
- Buyer sells groups of 20 to cashiers

Recent/weekly NCSC threat reports:

https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports

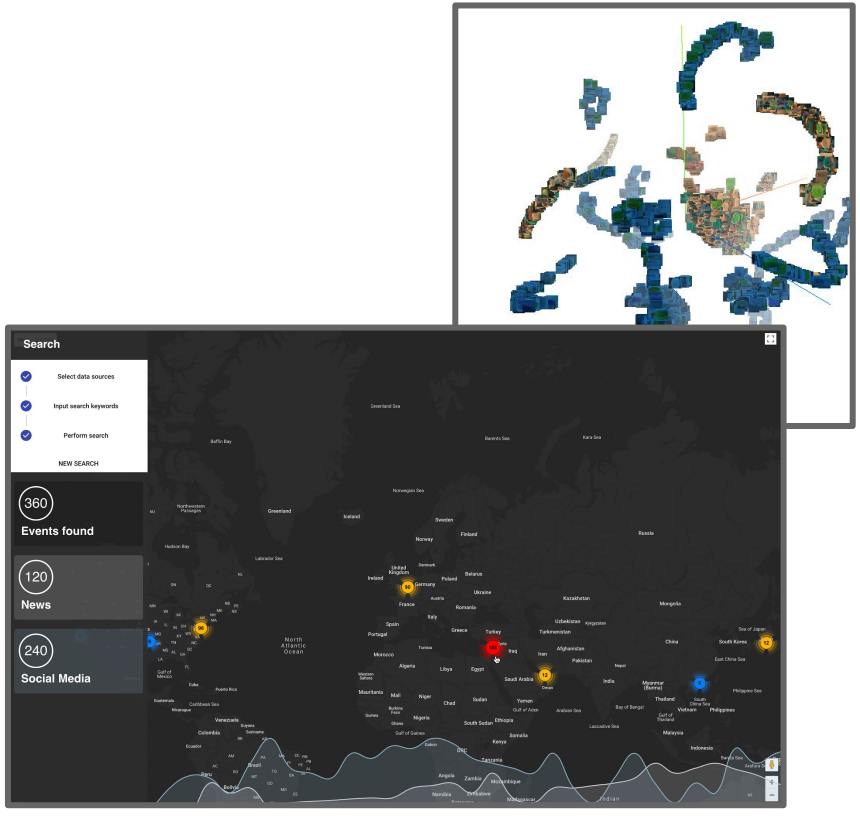


Planning strategies OSINT

With the advent of Machine Learning, strategies are more intelligent based on large-scale analytics

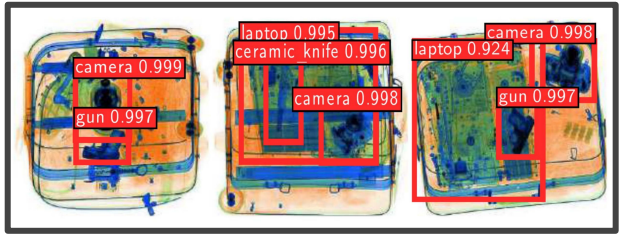
- Open source intelligence (OSINT)
- Sentiment analysis
- Targeted advertising
  - Targeted political campaigns
- Identifying criminals
  - Identifying threats

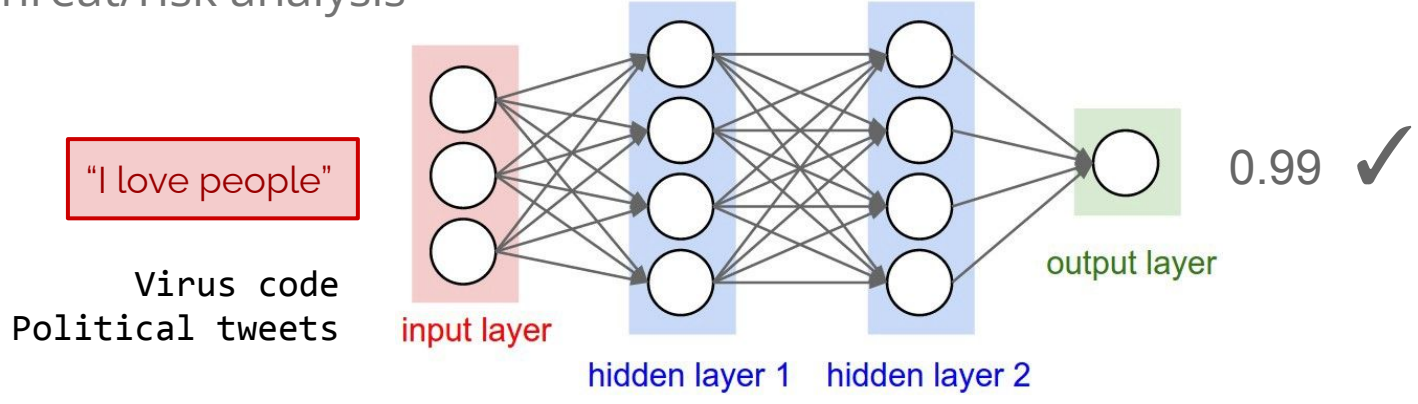
... positive and negative applications



Planning strategies ML techniques

- Classifiers
- Sentiment analysis
- Threat/risk analysis





https://github.com/bentrevett/pytorch-sentiment-analysis

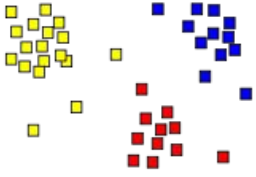
https://github.com/bentrevett/pytorch-sentiment-analysis/blob/main/4%20-%20Transformers.ipynb

https://www.sbert.net/ - recommended for OSINT final year projects

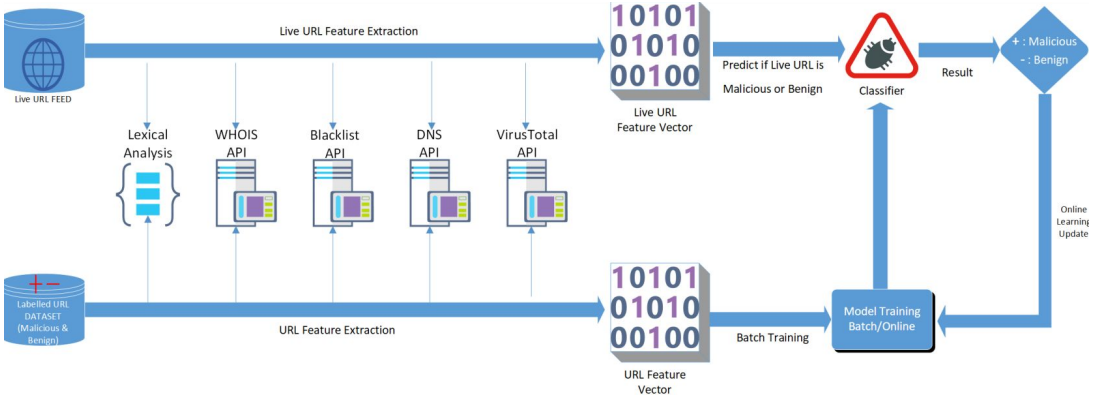
Planning strategies ML techniques

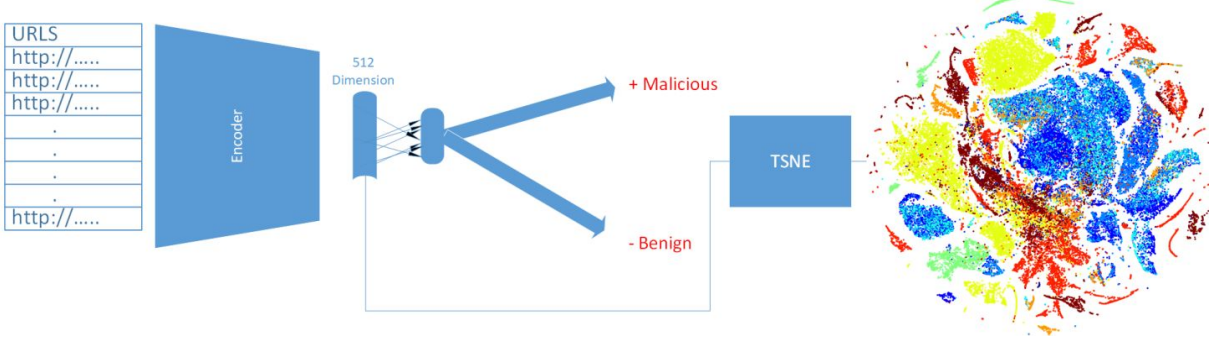
1. Automatic Classification ✓ ✓ ✗ ✗ ✓

2. Automatic Clustering



3. Automatic Localisation

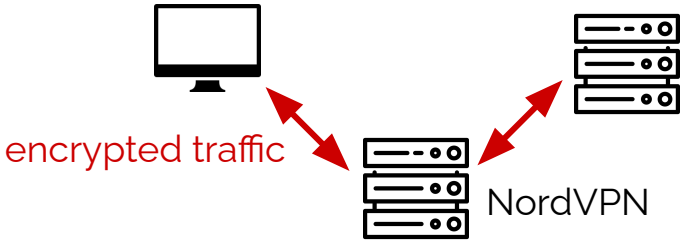




State-of-the-art: https://umap-learn.readthedocs.io/en/latest/supervised.html

IPs → ISP → identify you
https://whatismyipaddress.com/
Law: “Snoopers' Charter” & RIPA

Public WiFi → MITM/identify you
University Wired/Wireless → identify you

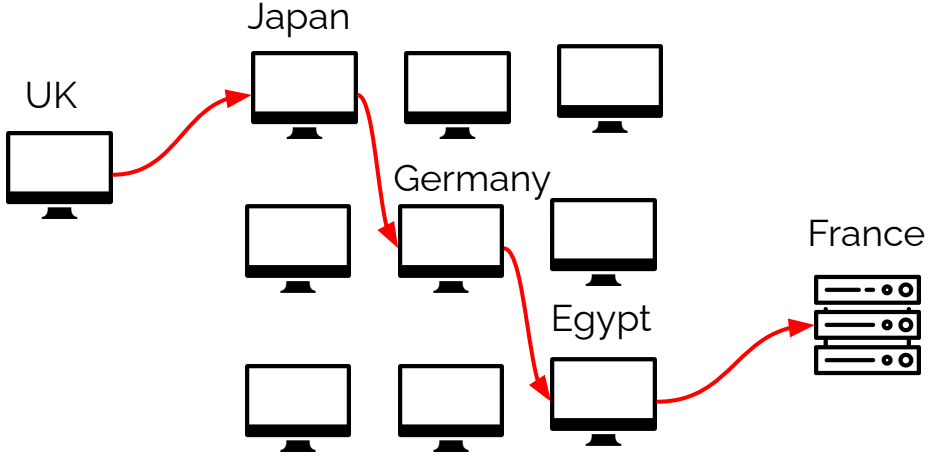


VPNs (Virtual Private Networks)

- Free VPNs log your information and sell them to 3rd parties.
- This is how they make money & survive
- Carefully check the T&C of the VPN
- Nice phone App & browser extension

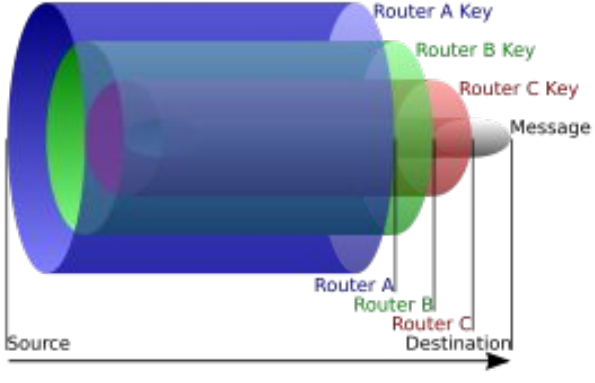
Tor enables *mostly* "anonymous" communication by onion routing

- Tor browser gives properly configured web browser (doesn't collect your history or cache your results). Javascript can be disabled easily.



Tor network "routers"

Onion routing encapsulates packets with layers of encryption



Case study: typical medium-sized corporate spending

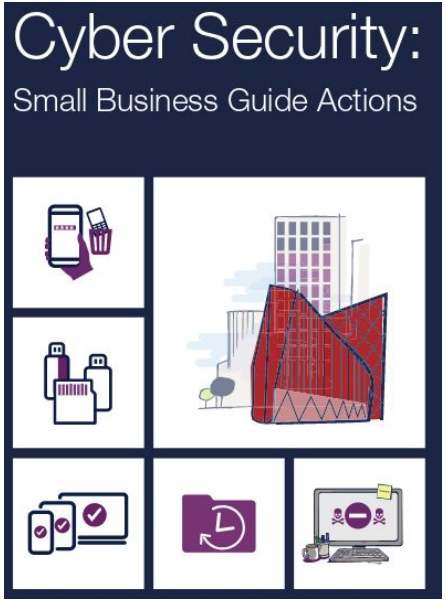
The remaining slides cover a small case study, which is the result of interviewing a local NE SME on appropriate Cyber Security budget & official guidance from the NCSC.

More links:

https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide

https://www.ncsc.gov.uk/files/small_business_guide_actions.pdf

National Cyber Security Centre
a part of GCHQ

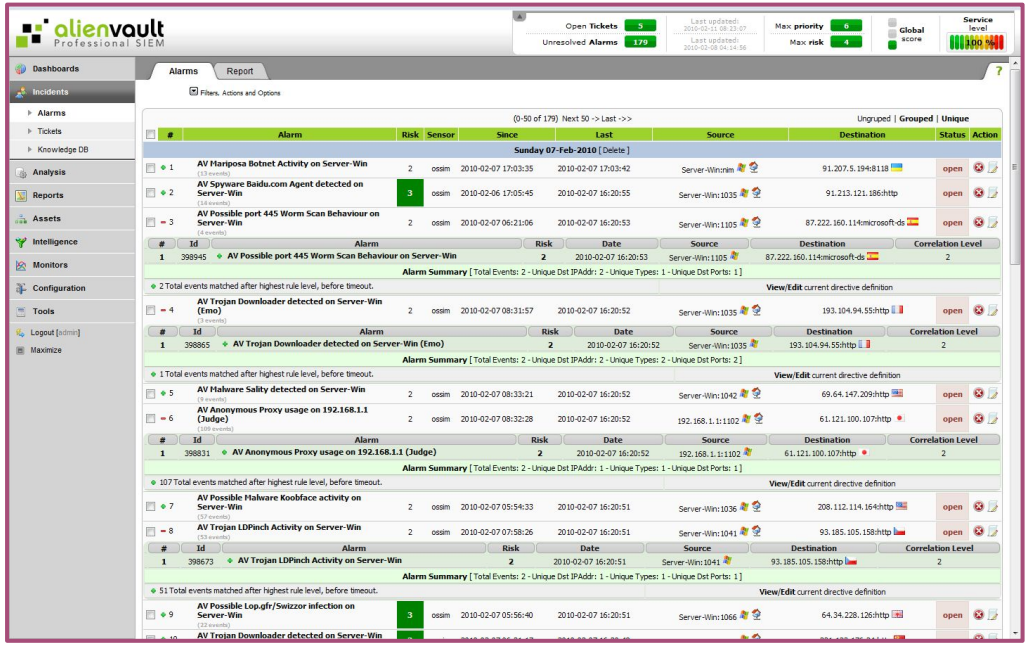


Security Operations Center (SOCs)

Teams proactively monitor the infrastructure

Tools/communities:

- Alien Vault
- Snort
- SNAIL
- OSEC
- OTX
- Logrhythm



Security Information & Event Management

Third party monitoring (£8k per year)

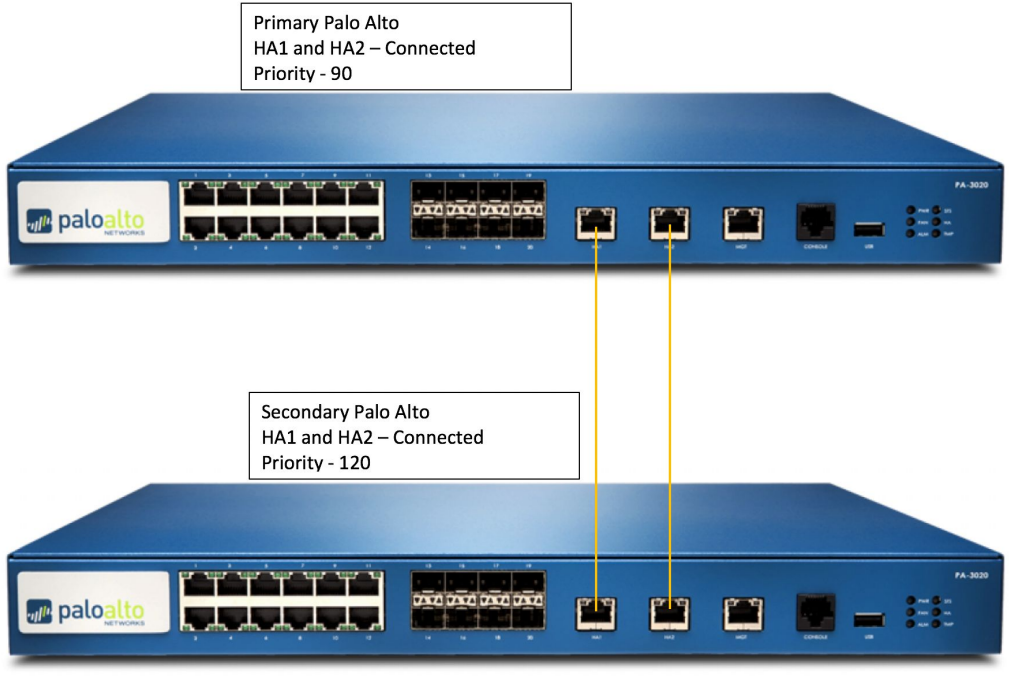
Log rhythm

- Create rules for alert types
- People review alerts & report back.
- ~**£5k per year** (standard package, what they choose)
- (~£70k per year for 24/7 package)

High Availability Pair

2 firewalls in active-active pair (means e.g. VOIP availability during updates)
Network/switches updated out-of-hours

1. Verify HA functionality before an upgrade
2. Confirms update on first device before updating the 2nd
3. Rollback w/o downtime
4. When finish the state will be unchanged.



https://www.thepacketwizard.com/blog/2018/02/08/palo-alto-upgrade-high-availability-ha-pair/

Automated Patch Management

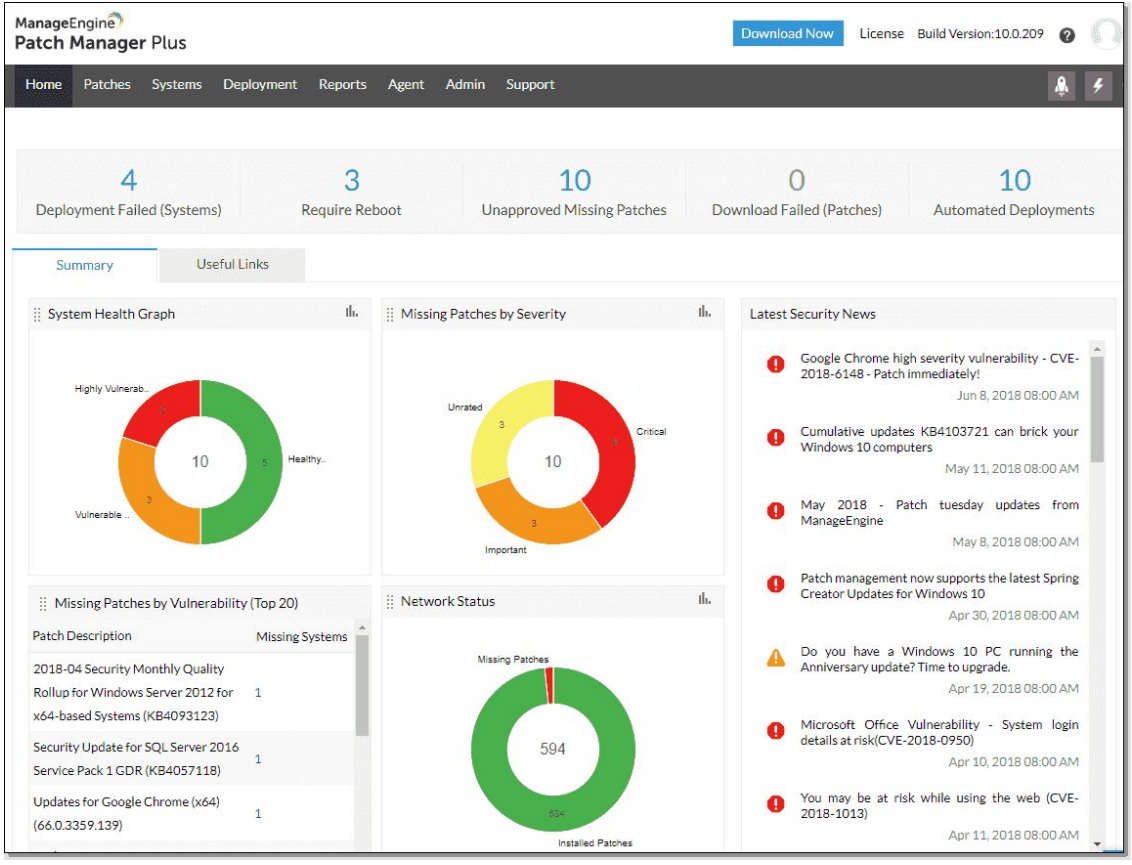
Patch manager plus pro (**£2k per year**)

Windows updates at appropriate times

- Adds control

Keeps software up to date but maintains compatibility

Includes third party (java, flash etc)



Endpoint protection, NG firewalls & full disk encryption

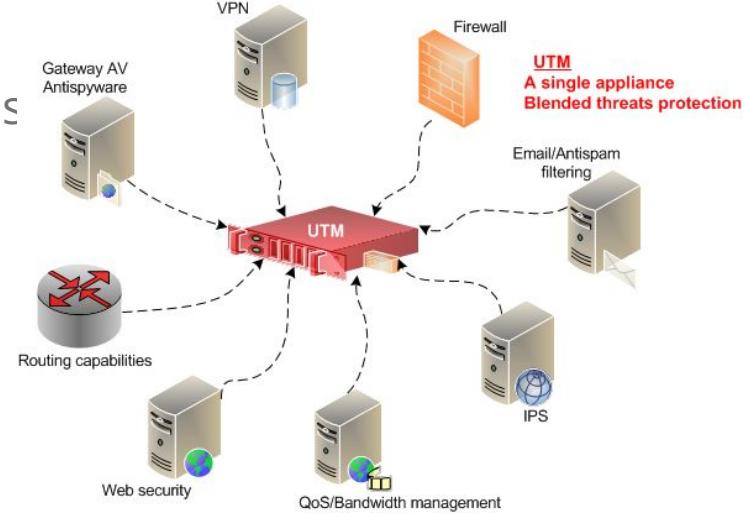
Safend data protection suite (DPS) endpoint protection

- e.g. locks down USBs ~**£20k+£2k** per year

UTM firewall (next-generation NG firewall, inspects packets in flight) …simple ones just blocks a port.

In-line antivirus, web filtering - ensure the firewalls don't slow e.g. uploading to Dropbox, advanced ones use AI to analyse threats

Hard drive encryption (TrueCrypt was compromised) - VeraCrypt



Falcon sandbox analysis

Suspicious file?

Spins up a VM, executes, sends screenshots/report of what it does

(balancing confidentiality - e.g. do we want to send personal details to third party?)

There are automated sandbox analysis such as Cuckoo, but can be a lot of effort to set up

Human Training

Training, e.g. “Junglemap NanoLearning”

- Delivers bite sized learning schedules, sends a link to half a dozen slides, reports back how many people and how long people spend on it - also does phishing exercises (e.g. new Costa shop example)