dimension data

accelerate your ambition

2017 Global Threat Intelligence Report

Cybersecurity insights for *protecting your digital business*

Validated threat data gathered

from NTT Security, NTT operating companies, and research sources:

3.5 trillion logs analysed

6.2 billion attacks

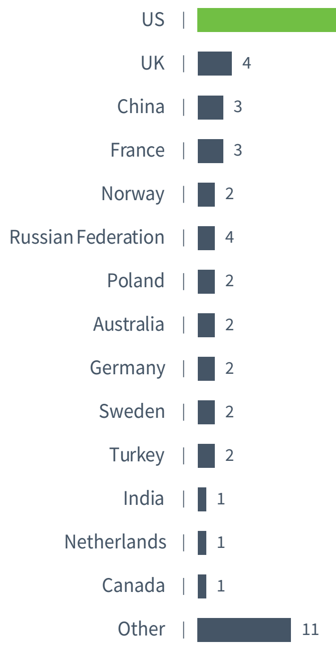
global honeypots and sandboxes in *over 100* different countries

10,000 NTT clients worldwide

10 security operations centres (SOCs)

Attack analysis

Sources of attack

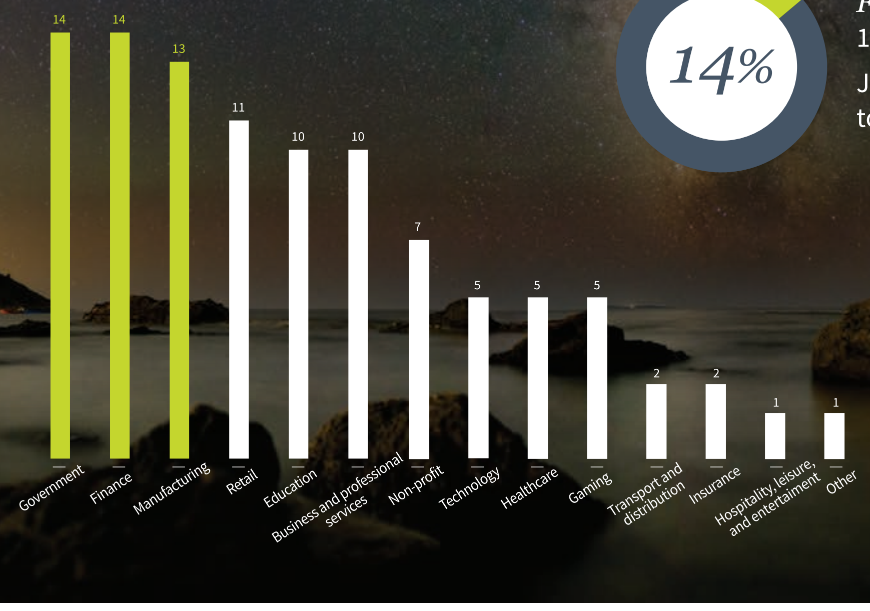


63% of attacks detected originated from IP addresses in the US

US has been the major source of hostile activity since 2013

– Threat actors often use *public cloud* to orchestrate attacks due to the low cost and stability of this infrastructure in the US

Attacks *by sector*



14%

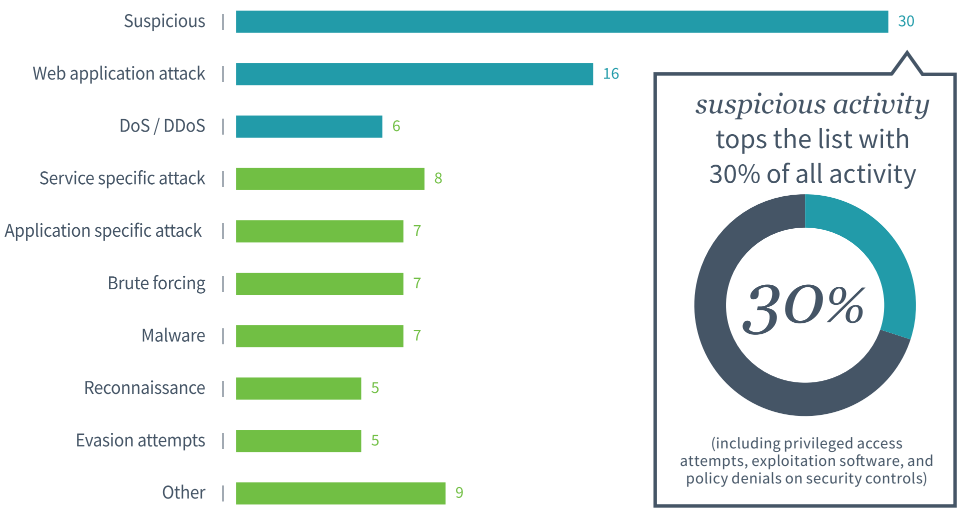
Finance returns to the top of the list with 14% of all detected attacks

Joined by *government* which appears at the top for the first time

- 2016 was marked by considerable global geo-political events which likely led to the spike

Attacks on *manufacturing sector* up from 7% to 13%

Attacks *by type*



suspicious activity tops the list with 30% of all activity

30%

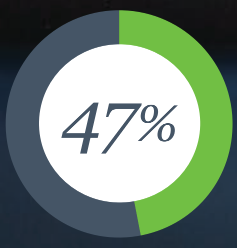
(including privileged access attempts, exploitation software, and policy denials on security controls)

web application attacks up from *15%* *16%*

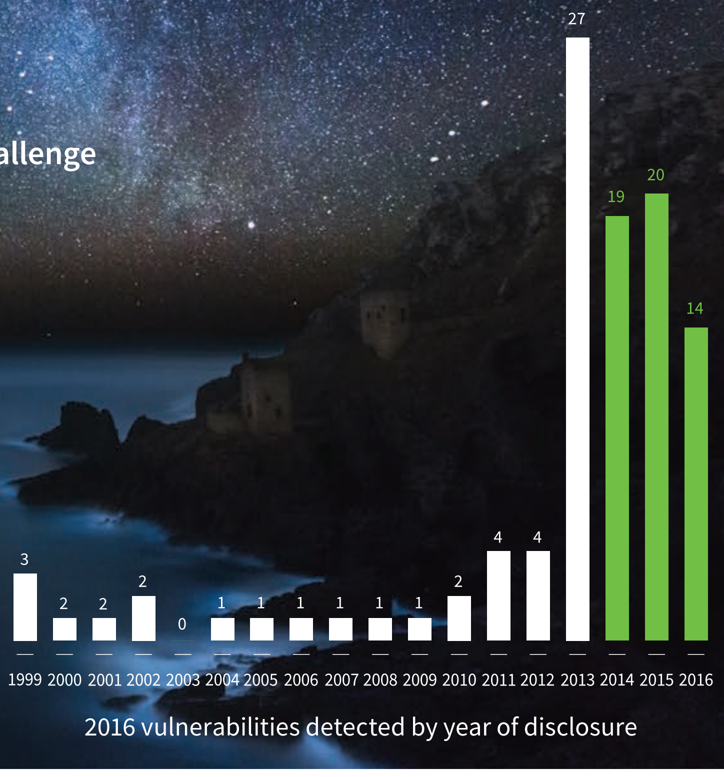
DoS/DDoS up from *3%* *6%*

Vulnerability **analysis**

Effective patch management remains a challenge



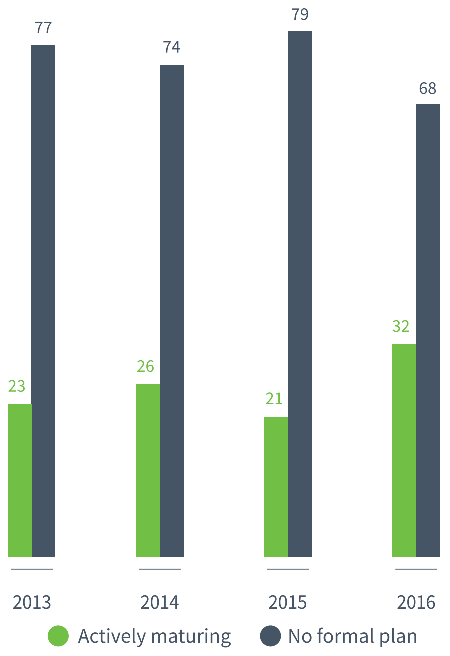
nearly 47% of vulnerabilities *are more than three years old*

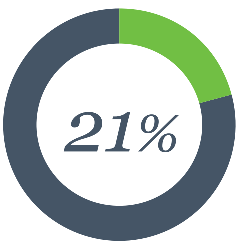


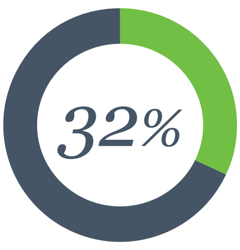
2016 vulnerabilities detected by year of disclosure

Incident *response*

Improved awareness signals a shift towards prioritising incident response

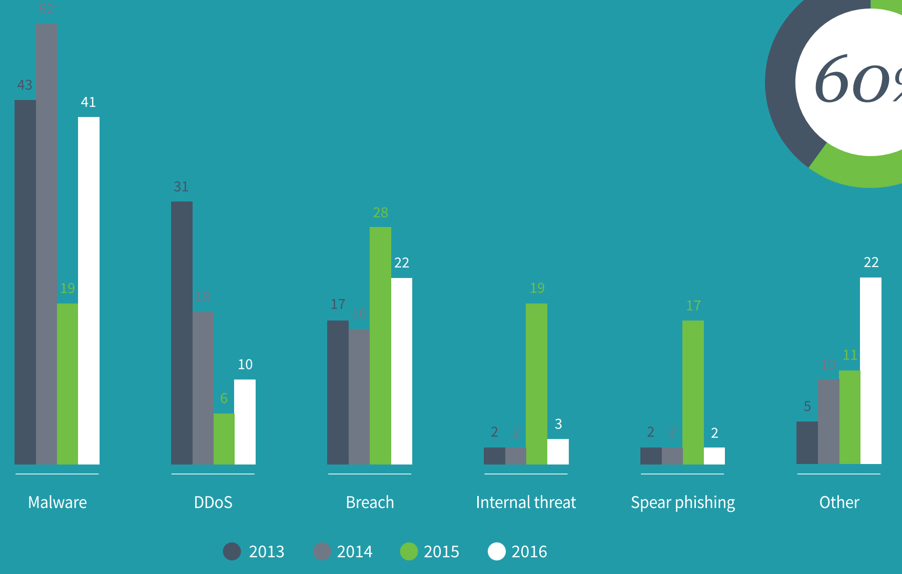






32% of organisations have a formal incident response *up from 21%*

Top cybersecurity threats **for digital businesses**



Phishing, social engineering, and ransomware

Phishing attacks topped the list at *60% of all incident response investigations*

Incident response engagements relating to malware up from 19% to 41%*:

- *ransomware* was the most common at 22% of all engagements

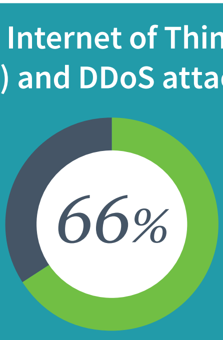
*includes ransomware, bot droppers, and payloads

Business email compromise (BEC) attacks

target a particular person within an organisation, and are typically much more financially damaging

BEC attacks are the second most common form of phishing

The Internet of Things (IoT) and DDoS attacks



66% of IoT attacks were *attempting to discover specific IoT devices* such as a particular model of video camera

Attacks targeting end users

Exploit kits target vulnerable software that's widely used on desktop and laptop computers

- *Nearly 30% of the attacks analysed targeted end-user products* such as Adobe Flash Player, Adobe Reader, Java, JavaScript, Microsoft Internet Explorer, and Microsoft Silverlight

Join the conversation

@DimensionData

Dimension Data

www.dimensiondata.com/globalthreatreport