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

Foreign Governments

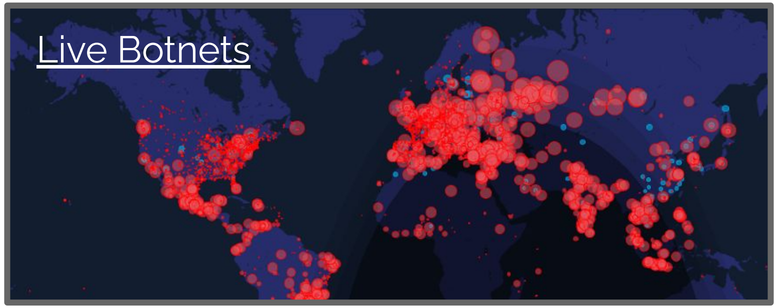
Political Activists

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)

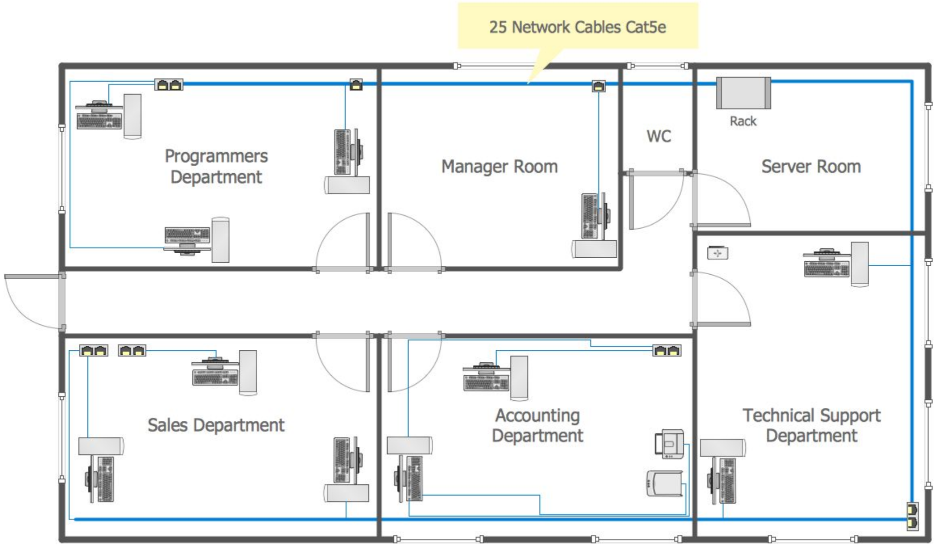


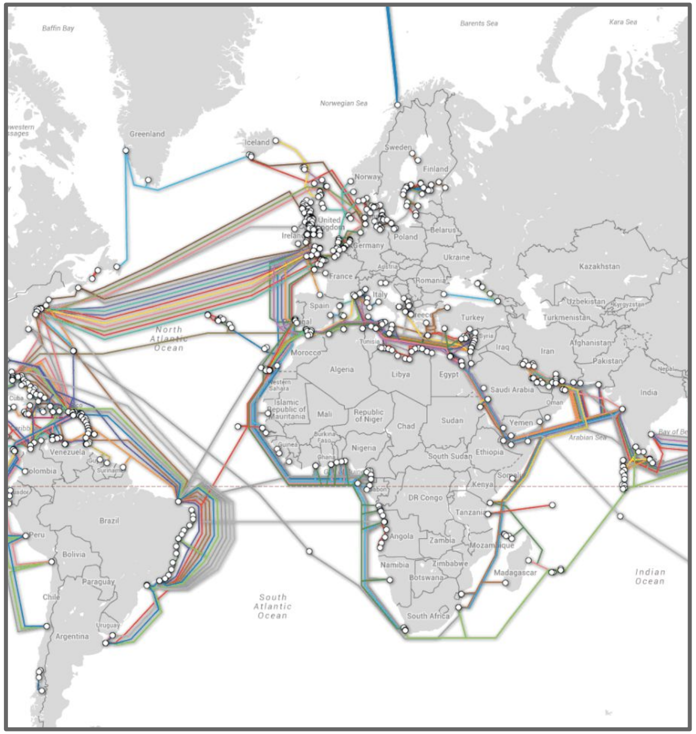
...depending on who the enemy is, different skills are required

Know the battlefield

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

- Think hierarchically



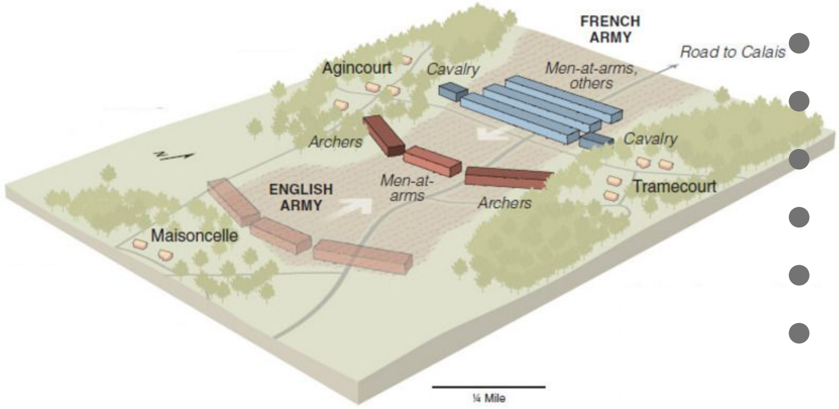


https://www.submarinecablemap.com

Know the most common tactics

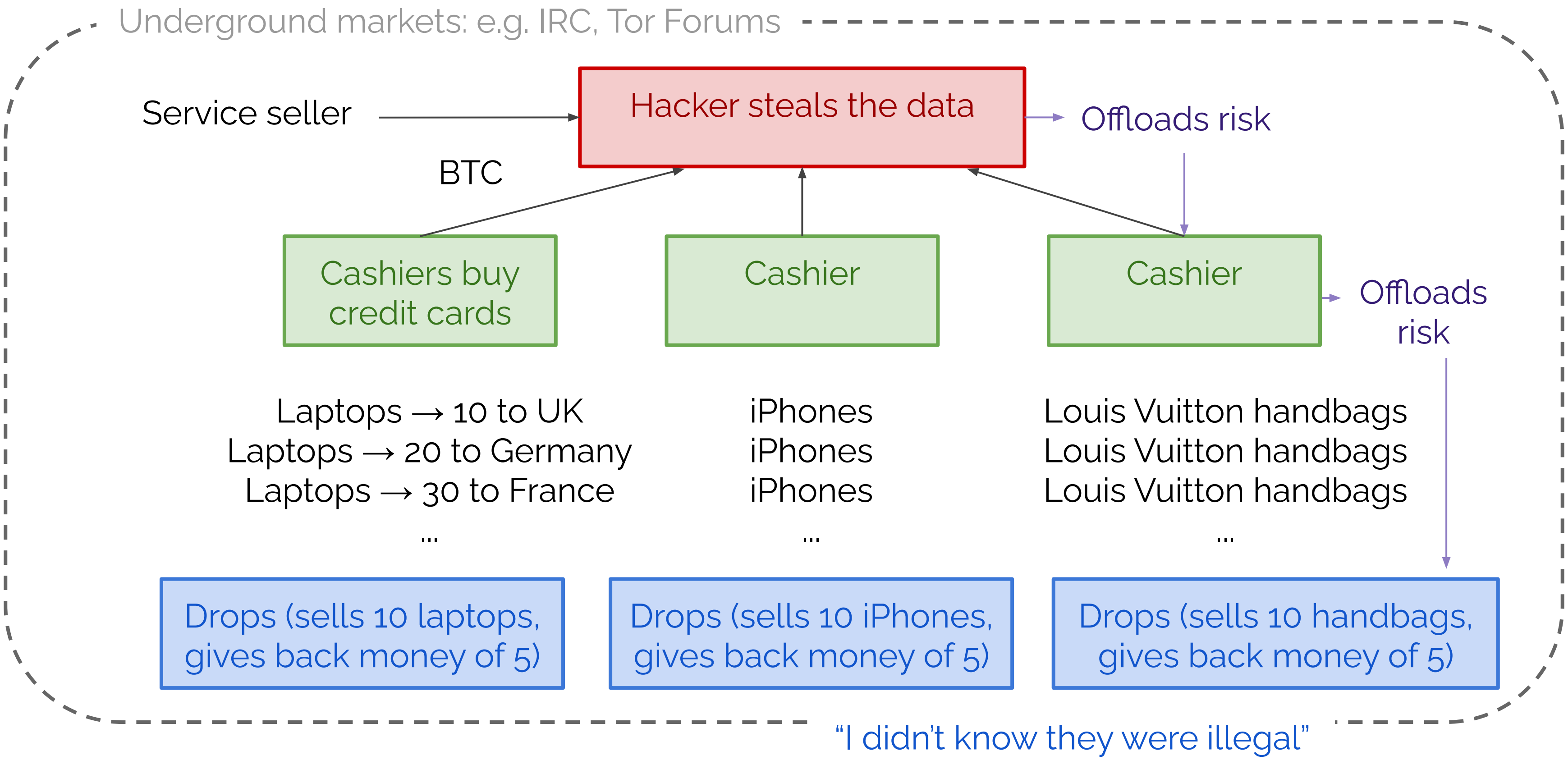
What is the motivation of most hackers? **£££ +**

- 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?



Underground markets: e.g. IRC, Tor Forums

Service seller

Hacker steals the data

Offloads risk

BTC

Cashiers buy credit cards

Cashier

Cashier

Offloads risk

Laptops → 10 to UK
Laptops → 20 to Germany
Laptops → 30 to France
...

iPhones
iPhones
iPhones
...

Louis Vuitton handbags
Louis Vuitton handbags
Louis Vuitton handbags
...

Drops (sells 10 laptops, gives back money of 5)

Drops (sells 10 iPhones, gives back money of 5)

Drops (sells 10 handbags, gives back money of 5)

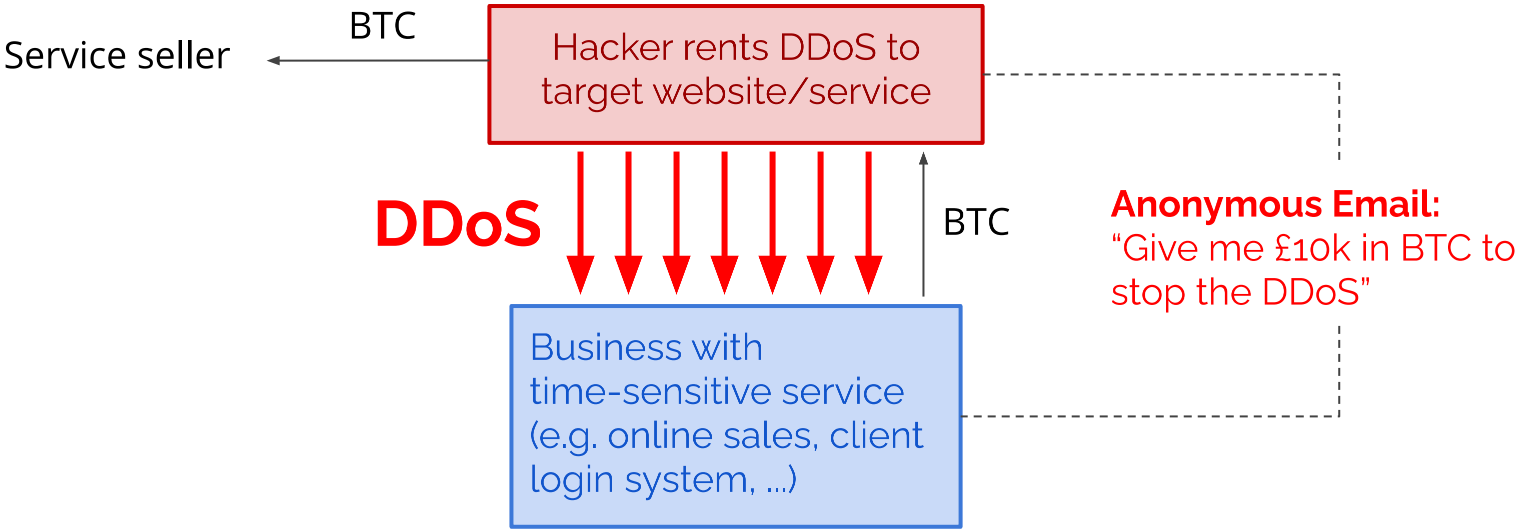
"I didn't know they were illegal"

Tactics

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

Recording of underground market I captured recently

...more common tactics



Service seller

BTC

Hacker rents DDoS to target website/service

DDoS

BTC

Business with time-sensitive service (e.g. online sales, client login system, ...)

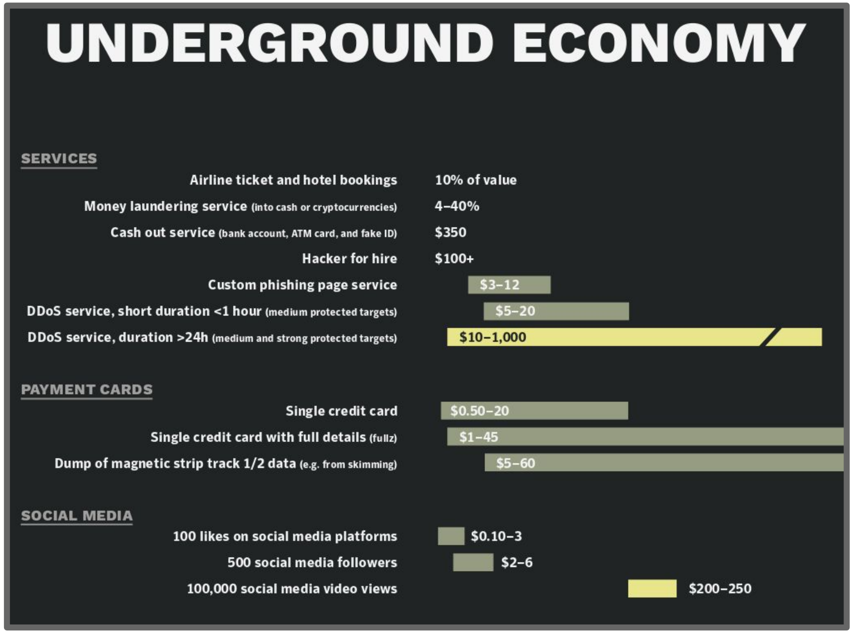
Anonymous Email:
"Give me £10k in BTC to stop the DDoS"

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 1 BTC (~£5k)
- Buyer sells groups of 20 to cashiers



Recent/weekly NCSC threat reports:

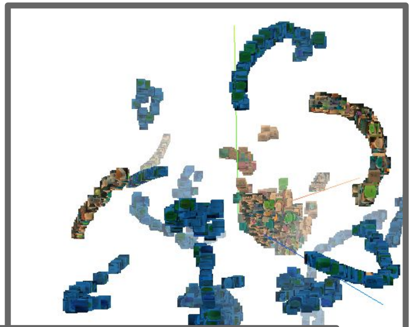
https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports

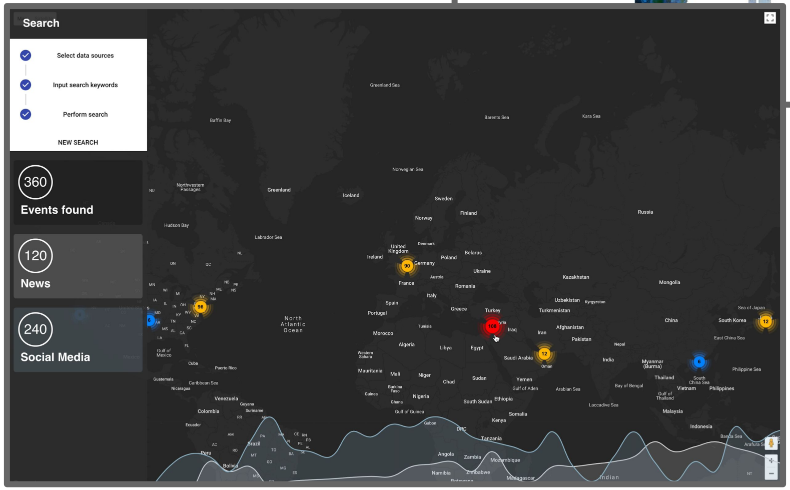
Planning strategies OSINT

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





Search

☑ Select data sources

☑ Input search keywords

☑ Perform search

NEW SEARCH

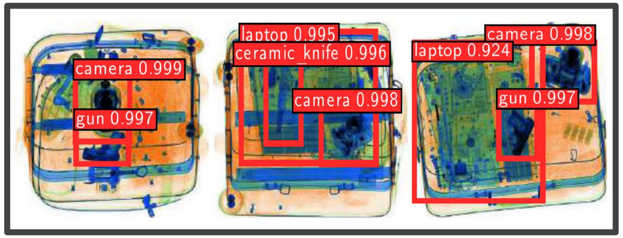
360 Events found

120 News

240 Social Media

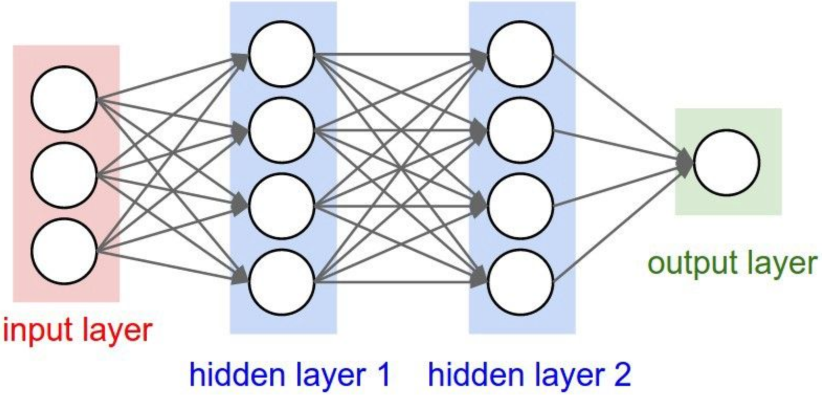
Planning strategies ML techniques

- Classifiers
- Sentiment analysis
- Threat/risk analysis



"I love people"

Virus code
Political tweets



0.99 ✓

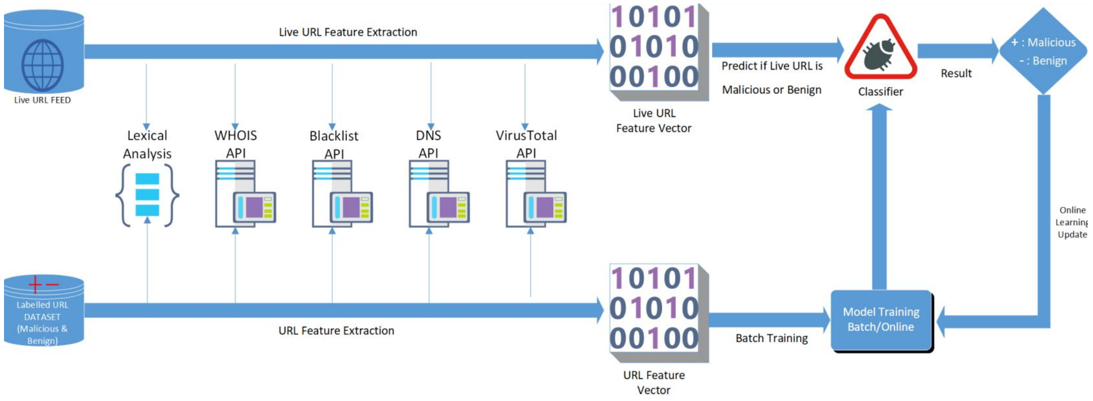
https://github.com/bentrevett/pytorch-sentiment-analysis

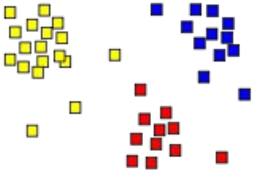
https://colab.research.google.com/github/bentrevett/pytorch-sentiment-analysis/blob/master/6 - Transformers for Sentiment Analysis.ipynb

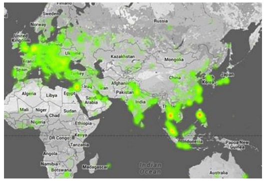
Planning strategies ML techniques

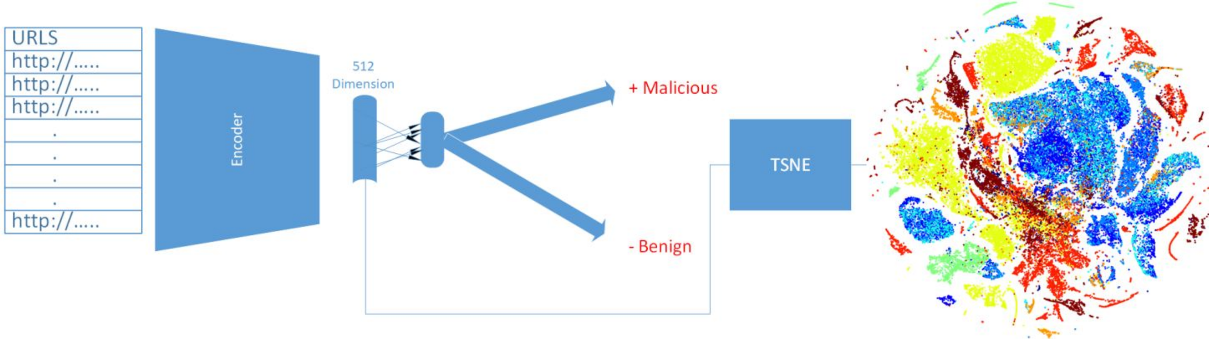
✓
✓
✗
✗
✓

1. Automatic Classification
2. Automatic Clustering
3. Automatic Localisation









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

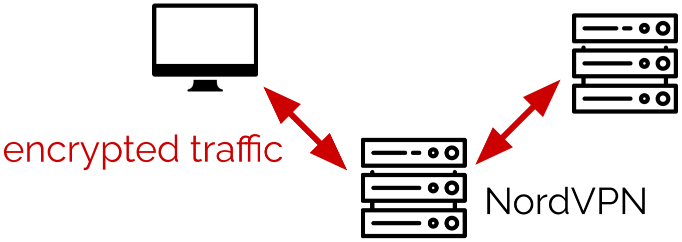
Spies Can “we” stay anonymous?

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)

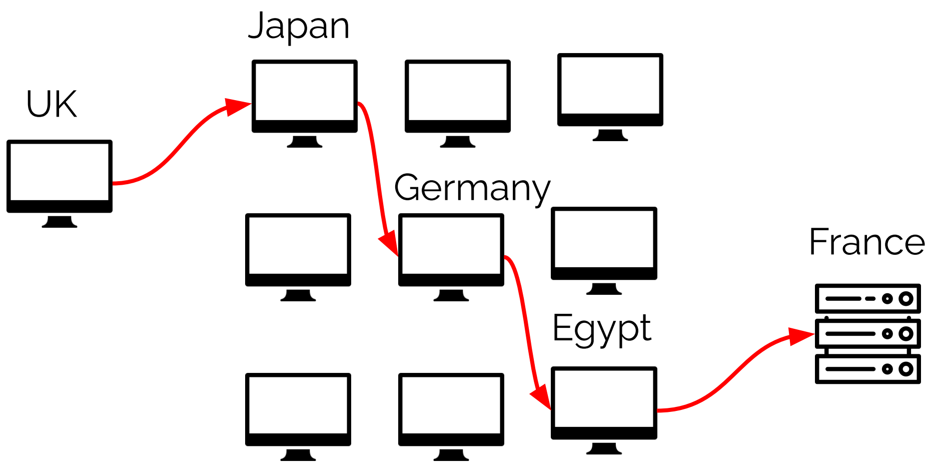
- Free VPNs log your information and sell them to 3rd parties.
- This is how they make money & survive
- Carefully check the T&C of the VPN
- Nice phone App & browser extension



Spies Can “we” stay anonymous?

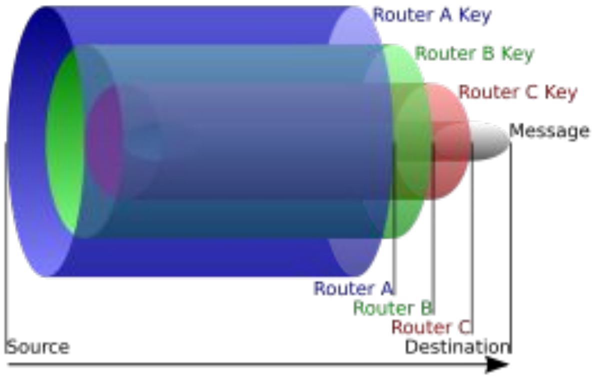
Tor enables *mostly* “anonymous” communication by onion routing

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



Tor network “routers”

Onion routing encapsulates packets with layers of encryption



Case study: typical medium-sized corporate spending

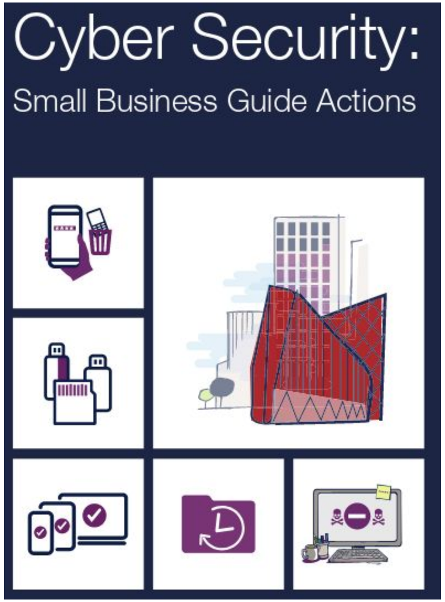
The remaining slides cover a small case study, which is the result of interviewing a local NE SME on appropriate Cyber Security budget & official guidance from the NCSC.

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



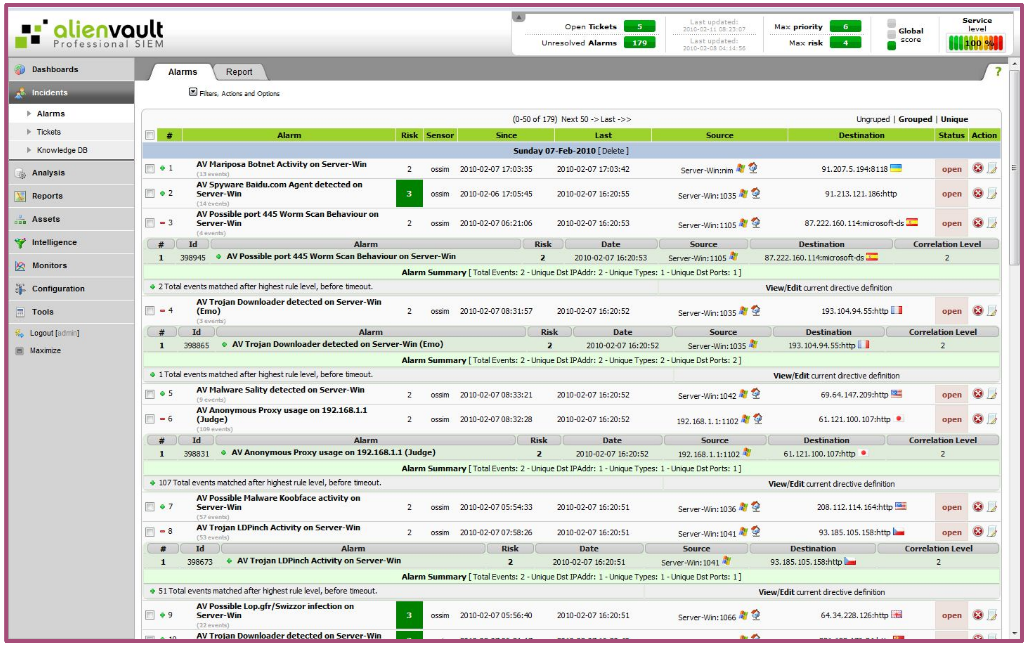
Cyber Security:
Small Business Guide Actions

Security Operations Center (SOCs)

Teams proactively monitor the infrastructure

Tools/communities:

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



(0-50 of 179) Next 50 -> Last ->>   Ungruped | **Grouped** | **Unique**

#	Alarm	Risk	Sensor	Since	Last	Source	Destination	Status	Action
	Sunday 07-Feb-2010 [Delete]								
1	**AV Mariposa Botnet Activity on Server-Win** (13 events)	2	ossim	2010-02-07 17:03:35	2010-02-07 17:03:42	Server-Win:nim	91.207.5.194:8118	open	
2	**AV Spyware Baidu.com Agent detected on Server-Win** (14 events)	3	ossim	2010-02-06 17:05:45	2010-02-07 16:20:55	Server-Win:1035	91.213.121.186:http	open	
3	**AV Possible port 445 Worm Scan Behaviour on Server-Win** (4 events)	2	ossim	2010-02-07 06:21:06	2010-02-07 16:20:53	Server-Win:1105	87.222.160.114:microsoft-ds	open	

#	Id	Alarm	Risk	Date	Source	Destination	Correlation Level
1	398945	**AV Possible port 445 Worm Scan Behaviour on Server-Win**	2	2010-02-07 16:20:53	Server-Win:1105	87.222.160.114:microsoft-ds	2

Alarm Summary [Total Events: 2 - Unique Dst IPAddr: 2 - Unique Types: 1 - Unique Dst Ports: 1]

2 Total events matched after highest rule level, before timeout.   **View/Edit** current directive definition

#	Alarm	Risk	Sensor	Since	Last	Source	Destination	Status	Action
4	**AV Trojan Downloader detected on Server-Win (Emo)** (3 events)	2	ossim	2010-02-07 08:31:57	2010-02-07 16:20:52	Server-Win:1035	193.104.94.55:http	open	

#	Id	Alarm	Risk	Date	Source	Destination	Correlation Level
1	398865	**AV Trojan Downloader detected on Server-Win (Emo)**	2	2010-02-07 16:20:52	Server-Win:1035	193.104.94.55:http	2

Alarm Summary [Total Events: 2 - Unique Dst IPAddr: 2 - Unique Types: 2 - Unique Dst Ports: 2]

1 Total events matched after highest rule level, before timeout.   **View/Edit** current directive definition

#	Alarm	Risk	Sensor	Since	Last	Source	Destination	Status	Action
5	**AV Malware Sality detected on Server-Win** (9 events)	2	ossim	2010-02-07 08:33:21	2010-02-07 16:20:52	Server-Win:1042	69.64.147.209:http	open	
6	**AV Anonymous Proxy usage on 192.168.1.1 (Judge)** (109 events)	2	ossim	2010-02-07 08:32:28	2010-02-07 16:20:52	192.168.1.1:1102	61.121.100.107:http	open	

#	Id	Alarm	Risk	Date	Source	Destination	Correlation Level
1	398831	**AV Anonymous Proxy usage on 192.168.1.1 (Judge)**	2	2010-02-07 16:20:52	192.168.1.1:1102	61.121.100.107:http	2

Alarm Summary [Total Events: 2 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]

107 Total events matched after highest rule level, before timeout.   **View/Edit** current directive definition

#	Alarm	Risk	Sensor	Since	Last	Source	Destination	Status	Action
7	**AV Possible Malware Koobface activity on Server-Win** (57 events)	2	ossim	2010-02-07 05:54:33	2010-02-07 16:20:51	Server-Win:1036	208.112.114.164:http	open	
8	**AV Trojan LDPinch Activity on Server-Win** (53 events)	2	ossim	2010-02-07 07:58:26	2010-02-07 16:20:51	Server-Win:1041	93.185.105.158:http	open	

#	Id	Alarm	Risk	Date	Source	Destination	Correlation Level
1	398673	**AV Trojan LDPinch Activity on Server-Win**	2	2010-02-07 16:20:51	Server-Win:1041	93.185.105.158:http	2

Alarm Summary [Total Events: 2 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]

51 Total events matched after highest rule level, before timeout.   **View/Edit** current directive definition

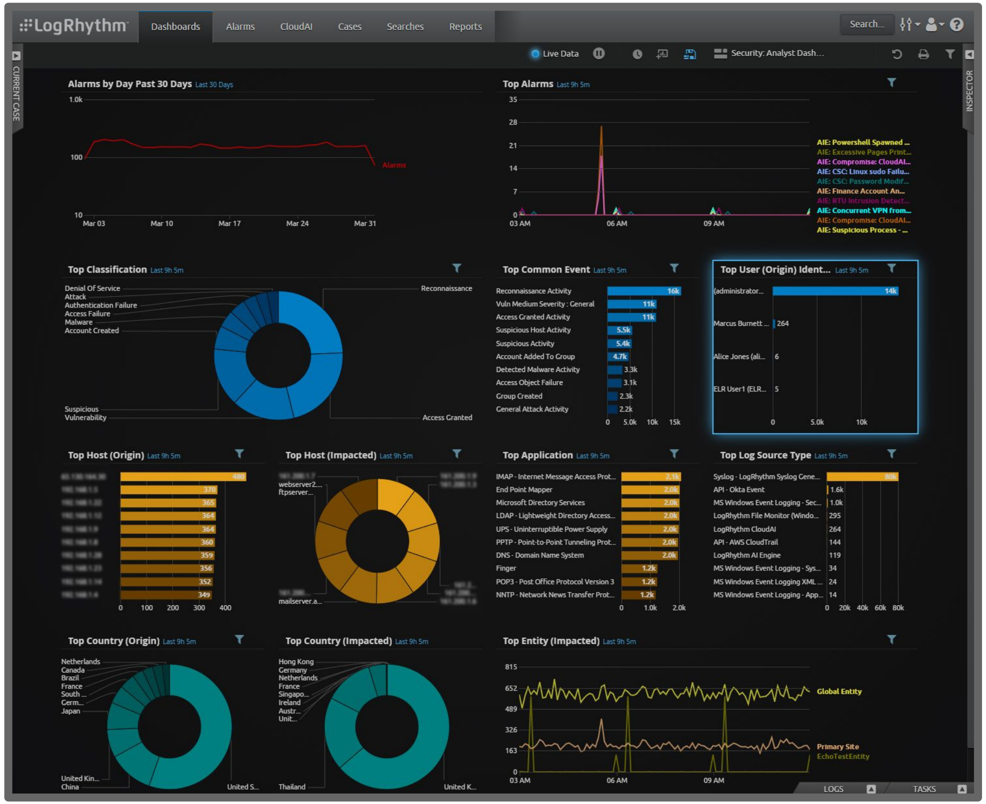
#	Alarm	Risk	Sensor	Since	Last	Source	Destination	Status	Action
9	**AV Possible Lop.gfr/Swizzor infection on Server-Win** (22 events)	3	ossim	2010-02-07 05:56:40	2010-02-07 16:20:51	Server-Win:1066	64.34.228.126:http	open	
10	**AV Trojan Downloader detected on Server-Win**								

Security Information & Event Management

Third party monitoring (£8k per year)

Log rhythm

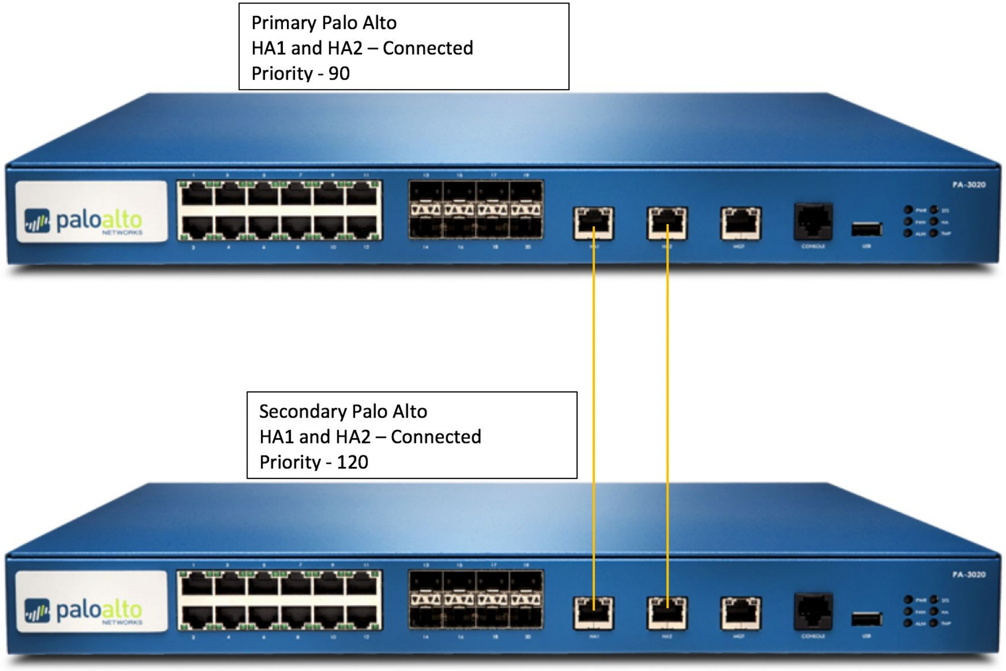
- Create rules for alert types
- People review alerts & report back.
- ~**£5k per year** (standard package, what they choose)
- (~£70k per year for 24/7 package)


LogRhythm
Dashboards
Alarms
CloudAI
Cases
Searches
Reports
Search...
Live Data
Security: Analyst Dash...
CURRENT CASE
INSPECTOR
Alarms by Day Past 30 Days Last 30 Days
1.0k
100
10
Mar 03
Mar 10
Mar 17
Mar 24
Mar 31
Alarms
Top Alarms Last 9h 5m
35
28
21
14
7
0
03 AM
06 AM
09 AM
AIE: Powershell Spawned ...
AIE: Excessive Pages Print...
AIE: Compromise: CloudAI...
AIE: CSC: Linux sudo Failu...
AIE: CSC: Password Modif...
AIE: Finance Account An...
AIE: RTU Intrusion Detect...
AIE: Concurrent VPN from...
AIE: Compromise: CloudAI...
AIE: Suspicious Process - ...
Top Classification Last 9h 5m
Denial Of Service
Attack
Authentication Failure
Access Failure
Malware
Account Created
Suspicious
Vulnerability
Reconnaissance
Access Granted
Top Common Event Last 9h 5m
Reconnaissance Activity 16k
Vuln Medium Severity : General 11k
Access Granted Activity 11k
Suspicious Host Activity 5.5k
Suspicious Activity 5.4k
Account Added To Group 4.7k
Detected Malware Activity 3.3k
Access Object Failure 3.1k
Group Created 2.3k
General Attack Activity 2.2k
0
5.0k
10k
15k
Top User (Origin) Ident... Last 9h 5m
(administrator... 14k
Marcus Burnett ... 264
Alice Jones (ali... 6
ELR User1 (ELR... 5
0
5.0k
10k
Top Host (Origin) Last 9h 5m
400
370
365
364
364
360
359
356
352
349
0
100
200
300
400
Top Host (Impacted) Last 9h 5m
webserver2...
ftpserver...
mailserver.a...
Top Application Last 9h 5m
IMAP - Internet Message Access Prot... 2.1k
End Point Mapper 2.0k
Microsoft Directory Services 2.0k
LDAP - Lightweight Directory Access... 2.0k
UPS - Uninterruptible Power Supply 2.0k
PPTP - Point-to-Point Tunneling Prot... 2.0k
DNS - Domain Name System 2.0k
Finger 1.2k
POP3 - Post Office Protocol Version 3 1.2k
NNTP - Network News Transfer Prot... 1.2k
0
1.0k
2.0k
Top Log Source Type Last 9h 5m
Syslog - LogRhythm Syslog Gene... 80k
API - Okta Event 1.6k
MS Windows Event Logging - Sec... 1.0k
LogRhythm File Monitor (Windo... 295
LogRhythm CloudAI 264
API - AWS CloudTrail 144
LogRhythm AI Engine 119
MS Windows Event Logging - Sys... 34
MS Windows Event Logging XML ... 24
MS Windows Event Logging - App... 14
0
20k
40k
60k
80k
Top Country (Origin) Last 9h 5m
Netherlands
Canada
Brazil
France
South ...
Germ...
Japan
United Kin...
China
United S...
Top Country (Impacted) Last 9h 5m
Hong Kong
Germany
Netherlands
France
Singapo...
Ireland
Austr...
Unit...
Thailand
United K...
Top Entity (Impacted) Last 9h 5m
815
652
489
326
163
0
03 AM
06 AM
09 AM
Global Entity
Primary Site
EchoTestEntity
LOGS
TASKS

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.


Primary Palo Alto
HA1 and HA2 – Connected
Priority - 90

Secondary Palo Alto
HA1 and HA2 – Connected
Priority - 120

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

Automated Patch Management

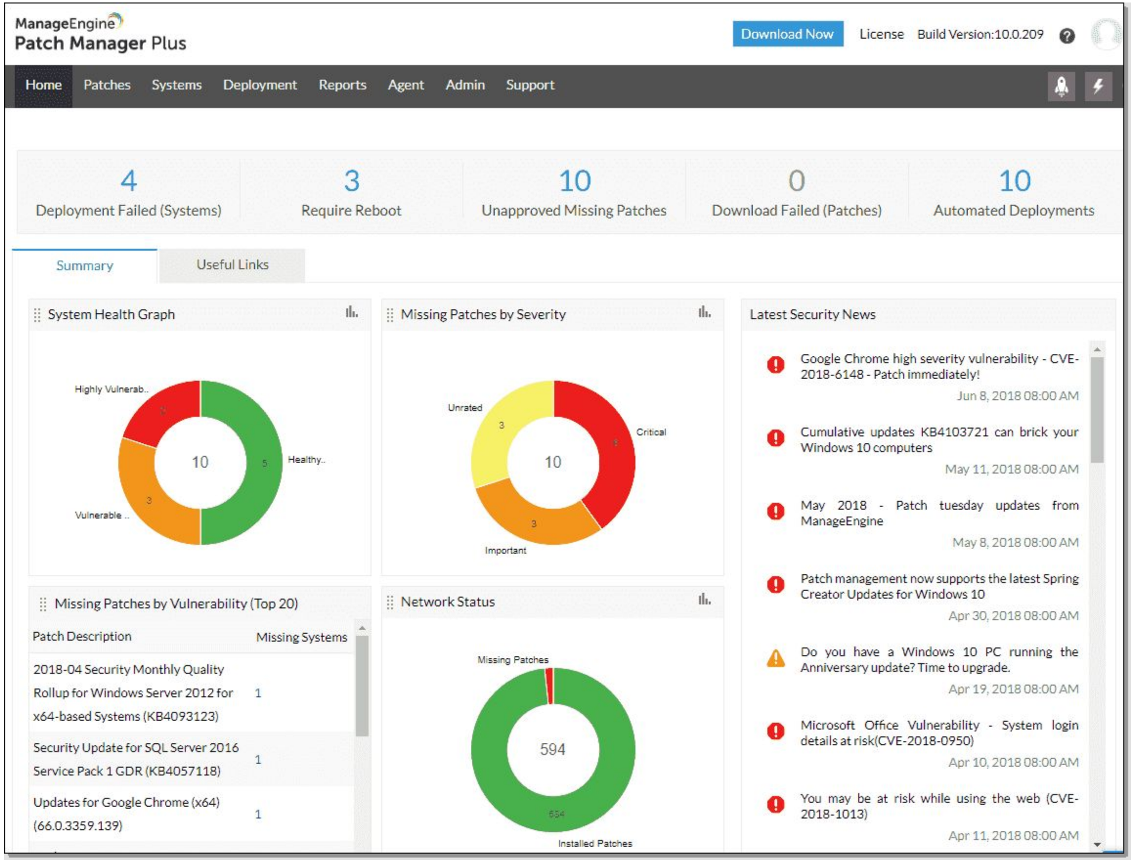
Patch manager plus pro (**£2k per year**)

Windows updates at appropriate times

- Adds control

Keeps software up to date but maintains compatibility

Includes third party (java, flash etc)



4 Deployment Failed (Systems)

3 Require Reboot

10 Unapproved Missing Patches

0 Download Failed (Patches)

10 Automated Deployments

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

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

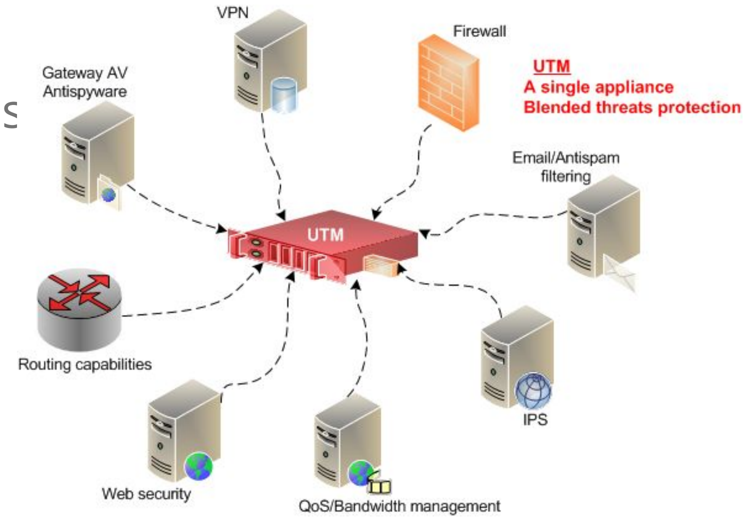
Endpoint protection, NG firewalls & full disk encryption

Safend data protection suite (DPS) endpoint protection

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

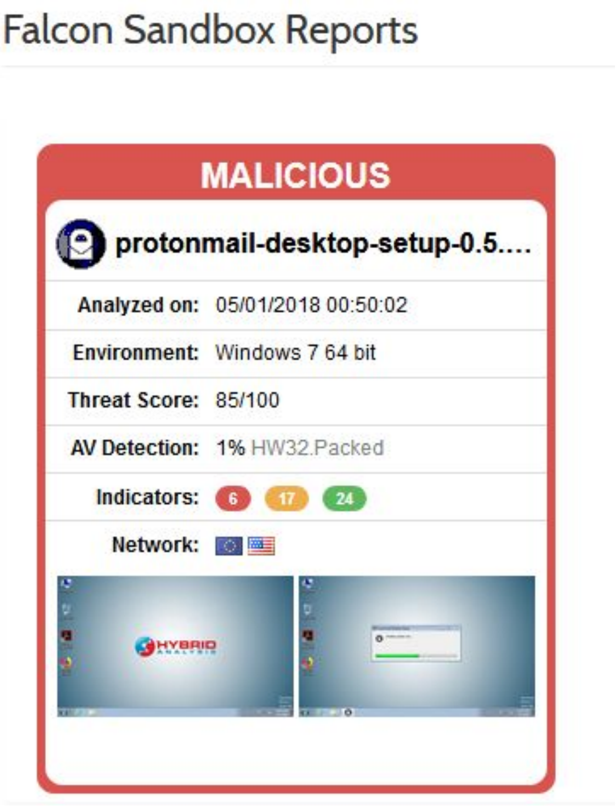
UTM firewall (next-generation NG firewall, inspects packets in flight) ...simple ones just blocks a port.

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



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

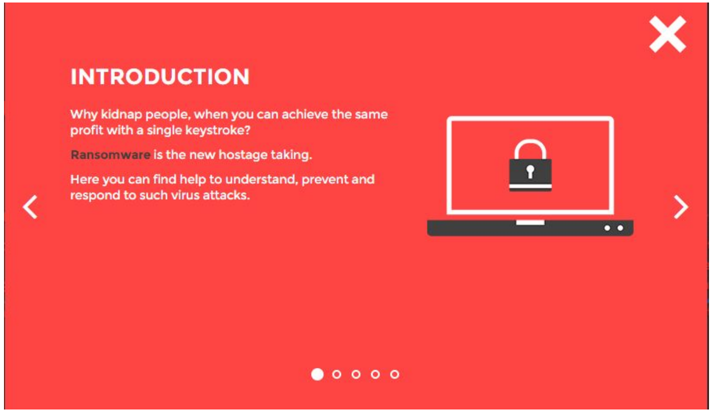
(balancing confidentiality - e.g. do we want to send personal details to third party?)

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)

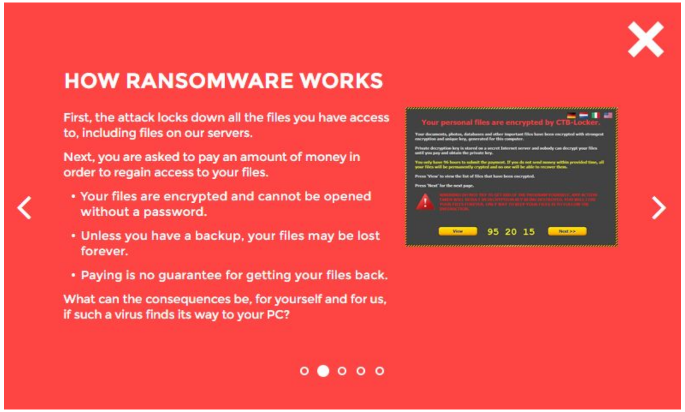


INTRODUCTION

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.



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?

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

[illegible]