INcontext International: INfographics
Issue 56: 18 May 2017

CYBERSPACE:

THE 5TH BATTLEGROUND*

*The 4 traditional domains of war = land, sea, air and space

TOP 5 CYBER THREATS

REPORTED BY GOVERNMENTS

59% **MALWARE**
Software used to damage, disrupt or gain access to computer systems
Includes: computer viruses, worms, 'trojan horses', ransomware, spyware, adware, scareware, and other malicious programmes

57% **PHISHING**
Acquiring sensitive information from a computer (passwords, bank account details, usernames) by pretending to be a trustworthy entity

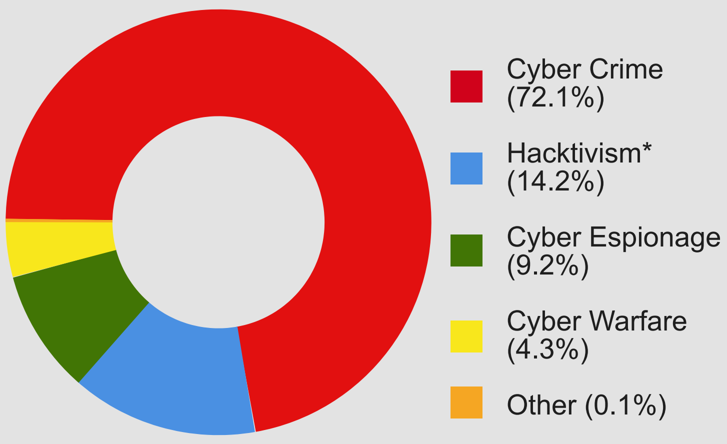
44% **DATA LEAKAGE**
Sensitive data falling into the hands of third persons either by mistake or on purpose

43% **HACKING**
Gaining unauthorised access to a computer system

42% **SPAM**
Electronic messages sent to a bulk of users aimed at advertising, phishing, or spreading malware

* Data from US-CERT, 2013 (http://www.debatingeurope.eu)

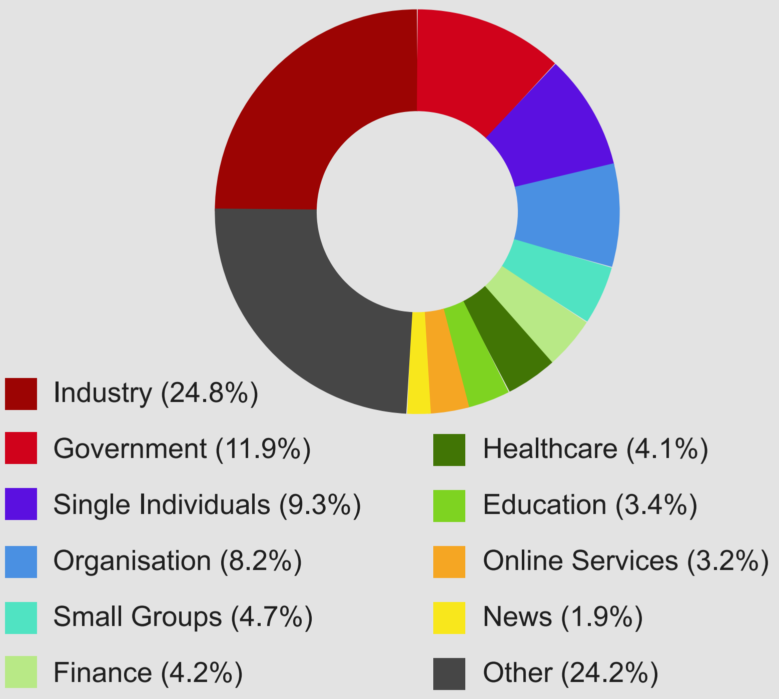
Motivations Behind Attacks: 2016



* gaining unauthorised access to computer systems and carrying out various disruptive actions to achieve political or social goals. E.g. altering or defacing a government website

Source: www.hackmageddon.com

Top 10 Distribution of Targets: 2016



CYBER CRIME VS CYBER WARFARE

CYBER WEAPONS: malware agents employed for military, paramilitary, or intelligence objectives

CYBER CRIME

use of cyber weapons/tools to execute a criminal act driven by any number of reasons (usually profit/greed)

E.g. WannaCry (most recent attack)

- Ransomware infected 300,000 computers in more than 150 countries
- Ransoms of $300 to $600 to restore access
- Only about $ 50,000 paid (very low return)
- Unprecedented global impact

Targets: payment card details, authentication credentials, copyrighted material, medical records, classified information, bank account details, personal information, system information, sensitive organisational data, trade secrets

Average cost to a small-medium business from a cyber-attack $188,242

CYBER WARFARE

use of cyber weapons to destroy enemy capabilities and/or populations (sabotaging infrastructure, disrupting critical systems, or inflicting physical damage on an enemy)

E.g. Stuxnet (2010)

- Responsible for causing damage to Iran's nuclear programme
- Believed to be a jointly-built US-Israeli cyberweapon
- No organisation or state has officially admitted responsibility

Targets: Usually very specific, but Stuxnet escaped confines of Iranian facility, infecting computers in at least 9 other countries

May have destroyed up to 1,000 Iranian centrifuges (10 percent)

It is possible to have state-sponsored hostilities or acts of aggression that don't cross the line to become an "act of war"