PROFiT

Prevention of Fraud in Travel

# THE COUNTER FRAUD CAMPAIGN 2019

## PART 16: KNOW YOUR ENEMIES

Prevention of Fraud in Travel (PROFiT) and the Fraud Intelligence Network (FIN) are working with the City of London Police to reduce fraud in the travel industry. PART 16 is a look at the various malicious people and groups that might compromise your business payment and IT infrastructure.

PROFiT is the only official travel industry counter fraud body. We work on your behalf to carry out analysis and research, disseminate best practice and disrupt crime.

**Find out how you can join the fight against crime. Contact via:** contactus@profit.uk.com

**If your website is subjected to cybercrime** including using one of the methods outlined in this email campaign, then report it to **ACTION FRAUD**.
USE THE ONLINE REPORTING TOOL: https://reporting.actionfraud.police.uk/login
OR CALL ACTION FRAUD: 0300 123 2040 **(**helpline 24/7 for live attacks 8am till 8pm for others**)**

## BACKGROUND

1.0 Since 1969 there has been a succession of films[1] and high-profile court cases which have given a general impression that most cyber-attacks are carried out by lone (often teenage) geeks operating from their bedrooms and are rare events. In fact, DCMS stated that around one third of UK businesses and a fifth of charities reported having cyber-attacks or breaches during the 12 months up until September 2019[2].

1.1 The films and reports make it seem that these lone hackers know some clever tricks enabling them to hack even the most secure systems. Some well-known UK cases are:

- **Mathew Bevan** & **Richard Price** (1996) https://toptensofall.wordpress.com/mathew-bevan-born-june-10-1974/
- **Gary McKinnon** (2016) https://www.theguardian.com/world/gary-mckinnon
- **Jack Chappell** (2017) https://www.cps.gov.uk/west-midlands/news/hacker-sentenced-cyber-attacks-high-profile-companies
- **Alex Bessell** (2018) https://www.bbc.co.uk/news/uk-england-42733638
- **Laurie Love** (2018) https://www.theguardian.com/law/2018/feb/05/hacking-suspect-lauri-love-wins-appeal-against-extradition-to-us
- **Zain Qaiser** (2019) https://www.theguardian.com/uk-news/2019/apr/09/uk-hacker-jailed-six-years-blackmailing-pornography-website-users

1.2 Whilst the types of hacker portrayed in the films do exist, they are not the predominant threat to businesses because they often, but not exclusively, target Government agencies and other high-profile victims. In the following sections we look at some of the other organisations and individuals that might be a cyber threat to your business. These actors are operating alongside your business 24/7 so you need to take steps to ensure you are at less risk of becoming a target.

### PEOPLE AND ORGANISATION THAT COMPROMISE YOUR DATA

HACKTIVISTS

2.0 If anyone finds a way around your security to access your systems, they are endangering your whole operation. A hacktivist is someone who uses hacking to bring about political and social

[1] https://cybersecurityventures.com/movies-about-cybersecurity-and-hacking/

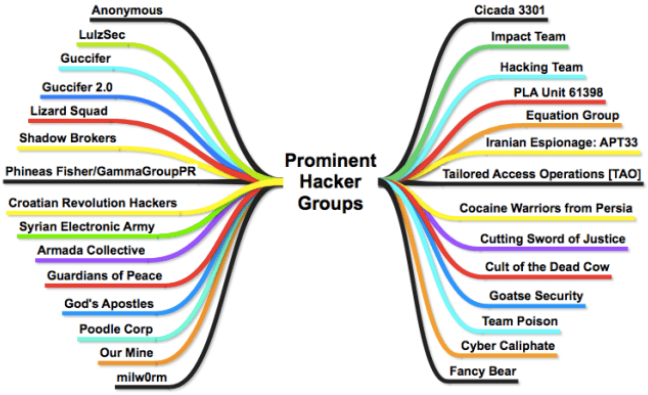
[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

change. The term “hacktivist” can be traced back to 1994, originating from the hacker group “Cult of the Dead Cow”. Hacktivists are becoming less effective as organisations have become aware of the risks and taken steps to harden themselves. This has been further driven by GDPR.

2.1 Whilst some hacktivists may mean well, several of these groups have been linked directly to the espionage services of foreign powers (see below) such as ‘Cosy Bear’ and ‘Crazy Bear’ which are believed to be linked to the Russian intelligence agencies the GRU and FSB. You may not think that your organisation is vulnerable to being attacked by hacktivists but some of these groups aim to undermine the economic fabric of the West whilst some groups are linked to anarchists, and others linked to issues such as the environment and climate change, privacy and free speech.

2.2 A hacking attack is a breach of your security and a crime. Once someone has successfully found out how to access a system, even if they do not make their presence known in any-way, they increase your vulnerability as the method of exploitation used can quickly become known to the wider criminal fraternity and make you a target.

| Some of the better-known hacktivist groups | | |
|---|---|---|
| ● The 414s | ● Infonomicon | ● RedHack |
| ● AnonCoders | ● IPhone Dev Team | ● Rocket Kitten |
| ● Anontune | ● Iranian Cyber Army | ● Securax |
| ● Anonymous (group) | ● Islamic State Hacking Division | ● The Shadow Brokers |
| ● Antisec Movement | ● Israeli Elite Force | ● Shaltai Boltai |
| ● *Backtrace Security* | ● L0pht | ● Shmoo Group |
| ● Chaos Computer Club | ● Lazarus Group | ● Syrian Electronic Army |
| ● Cozy Bear | ● Legion of Doom (hacking) | ● Tailored Access Operations |
| ● Croatian Revolution Hackers | ● Level Seven (hacking group) | ● Tapandegan |
| ● Cult of the Dead Cow | ● Lizard Squad | ● Team Elite |
| ● CyberBerkut | ● Lords of Dharmaraja | ● TeaMp0isoN |
| ● Chinese cyberwarfare | ● LulzSec | ● TeslaTeam |
| ● The Dark Overlord (hackers) | ● LulzRaft | ● TESO (Austrian hacker group) |
| ● Dark0de | ● Legion of Doom (hacking) | ● The Unknowns |
| ● Decocidio | ● Level Seven (hacking group) | ● Threat actor |
| ● Derp (hacker group) | ● MalSec | ● Titan Rain |
| ● Digital DawgPound | ● Masters of Deception | ● TOG (hackerspace) |
| ● Fancy Bear | ● Mazafaka (hacker group) | ● Turla (malware) |
| ● G0v | ● Milw0rm | ● UGNazi |
| ● Gay Nigger Association of America | ● Moonlight Maze | ● UXu |
| ● Genocide2600 | ● Network Crack Program Hacker Group | ● W00w00 |
| ● Ghost Security | ● NSA Playset | ● World of Hell |
| ● Ghost Squad Hackers | ● NSO Group | ● Xbox Underground |
| ● Global kOS | ● NullCrew | ● XDedic |
| ● GlobalHell | ● Operation High Roller | ● Yemen Cyber Army |
| ● Goatse Security | ● Operation Sundevil | ● MalSec |
| ● HacDC | ● OurMine | ● RedHack |
| ● Hack Canada | ● P.H.I.R.M. | ● Rocket Kitten |
| ● HackBB | ● Pakbugs | ● Securax |
| ● Hacker Dojo | ● Pangu Team | ● The Shadow Brokers |
| ● HackerspaceSG | ● Phone Losers of America | ● Shaltai Boltai |
| ● Hacktivismo | ● Plover-NET | ● Shmoo Group |
| ● Hackweiser | ● Port7Alliance | ● Syrian Electronic Army |
| ● Harford Hackerspace | ● Power Racing Series | ● Tailored Access Operations |
| ● Helith | ● Pumping Station: One | ● Tapandegan |
| ● *Hell (forum)* | ● Red Apollo | ● Team Elite |
| ● Honker Union | ● Iranian Cyber Army | ● TeaMp0isoN |
| ● Vladislav Horohorin | ● Islamic State Hacking Division | ● TeslaTeam |
| ● HubCityLabs | ● Israeli Elite Force | ● |
| ● *Impact Team* | ● L0pht | ● |



CRIMINALS

3.0 The group of people that you are most likely to be compromised by are criminals either acting alone or as part of an organised group. The most frequently encountered cybercriminals act to divert funds into their own hands, steal data for extortion, to use in their own crimes, or to sell on to others.

3.1 According to IT Governance, a body that monitors publicised breaches, by the end of September there had been 10,331,579,614 breached records.[3] From the travel industry viewpoint notable examples of compromised data in 2019 includes (these are hyperlinks):

- Teletext Holidays left audio files of customer purchases unprotected online (212,000)
- Phone numbers linked to Facebook users found online (419,000,000)
- Air New Zealand warns Airpoints members after employee falls for phishing email (100,000)
- British Airways e-ticketing flaw exposes passenger's personal data (unknown)
- Hackers compromise guest record database at Choice Hotel (700,000)
- Airbnb customers say their accounts have been hacked (unknown)
- History repeats itself as Facebook third-party apps expose users' personal data (540 million)
- Software company Citrix says hackers accessed its internal network (unknown)
- Airline e-ticket system vulnerabilities could compromise personal data (unknown)
- Hacker puts up for sale third round of hacked databases on the Dark Web (93 million)
- 620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts (620 million)
- Over 140 International Airlines Affected by Major Security Breach (unknown)
- Singapore Airlines experiences security breach, personal information of more than 280 KrisFlyer members disclosed (280 million)
- Nearly 5 million passengers' data leaked from online train ticketing platforms (5 million)

3.2 When organised crime hacks travel companies it is as a source of funds, to facilitate people smuggling, a source of identities and to make travel arrangements. Lone criminals will use the funds obtained from cyber-crime to commit extortion, auctioning-off data to criminals, or money diverted into their accounts, to pay off debts, or fund lifestyle, addiction, or debt.

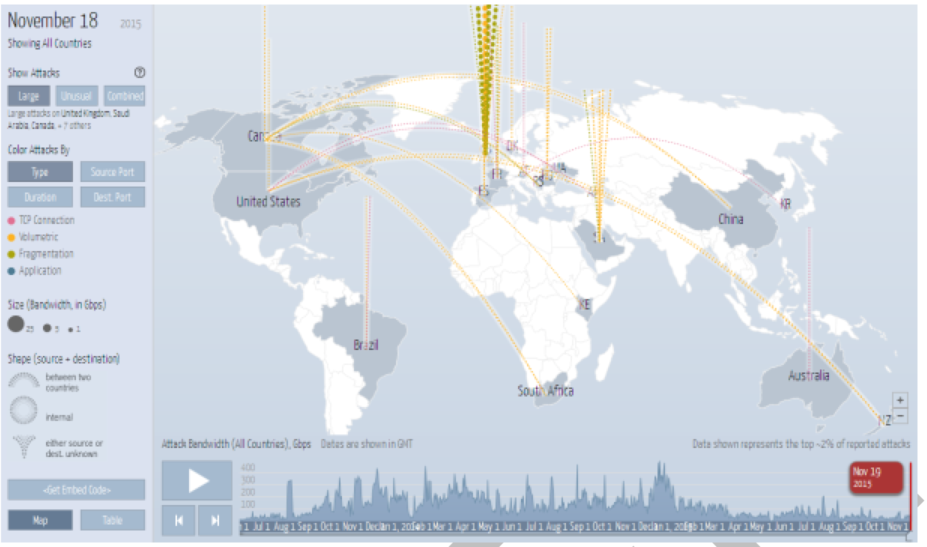
TERRORIST GROUPS

4.0 Generally traditional terrorists, despite their intentions to damage western interests, are less developed in their computer network capabilities and propensity to pursue cyber means than other types of adversaries. They are likely, therefore, to pose only a limited cyber threat. Since bombs still work better than bytes, terrorists are likely to stay focused on traditional attack methods in the near term.

4.1 Their goal is to spread terror throughout the civilian population. Their sub-goals include attacks to cause casualties and attacks to weaken the economy to detract from the Global War on Terror.

[3] https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-september-2019-531-million-records-leaked

During 2015, one week after the UK Government warned of the possibility of a cyber terror attack the UK came under a major DDOS attack believed to eminate from ISIS[4]. The attack map below shows the scale of the attack:



4.2 During the same year SenseCy alleged that ISIS also attacked Centcom, the Mount View Telegraph website, the Twitter Account of the Albuquerque Journal, the IB Times website, Newsweek's Twitter account, TV5 Monde's network, and Twitter.[5] It is unlikely that travel companies will be the specific target of a cyber terror attack, but companies could become victims of an attack where weaknesses in software are being exploited and the company has not kept its software suite up-to-date. The problem is recognised at an international level and is the subject of a United Nations report[6].

FOREIGN POWERS

4.0 Several countries have significant cyber-attack capability and whilst most of this is aimed at the infrastructure of other states, financial and business infrastructure is also often targeted as a way of destabilising the economic infrastructure of the target:

**Russia** has a robust cybercrime black market, valued at approximately US$2 billion per year, and hosts as many as 30 highly capable cybercrime groups. Russia is also known for state-sponsored hacking predominantly through the FSB and GRU.

**China** is the originator of approximately 30 percent of all cyber-attacks worldwide. The country has been accused of perpetrating state-sponsored attacks against foreign governments and businesses. China has one of the largest military groups of cyber experts in the world. The Peoples Liberation Army has a dedicated unit based in Shanghai called PLA Unit 61398 which is said to be involved in industrial espionage amongst other things.

**North Korea** has generated an estimated $2 billion for its weapons of mass destruction programs using "widespread and increasingly sophisticated" cyberattacks to steal from banks and cryptocurrency exchanges, according to a confidential U.N. report.

**Iran**: U.S. officials rank Iran as one of the country's four top cyber adversaries alongside Russia, China and North Korea.

**Eastern Europe**: At least 30 groups operate in this region, notably in **Ukraine**, **Belarus** and **Poland**. Cybercrime groups are commonly linked to organised crime groups and their methods include distributed denial of service attacks, as well as the deployment of malware, botnets and ransomware.

[4] https://www.telecomstechnews.com/news/2015/nov/18/uk-pummelled-ddos-after-isis-cyber-attack-warning/

[5] https://blog.sensecy.com/2015/12/23/2015-activity-timeline-allegedly-isis-affiliated-cyber-attacks/

[6] https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

**Romania** is home to several cybercrime organisations that are suspected of targeting electronic payment systems. Two such attacks led to losses of US$8 million (in an attack targeting individuals) and US$240 million (in an attack on financial institutions).

**Brazil** has several cybercrime groups that conduct attacks both within the country and internationally. Brazilian cybercrime groups have adapted tools and techniques from Eastern European hacker groups and often use highly complex Russian-made software in their attacks.

**Nigeria** continues to be one of the primary origins of scam and phishing emails. However, in addition to these scams, groups of young, disenchanted, unemployed and relatively tech-savvy individuals spend significant amounts of time establishing online fraud schemes.

**Vietnam**: Network-intrusion attacks originating from Vietnam has increased significantly. Such attacks are used to steal information which can be sold or used for financial gain. This included the theft of approximately 200 million personal records from the US and Europe.

**Indonesia**: The number of cyber-attacks being launched from Indonesia has increased considerably, with approximately 38 percent of all incidents worldwide being launched from Indonesia. The country also has one of the highest rates of botnet activity in South East Asia.

**South Korea**: The country has recorded high levels of cybercrime and hacking. This was partly due to the comparatively outdated technology used for online banking in South Korea. Cyber criminals have also launched international attacks, mainly targeting the US.

**United States**: A high number of cyber-attacks originate from the US and are perpetrated both by criminals and governmental organisations. These are aimed at various countries.

## SOCIAL MEDIA ORGANISATIONS

6.0 Social media platforms operate in the most intrusive and all-encompassing manner. Any organisation that allows staff to access social media at work or does business through social media should be aware that all aspects of their business will be captured and may be used without their knowledge or consent. However, what many are unaware of is that social media platforms also capture information on the business's IT infrastructure.

6.1 If you study the Privacy Polices of the popular social media products, they inform you that they collect and use all sorts of information about your activity. As an example, with Facebook this includes:

- All communications and other information that you and your customers provide.
- When you create an account.
- When you create or share content and message or communicate with others.
- Information on your people, pages, accounts, hashtags/tweets etc., and products.
- Information that you upload, sync or import.
- Information on your usage.
- Information about transactions made on their products including collecting the whole payment card number, authentication information, and billing data.

6.2 Facebook also collects following information from and about the computers, phones, connected TVs and other web-connected devices you use to access their services and they combine this information across different devices that you use. The specific data they gather on each device is as follows:

- The operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- The operations and behaviours performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements.
- The unique identifiers, device IDs and other identifiers, such as from games, apps or accounts that you use, and Family Device IDs.
- Bluetooth signals, information about nearby Wi-Fi access points, beacons and mobile phone masts.
- The name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are

nearby or on your network.

- Data from cookies stored on your device, including cookie IDs and settings.

6.3 The vast store of information that these platforms gather and then keep about your business and customer's activity and IT infrastructure is much more than required to carry out their stated aims of service provision, personalisation, and improvement of their products. When you trade on social media you are allowing these organisations to get behind your security infrastructure and access every aspect of your company.

6.4 You are also trusting social media companies and their employees to store this information safely and securely and not to misuse it in any way. It would be very difficult to prove that social media sites had been the source of a data loss or customers compromised cards. Remember; there is no way of anyone knowing whether your trust is misplaced or not.

Like what we do to protect you?

We are always short of funds and need your support.

Find out how you can join PROFiT and fight fraud by emailing contactus@profit.uk.com

**Next Week: Part 17 Spam & Malware**