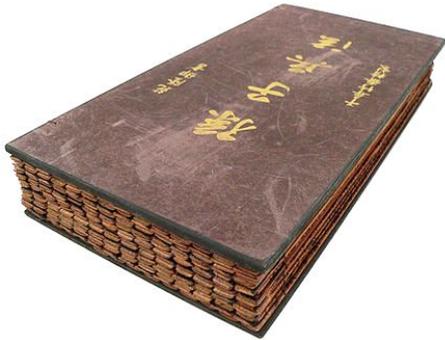


Cyber Security

The threat landscape

Chris G. Willcocks
Durham University



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)



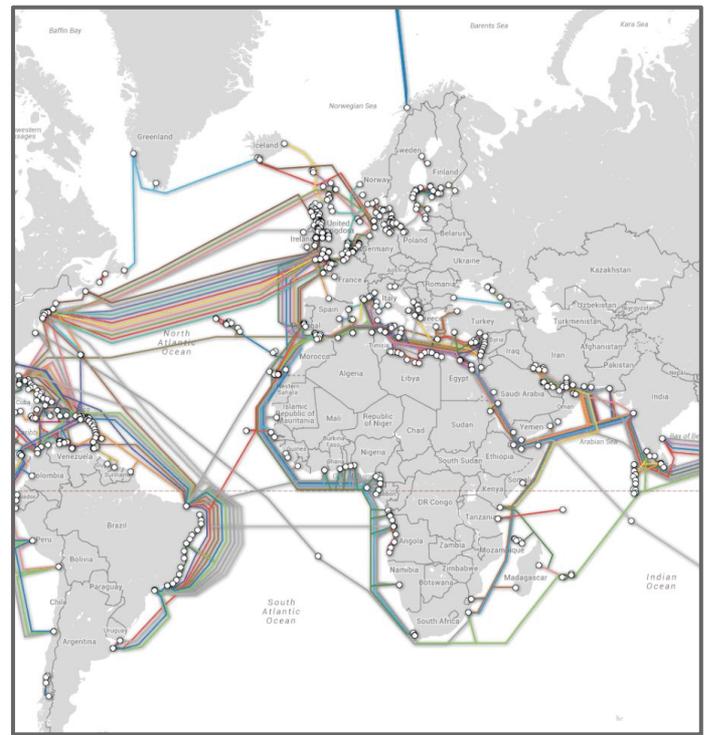
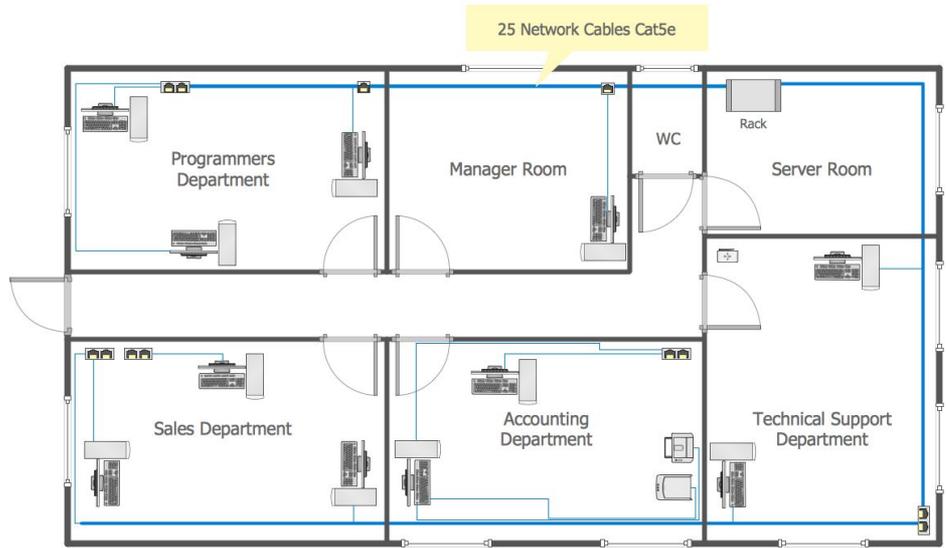
...depending on who the enemy is, different skills are required



Know the battlefield

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

- Think hierarchically



<https://www.submarinecablemap.com>

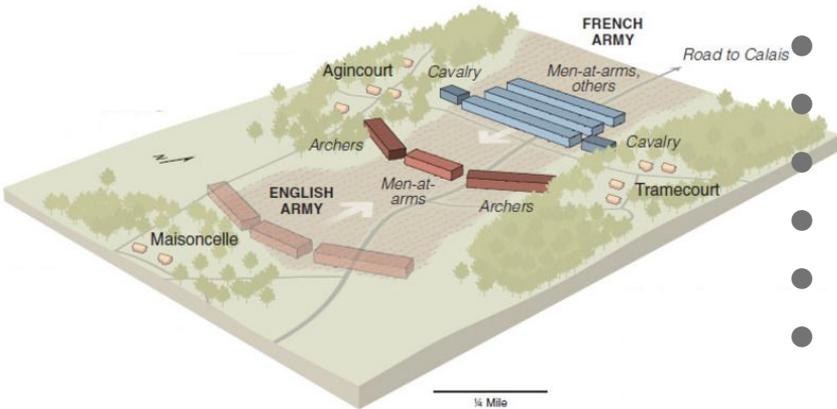


Know the most common tactics

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



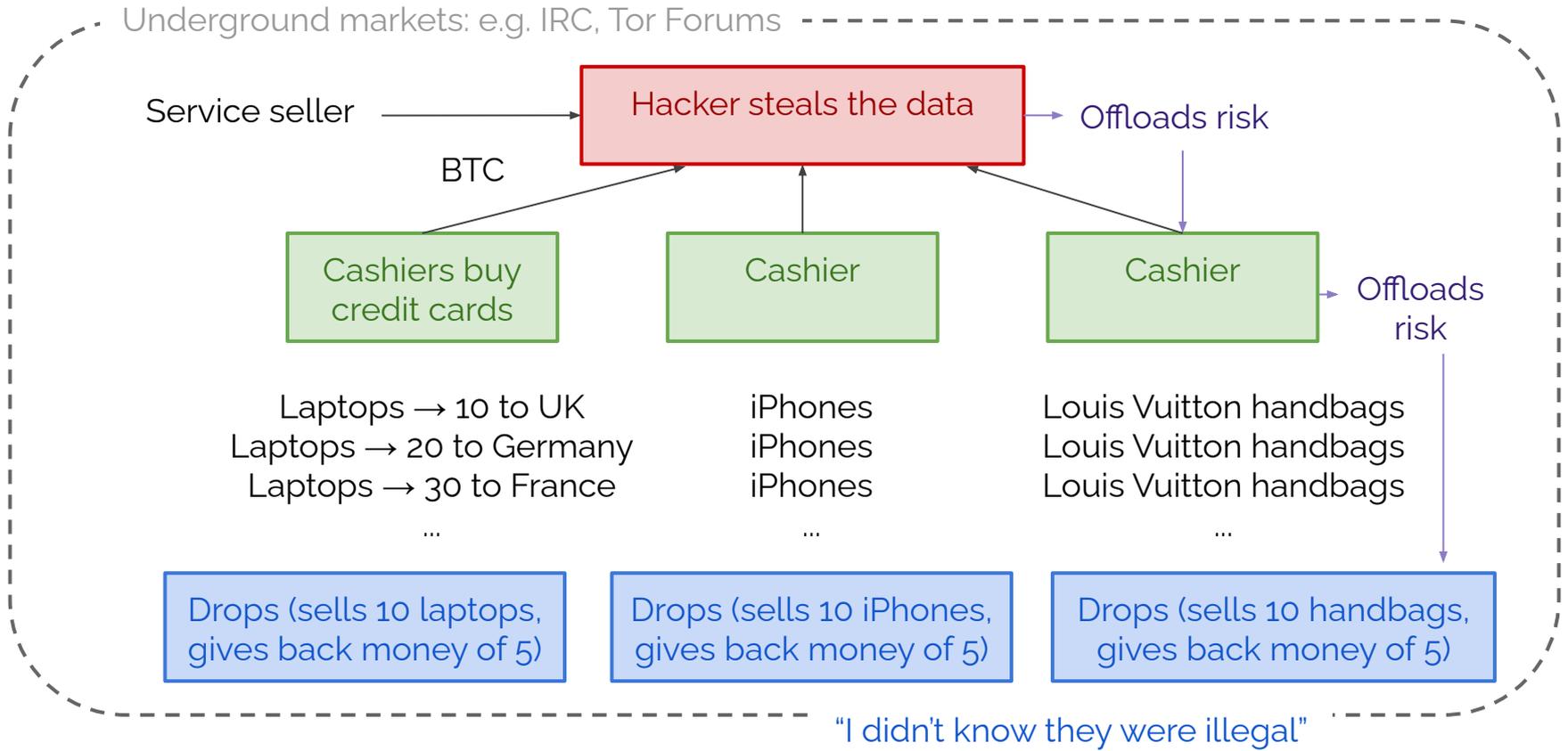
- Steal credit cards, paypal logins, ...
- Ransomware
- Industrial espionage (steal some sensitive information to sell to someone else)



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



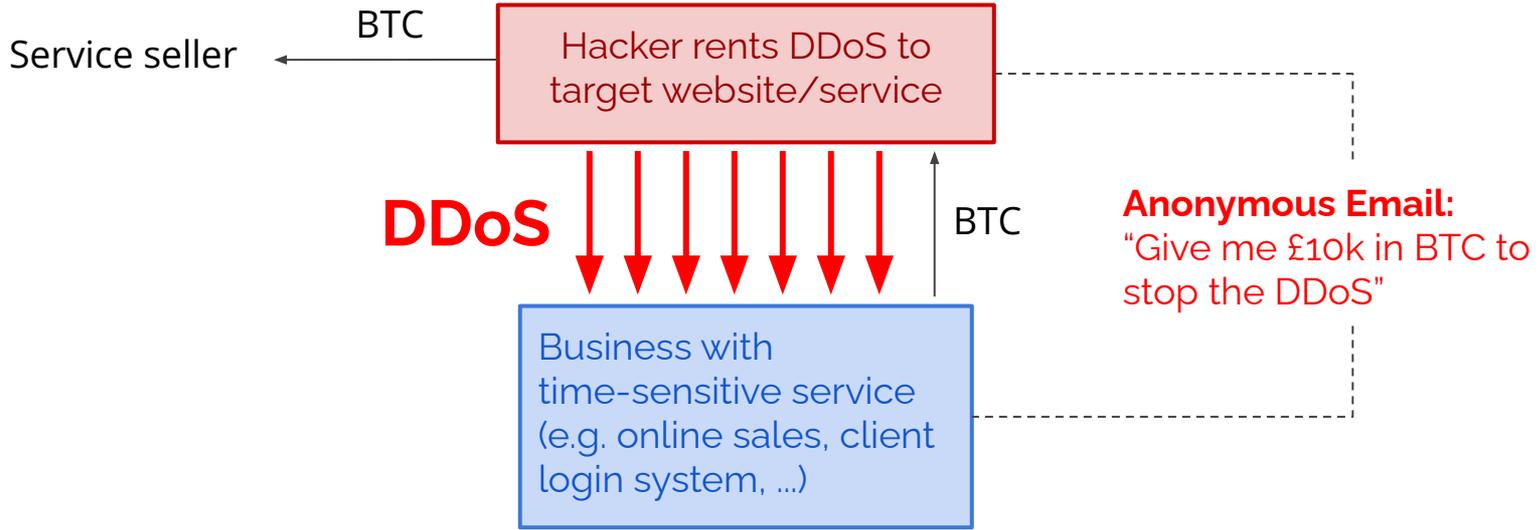
Tactics What do hackers do with 1,000,000 credit card numbers?





Recording of underground market I captured recently

...more common tactics





Know the economy

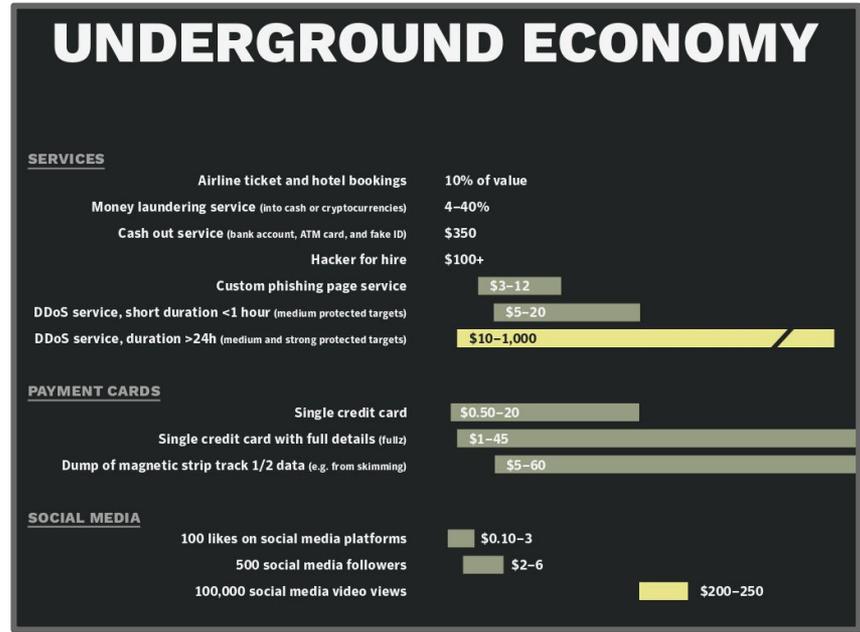
- Bitcoin transactions changes cyber landscape by enabling anonymous transactions

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>



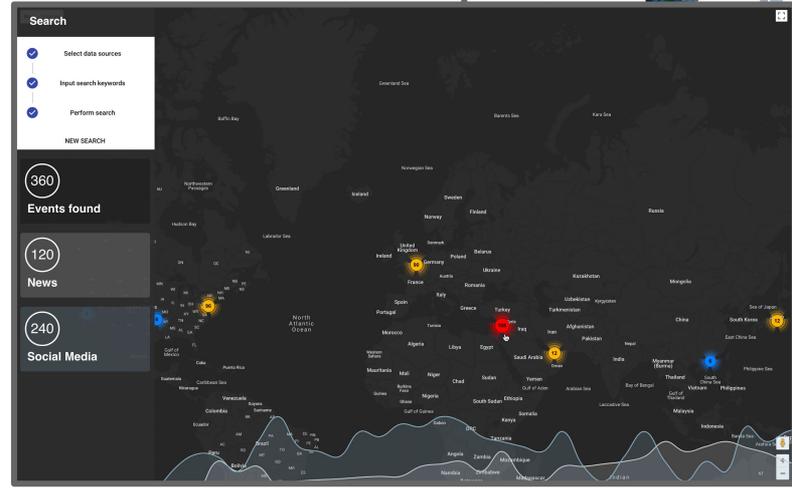
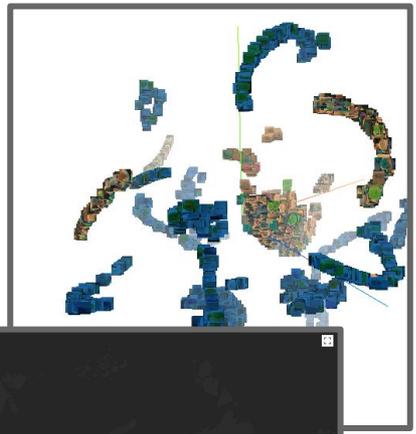


Planning strategies OSINT

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

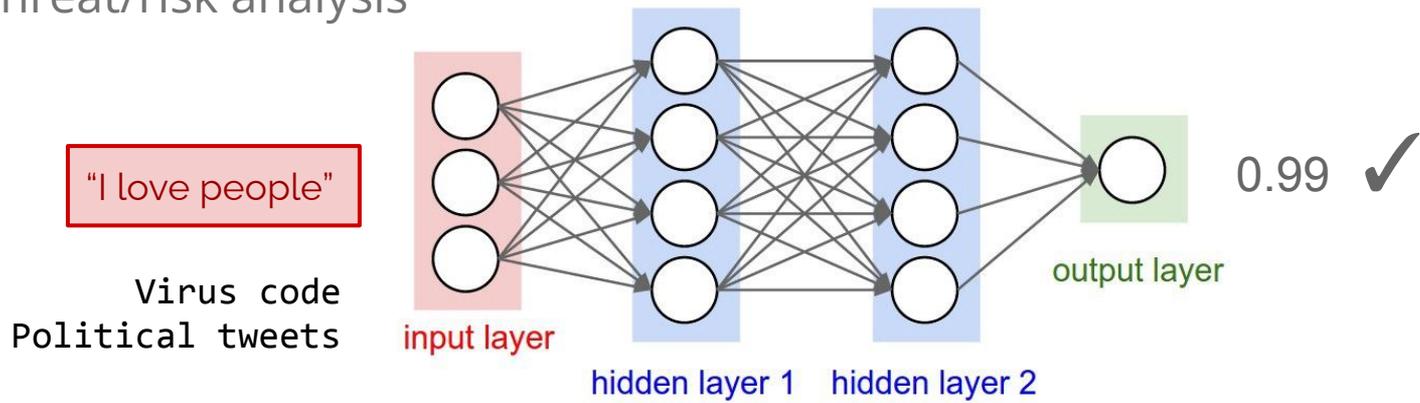
... positive and negative applications





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



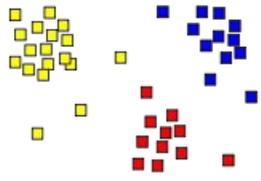
Planning strategies ML techniques

1. Automatic Classification

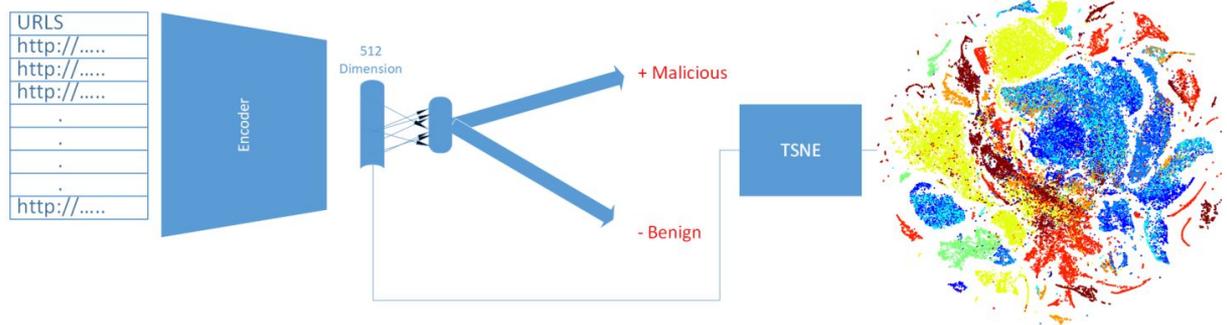
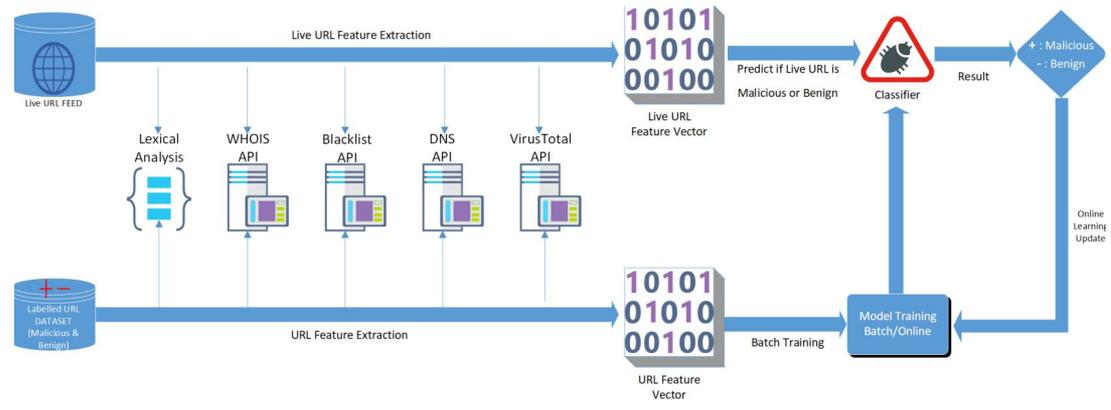
- ✓
- ✓
- ✗
- ✗
- ✓



2. Automatic Clustering



3. Automatic Localisation



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



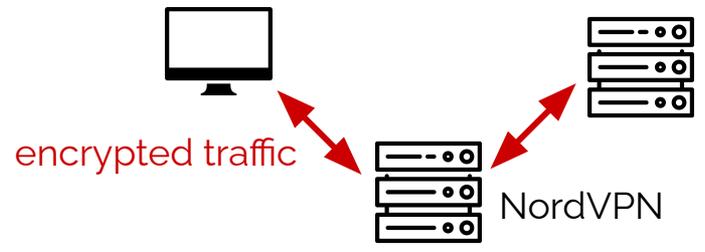
Spies Can "we" stay anonymous?

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

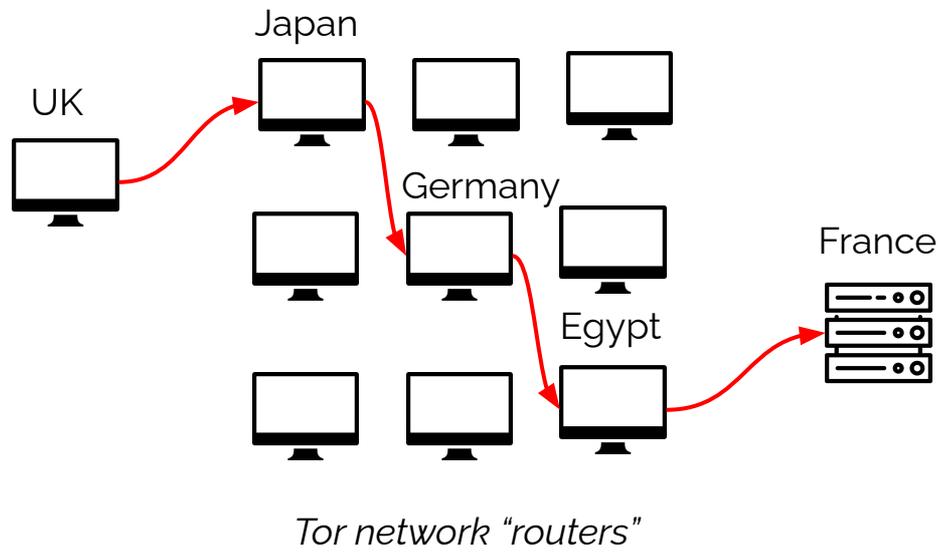




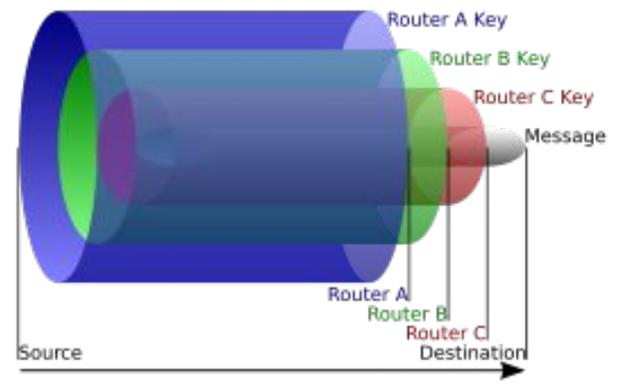
Spies Can "we" stay anonymous?

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.



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.

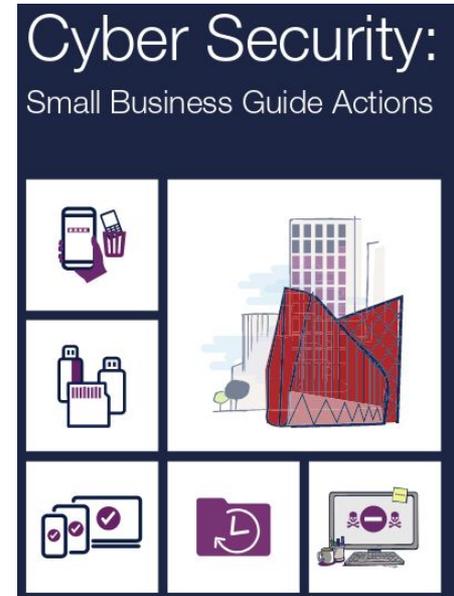
More links:

<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

The screenshot displays the AlienVault Professional SIEM interface. At the top, there are status indicators for Open Tickets (5), Unresolved Alarms (179), Last updated (2010-02-11 08:23:07), Max priority (6), Max risk (4), Global score, and Service level (100%). The main content area shows a list of alerts under the 'Alarms' tab. The table includes columns for Alarm, Risk, Sensor, Since, Last, Source, Destination, Status, and Action. Several alerts are visible, such as 'AV Havgosa Botnet Activity on Server-Win', 'AV Spyware Baidu.com Agent detected on Server-Win', and 'AV Possible port 445 Worm Scan Behaviour on Server-Win'. Each alert entry includes a risk level (e.g., 2 or 3) and a correlation level (e.g., 2). The interface also features a sidebar with navigation options like Dashboards, Incidents, Tickets, Knowledge DB, Analysis, Reports, Assets, Intelligence, Monitors, Configuration, Tools, and Logout [admin].



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)

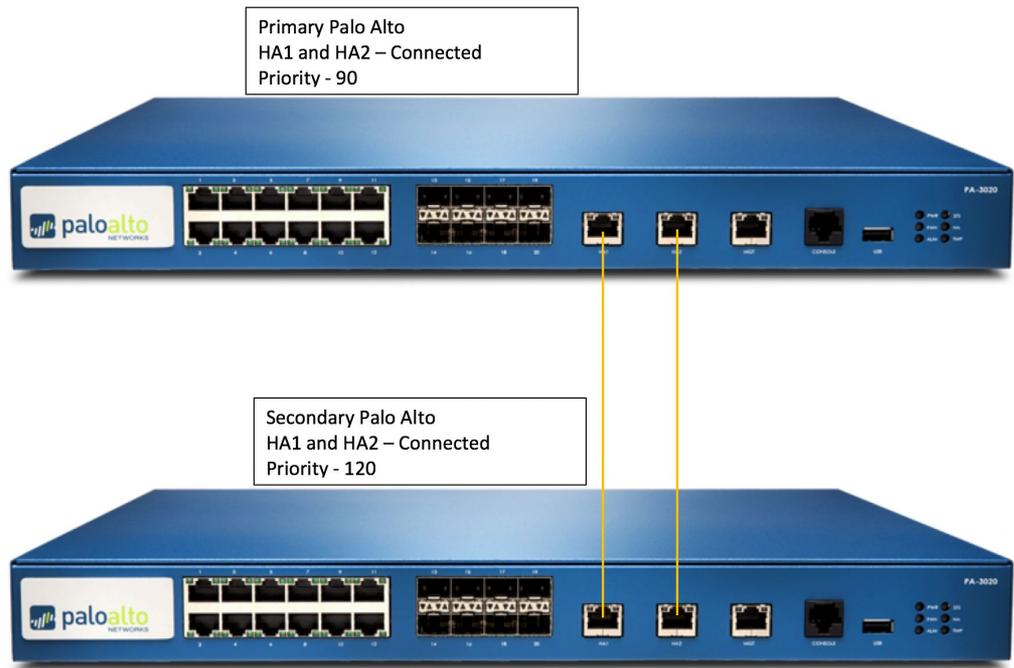




High Availability Pair

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.





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)

ManageEngine Patch Manager Plus | Download Now | License | Build Version:10.0.209

Home | Patches | Systems | Deployment | Reports | Agent | Admin | Support

4 Deployment Failed (Systems) | 3 Require Reboot | 10 Unapproved Missing Patches | 0 Download Failed (Patches) | 10 Automated Deployments

Summary | Useful Links

System Health Graph

Highly Vulnerab. (2) | Vulnerable... (3) | Healthy... (5) | 10

Missing Patches by Severity

Unrated (3) | Important (3) | Critical (4) | 10

Latest Security News

- Google Chrome high severity vulnerability - CVE-2018-6148 - Patch immediately! (Jun 8, 2018 08:00 AM)
- Cumulative updates KB4103721 can brick your Windows 10 computers (May 11, 2018 08:00 AM)
- May 2018 - Patch tuesday updates from ManageEngine (May 8, 2018 08:00 AM)
- Patch management now supports the latest Spring Creator Updates for Windows 10 (Apr 30, 2018 08:00 AM)
- Do you have a Windows 10 PC running the Anniversary update? Time to upgrade. (Apr 19, 2018 08:00 AM)
- Microsoft Office Vulnerability - System login details at risk(CVE-2018-0950) (Apr 10, 2018 08:00 AM)
- You may be at risk while using the web (CVE-2018-1013) (Apr 11, 2018 08:00 AM)

Missing Patches by Vulnerability (Top 20)

Patch Description	Missing Systems
2018-04 Security Monthly Quality Rollup for Windows Server 2012 for x64-based Systems (KB4093123)	1
Security Update for SQL Server 2016 Service Pack 1 GDR (KB4057118)	1
Updates for Google Chrome (x64) (66.0.3359.139)	1

Network Status

Missing Patches (1) | Installed Patches (594) | 594

Endpoint protection, NG firewalls & full disk encryption



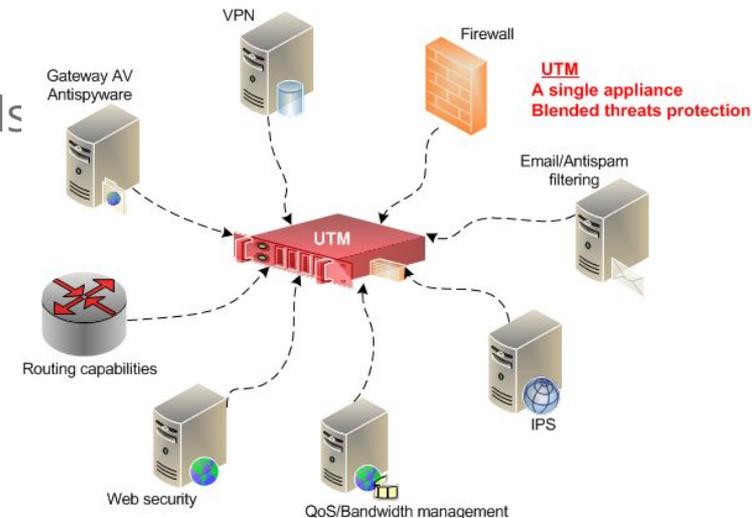
[Safend data protection suite](#) (DPS) endpoint protection

- 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 Reports

MALICIOUS

 **protonmail-desktop-setup-0.5....**

Analyzed on: 05/01/2018 00:50:02

Environment: Windows 7 64 bit

Threat Score: 85/100

AV Detection: 1% HW32.Packed

Indicators: 6 17 24

Network:  



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)

INTRODUCTION

Why kidnap people, when you can achieve the same profit with a single keystroke?

Ransomware is the new hostage taking.

Here you can find help to understand, prevent and respond to such virus attacks.



Navigation: back, forward, close (X), progress dots

HOW RANSOMWARE WORKS

First, the attack locks down all the files you have access to, including files on our servers.

Next, you are asked to pay an amount of money in order to regain access to your files.

- Your files are encrypted and cannot be opened without a password.
- Unless you have a backup, your files may be lost forever.
- Paying is no guarantee for getting your files back.

What can the consequences be, for yourself and for us, if such a virus finds its way to your PC?



Navigation: back, forward, close (X), progress dots