Digital Vision
for Cyber Security

CloudHopper

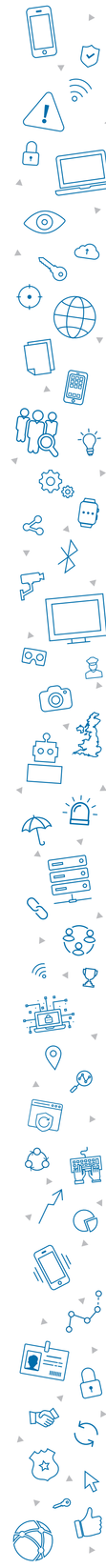
When did it start?	Summer 2016
What?	Cyber-espionage (stole personal details; exfiltrated data)
By whom?	A group called APT10 – possibly state-sponsored
Motivation?	Seize trade/business assets and secrets; Compromise confidential data
Targeted at?	Critical national infrastructures and public services via their Managed Service Providers (MSPs)
The cost?	While the extent of the exploitation of these vulnerabilities is unknown, it necessitated a significant amount of remedial work across the public sector and its Managed Service Providers to add additional measures to reduce potential future impact
What's the exploit?	Microsoft Office vulnerabilities
Who was impacted?	UK, US, Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa, India, Thailand, South Korea, Australia
How did it get in?	Spear-phishing
How did it spread?	Harvested system administrators' details
How was it halted?	Major exercises by MSPs to plug vulnerabilities
What did we learn?	Importance of proactive threat intelligence

WannaCry

When did it start?	12 May 2017
What?	Ransom attack (money demanded for return of seized data)
By whom?	Unclear
Motivation?	Unclear: political, financial, anarchical, or even a mistake
Targeted at?	Microsoft environment – specific target a mystery
The cost?	Potentially hundreds of £millions in operational losses
What's the exploit?	Weaponised an exploit called Eternal Blue, originally developed by (and stolen from) the US National Security Agency (NSA)
Who was impacted?	Over 200,000 machines in 150 countries (four most infected countries: Taiwan, India, Ukraine and Russia). Collateral damage to organisations including NHS, Renault France, Nissan UK, Telefonica Spain, Portugal Telecom, MegaFon Russia
How did it get in?	Phishing attack
How did it spread?	Worm spread infection networks
How was it halted?	'Kill switch' discovered by 'MalwareTech', a security researcher
What did we learn?	Vulnerability of critical services with legacy equipment

NotPetya

When did it start?	27 June 2017
What?	Premeditated destructive attack (demanded ransoms – rendered machines unbootable - even if victims paid the ransom, the 'key' to retrieve data did not exist – paying the ransom was pointless)
By whom?	Unclear
Motivation?	Unclear
Targeted at?	Ukraine
The cost?	Hundreds of £millions; One company alone reported £100 million lost revenue
What's the exploit?	Again, used Eternal Blue
Who was impacted?	Companies in Ukraine and global companies with subsidiaries there; collateral damage: a UK ad agency, an Indian container port, a global law firm
How did it get in?	Phishing attacks or compromised source code in financial software used in Ukraine
How did it spread?	Multiple spreading techniques
How was it halted?	Antivirus software; indicators of compromise identified and addressed; security patches
What did we learn?	Even after WannaCry, some businesses were still unprotected



8 key lessons the world learned

1

An attack can come **anywhere anytime**, and can spread wherever it can – not just to specific targets.

2

Always keep endpoints **patched** (even after WannaCry attack, some businesses still failed to patch systems).

3

Always run supported **operating systems** and **applications** (many businesses still use unsupported versions of Windows XP and Server 2003 to run the business-critical operations).

4

Establish and test **Security Incident Response** procedures to react to an attack.

5

Ensure employees are properly **informed and trained** to spot suspicious activity.

6

Use **Threat Intelligence and Behavioural Analysis**: using Antivirus software alone is not enough.

7

Implement and test a **backup strategy** to support businesses-critical assets and operational data after a ransomware attack.

8

Establish appropriate **business continuity and disaster recovery** plans and rehearse them regularly to make sure they are fit for purpose.