Cyber threat actors

Paraskevas, A., 2022, Cyber Threat Actors, in Buhalis, D., (ed), Encyclopedia of Tourism Management and Marketing Edward Elgar Publishing, Cheltenham.

Cyber Threat Actors

Alexandros Paraskevas
Alexandros.Paraskevas@uwl.ac.uk

Keywords: cyberattack, cybercrime, cyberespionage, cybersecurity, dark net, data breach

Cyber threat actors (CTAs) are groups or individuals who take advantage of cyber security vulnerabilities in computer networks and low security awareness or negligence in organisations to gain unauthorized access to their information systems and steal or otherwise affect their data and devices. The travel and tourism sector's ongoing digital transformation over the past two decades with the dramatic increase of online transactions, the introduction of traveller / hotel guest analytics, cloud integration, travel apps and connected devices, and digital payment technologies has increased the exposure of organisations within the sector to cyber threat actors and their vulnerability to cyberattacks (Paraskevas, 2020). These cyberattacks are carried out by a wide range of CTAs. Although there are a few academic typologies of CTAs offering several types of actors alongside their potential targets, expertise, resources, organisation, and motivation (e.g., the Delft University of Technology typology - de Bruijne et al, 2017), cyberattacks fall broadly under four categories: geopolitically motivated warfare, ideologically motivated activism, financially motivated crime, and emotionally motivated sabotage. Consequently, CTAs can be classified in state-sponsored actors, activists, cybercriminals, and insiders.

Insert Fig 1 here

State-sponsored actors, also known as 'Nation-State APTs' (Advanced Persistent Threat groups), are financially and technologically supported by nation-states to advance their geopolitical agendas and interests. (Pahi and Skopik, 2018). It is highly unlikely for anyone to be able to attribute attacks back to a particular country with certainty whereas their success rate is almost entirely assured. Historically, state-sponsored actors have attacked from entire national infrastructures to individual targets, including tourism organisations. In 2015, a cyberattack to the Polish national air carrier (LOT) computer systems at Warsaw's Okecie Airport forced the airline to ground its entire fleet. The attack was one of the main reasons for the approval by the country's president Andrzej Duda of a very controversial law involving loosening citizen digital data protection rules for national security purposes. Duqu 2.0 malware, a variant of Stuxnet which in 2010 caused significant damages to the Iranian nuclear programme, has been found in the computer networks of hotels in Austria and Switzerland in 2015 that were sites of the Iranian nuclear negotiations in a breach openly attributed to Israeli Defence Forces' Unit 8200.

State-sponsored actors focus mostly on industrial espionage and steal intellectual property, sensitive personally identifiable information (PII), and money to fund other espionage and exploitation activities (Ablon, 2018). To achieve their objectives, they target government officials, military personnel, senior corporate executives, and research scientists when they travel to extract every possible information about them, and information contained in the devices they carry. Their modes of operation usually include spear phishing e-mails and the use of network vulnerabilities and exploits that their targets may not have identified or managed to patch. Once in the network, they usually move laterally into share servers and other systems and remain there undetected for months

to years, collecting the data they need. APT28 or 'Fancy Bear', a group with suspected links to the Russian military intelligence agency GRU employed spear phishing e-mails with malicious document attachments to hotels in at least seven European and one Middle Eastern country in 2017. They gained control of these hotels' computer systems and Wi-Fi networks and obtained several high-ranking government, military and business hotel guests' passwords which were later used to attack their organisations. The 'Dark Hotel' group made its targets in more than 100 luxury hotels in Asia, Europe, and the US download malware which appeared as a legitimate software update of Adobe Acrobat immediately after they connected exploited with the hotel the Wi-Fi. The group operated unnoticed for seven years (2007-2014) and gained access to sensitive government, military, and corporate information from thousands of guests. As it was later connected with the SONY Pictures attack in 2011 it is considered to be backed by the North Korean government.

Other groups, allegedly sponsored by the Chinese State Security launched in 2015 the 'Cloud Hopper' cyberattack which targeted Sabre, the largest hotel and travel distribution systems provider in the world. The attack was aiming at PII of 'high-interest' persons and would be used for identity theft, physical surveillance and possibly blackmail. The same state-sponsored actors are also suspected for the 2018 Marriott/Starwood data breach which exposed data of 500 million hotel guests, making this data breach the second largest in the history after the 2013 breach of Yahoo that affected three billion user accounts.

Activists (or **hacktivists)** are individuals or groups who conduct ideologically motivated hacking activities. They often act as online whistle-blowers by disseminating ('doxxing') sensitive or even classified information they obtained by hacking databases. Other hacking tactics they employ include domain name service (DNS) hijacking followed by website defacement, i.e., they change completely the website appearance by hacking its hosting infrastructure and replace the content with their message (Delmas, 2018). In 2015, the hacktivist group Lizard Squad hijacked the official website of Malaysia Airlines and replaced the landing page with an image of a tuxedo-wearing lizard and the message: "Hacked by LIZARD SQUAD - OFFICIAL CYBER CALIPHATE". The motives for the attack are unclear, but in some regions the message reportedly included the sentence "ISIS will prevail". The most common, however, hacktivist tactic is to render their targets' websites unreachable by overwhelming them with more traffic than they can handle causing them to crash (distributed denial-of-service or DDoS attack). Ghost Squad Hackers, an offshoot of the hacktivist group Anonymous, orchestrated a DDoS attack in 2016 on the Trump Hotel Collection website and forced it to go offline. They announced that they were targeting Trump's hatemongering against Muslims and Mexicans.

Organised crime groups and **'Black Hats'** conduct financially motivated cyberattacks. When they target travel and tourism networks it is not just for credit card records but for travellers' passport data, contact details, birth dates, travel plans, air miles, loyalty points and personal preferences. All these data can be monetised in underground black markets and the dark web in a multitude of ways, ranging from fraud to identity theft and extortion. Dream Market, one of the largest dark web markets, was listing several vendors selling reward points from over a dozen different airline reward programmes, including Emirates Skywards, SkyMiles, and Asia Miles. These points are mostly used to obtain upgrades in hotel stays but also to redeem points at local retailers through gift cards. Delta SkyMiles and British Airways miles are on the top of the reward points listings in the three most popular marketplaces in the dark web (Bischoff, 2018). Dark web 'travel agents' sell packages of flights, hotel bookings, car rentals and tours and activities at a significant discount of their actual retail value. They use stolen credit cards or reward points and air miles from hacked traveller

accounts to buy travel services which they can offer at a discount to others. PII is also monetised by these actors. In 2016, more than 47,000 Asiana Airlines passengers' scanned personal documents, including resident registration numbers, digital passport scans, home addresses, bank accounts, phone numbers and family relations records went up on auction in a Dark web marketplace.

Inadvertent and **malicious Insiders** are arguably the most dangerous CTA for an organisation. Inadvertent insiders are members of staff who do not respond to cybersecurity awareness training and are negligent and those who create vulnerabilities by mistake. In 2017, Verizon found that an average 4.2% targets in a phishing campaign will click the malicious link or attachment and that those with a history of falling prey to phishing have higher propensity to be phished again. While this percentage is small, the impact of their actions is huge. Ponemon Institute (2020) estimates that on average 63% of data breaches every year are caused by employee insecure practice. Misjudgements and isolated errors of employees who generally follow secure practices and comply with policy are also sources of data breaches. The poor configuration of a server at the Pyramid Hotel Group which manages over 90 hotels under different brand affiliations exposed a huge number of sensitive data from these properties that could be used by other CTAs to override the security protocols of all the networked with Pyramid brands and gain control of all their customers' data too. Malicious insiders are 'second streamers', i.e., employees seeking illicit additional income usually through data theft. They could also be disgruntled employees who may collude with external threat actors to facilitate data breaches or sabotage the organisation's IT systems but also act on their own. In data theft they usually exfiltrate data slowly to personal accounts to avoid detection and maximize their gains while the are still employed by the organisation or complete large data exports when they are about to resign. In 2009 Starwood claimed that two executives involved in the development of 'W Hotels' brand who moved to Hilton Hotels to develop the 'Denizen Hotel' brand stole more than 100,000 electronic files before and after they changed jobs. Tools for compliance, data protection and user behavioural analytics have been proven useful for organisations to proactively protect themselves against both inadvertent error and malicious intent.

References

Ablon, L. (2018), Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. The RAND Corporation [available online: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf, accessed 16 January 2021].

Bischoff, P. (2018), How much are stolen frequent flyer miles worth on the dark web? Comparitech [available online: https://www.comparitech.com/blog/information-security/how-much-are-stolen-frequent-flyer-miles-worth-on-the-dark-web/, accessed 14 January 2021].

de Bruijne, M., van Eeten, M., Gañán, C.H. and Pieters, W. (2017), Towards A New Cyber Threat Actor Typology, Delft University of Technology [available online: https://www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf, accessed 15 January 2021].

Delmas, C., (2018). Is Hacktivism the New Civil Disobedience? Raisons Politiques, Vol. 1, pp.63-81.

Paraskevas, A., 2022, Cyber Threat Actors, in Buhalis, D., (ed), Encyclopedia of Tourism Management and Marketing Edward Elgar Publishing, Cheltenham.

Pahi, T. and Skopik, F., (2018). A Systematic Study and Comparison of Attack Scenarios and Involved Threat Actors. In Skopik, F. (Ed), Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level, Boca Raton, FL, CRC Press, pp. 19-67.

Paraskevas, A. (2020). Cybersecurity in Travel and Tourism: A Risk-Based Approach, in Xiang, Z., Fuchs, M., Gretzel, U. and Höpken, W. (eds), Handbook of e-Tourism, Cham: Springer Nature Switzerland AG, ISBN 978-3-030-05324-6, DOI: https://doi.org/10.1007/978-3-030-05324-6

Ponemon Institute (2020), 2020 Cost of Insider Threats, report sponsored by IBM Security, [available online: https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/, accessed 16 January 2021].

Verizon (2017), 2017 Data Breach Investigations Report [available online: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/, accessed 16 January 2021].