Identifying Future Threats and Trends

PID_00270256

Thomas Holt

Recommended minimum time required: 2 hours

Universitat Oberta de Catalunya

Thomas Holt

The assignment and creation of this UOC Learning Resource have been coordinated by the lecturer: Marc Balcells Magrans (2019)

First edition: September 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Publishing: FUOC

Index

Introduction

The prior chapters have presented the scope of cybercrimes that can occur and that produce negative economic consequences for their victims, as well as profit for the offenders. These chapters also highlight the symbiotic relationship between technology and cybercrimes as a whole. As new technologies are produced, it is extremely difficult to know which of them will take hold and why. Numerous devices and applications have been espoused as the future trends in the use of technology, such as GoogleGlass, virtual reality products like Oculus and enhanced or augmented reality applications. Nevertheless, most of them failed to gain a substantial market share or maintain user interest.

Similarly, the patterns for application use are likely to change with time and users' interest. An excellent example of these dynamics lies with applications like Facebook, which has a large user population but is beginning to retract (Cannarella & Spechler, 2014; PiperJaffray, 2014). This has been suggested to be due to generational differences in the perceived value of the platform, with younger users moving to platforms like SnapChat and Instagram (Duggan et al., 2015). The increasingly diversified nature of online platforms has also segmented user populations by place and by use, with larger user populations for WhatsApp in certain parts of Europe, Asia and Latin America as compared to the larger world (Statista, 2019). Scandals associated with Facebook's management of passwords and user data, as well as misuse by organizations like Cambridge Analytica and nation-state manipulations, have led many to delete their accounts and user profiles completely (Guynn, 2018; Mahdawi, 2018). External changes to law, such as the General Data Protection Regulation by the EU, may also make it difficult for Facebook to continue to operate in the same fashion in certain nations (Constine, 2018).

As a consequence, it is difficult to fully assess the ways in which general technology use patterns may shift as a function of social or technological change. Since these conditions naturally shape the practices of offenders, it is a challenge to successfully predict how offenses may change. Instead, it is more plausible to assume that the motivations of offenders will remain constant and simply evolve incrementally and proportionally in line with the technologies available (e.g. Holt & Bossler, 2016; Mativat & Tremblay, 1997).

Against this backdrop, this chapter will discuss some prospective trends that may continue over the next five years based on current criminological research and trend analyses from several cybersecurity vendors. This chapter is meant

to be speculative, but based on existing knowledge of cybercrime offending and victimization. The ideas presented should be taken with caution and considered ideas rather than established concrete facts.

1. Likely Trends in Economic Cybercrimes

Consistent patterns of cybercriminal activity over time do exist, and they provide potential directions for future use. For instance, it is clear that hackers are interested in obtaining sensitive data and manipulating end users in order to access their devices. This will undoubtedly continue over the next five to ten years, though the targets of their efforts may evolve. As the proportional market for tablet computers and smartphones continues to grow, attackers will increase their focus on creating tools to compromise these devices.

Example of increase of vulnerability

In 2017, 842 separate vulnerabilities were identified that directly affected Android software, which was a substantial increase from the 525 vulnerabilities identified in 2016 (CVE Details, 2019). Similarly, 592 vulnerabilities were identified that directly affected iOS users in 2016, which is a reflection of the global popularity of iPhones, iPads and other Apple products (Cunningham, 2016).

Malware writers and attackers are already developing a range of tools to compromise mobile devices, as noted in Chapter 2. Attackers recognize that developing and releasing apps that contain malware through the iOS App store, Google Play and other markets will enable backdoor access to user data. The number of programmes appears to have increased over the last few years, and has become more sophisticated in the acquisition of details.

Example of apps with malware

The security firm Sophos noted that 22 different apps that were posing as games and utilities hosted on the Google Play market in June 2018 actually contained malicious code to direct users to fraudulent ads (Yu, 2018).

Attackers also appear drawn to the Android application market due to its less strict regulation and to the fact that users can download apps from third party platforms that can be used on the device (McAfee, 2016). Thus, it seems reasonable to expect attackers to continue to target mobile platforms so long as individuals use these devices for virtually all popular social and financial applications (McAfee, 2016; Sophos, 2018).

As individuals and industry increasingly depend on the use of cloud-based storage –where data, files and images can be uploaded to Internet-connected web servers and managed from there– these resources are more likely to be targeted by hackers and data thieves (Mulazzani, Schrittwieser, Leithner, Huber & Weippl, 2011). Both Google and Apple offer cloud-based storage for images and video taken by customers on their mobile devices, as a form of data backup. Corporations are also increasingly using services like Dropbox, Google Drive, Microsoft's OneDrive and other services as a means to remotely host files and encourage group projects across disparate physical environments (Hansen, 2017).

Though cloud servers may be secured from compromise, and possibly encrypted depending on the user, they are not immune to attack. A hacker need only utilize a phishing scheme to acquire a user's email and password to access the account, and then gain access to the account's sensitive information.

Hackers are also using cloud storage as a mechanism to facilitate attacks against several targets. For instance, the security company Netskope (2016) found that services like Dropbox could be used as a tool to host malware and infect end users. Individuals can create accounts and add infected files to a folder and then share it with others in an attempt to infect their systems. Such an attack may be more successful than it would if the hacker sent files through email, as spam filters have become extremely effective at filtering out or blocking e-mails with attachments that include executable programs (Netskope, 2016). Additionally, cloud storage could decrease the efficacy of antivirus software and that of strategies to mitigate active attacks.

Example of pishing

There have been several notable instances of cloud storage compromise through phishing, such as a major dump of nude photos and videos of many celebrities on August 31, 2014 (Drury, 2015). Hackers use phishing techniques to obtain the iCloud account usernames and passwords of major and minor celebrities who stored images taken from their iPhones (Drury, 2015). Even though the attackers did not steal any financial information, they posted sensitive and embarrassing content from hundreds of celebrities' devices all over the web.

Example of the reduction in antivirus efficacy

For instance, if an infected system uploads files to cloud storage servers used by the organization and is cleaned afterwards to remove the infection, it could be re-infected when accessing that backed up file. Thus, cloud storage will undoubtedly continue to grow as a platform for exploitation and attack by hackers to affect individuals and organizations across the world.

2. IoT Devices and Cybercrime

In addition to tablets and mobile phones, consumers are increasingly acquiring wearables and Internet-enabled devices that store sensitive information or serve critical functions in several life areas. This is evident in the burgeoning market for Bluetooth-enabled, Internet-connected devices that can be worn anywhere on the body to capture information about the wearer. In fact, one company estimates that there will be over 411 million wearable devices in the market by 2020, ranging from smart watches to medical devices (Lamkin, 2016). Many of these devices capture and track user data related to several health behaviors, including exercise, heart rate and sleeping patterns, and can be linked to user-entered information, such as eating habits and daily caloric intake. These applications are thought to be beneficial by gamifying exercise and healthy behaviors, and by improving individual knowledge of fitness and wellness issues.

Such information may seem trivial, as it is specific to an individual and is not necessarily linked to financial information such as credit card data. At the same time, some of these services have been linked to private health insurance plans and consumer data in order to help shape payments and deductibles (Olson, 2014). Specifically, health insurance providers have begun to offer reduced plan costs to employees who take steps to improve their general lifestyle through regular exercise and meal intakes (Olson, 2014). Additionally, many wearables like FitBit are managed by applications, which are only as secure as the username and password established by the account holder. A further issue with wearables is that they are relatively insecure devices. They do not feature password protection or antivirus software on the physical devices themselves, and since information flows between the wearable and other devices such as phones, this information may be captured quite easily (Maddox, 2015).

These issues create a major opportunity for data breaches that could lead to the loss of information related to health services, which could be used to perform fraudulent healthcare payments or to acquire services without authorization (Collins et al., 2011).

Fitbit

For instance, Fitbit user accounts were targeted by fraudsters in 2016 in order to fraudulently obtain replacement devices (Krebs, 2016a). Additionally, a data breach that affected the web hosting services for FitBit and other companies was thought to lead to the loss of usernames, passwords and user data (CBS, 2017). How the victims of the breach were harmed remains unclear, but this highlights the potential for hackers to target these devices.

In much the same way, there are now various companies and utility providers offering wireless Internet-connected thermostats, home security systems and electronic-based controls, as well as phone services and home management devices such as Amazon's Alexa and Facebook Portal. These devices allow consumers to easily and remotely manage all aspects of their home life, from front door surveillance via Ring to energy use via devices like Nest or to ordering food and supplies. Many of these devices are also application- or browser-based, which creates what is increasingly known as the Internet of Things: all non-computing devices that are connected via the Internet (Curtis, 2013).

The creation and increasingly common implementation of IoT devices ensures that consumer interactions with household devices are convenient, though it creates substantial potential for compromise.

Using an application-based home security device that is managed by phone essentially transforms the device into a set of keys that can be accessed and used from any location (Curtis, 2013). Depending on the security settings of the phone, it may be quite easy for anyone to obtain and control access to the building and its security. Similarly, usernames and passwords for the application management interface can be phished to allow remote management of all devices.

The simple configurations and poor security of these devices create immediate opportunities for attackers, as many are initially configured with simple passwords that can be identified through Google searches (Curtis, 2013). Hackers have been able to demonstrate how easily these devices can be compromised remotely, and even infected with malicious software in order to affect the user (Franceschi-Bicchierai, 2016).

Mirai

In 2016, IoT devices were targeted by attackers in order to create a stable botnet-like attack platform running through webcams and other dedicated devices (Krebs, 2016b). Since these devices have no antivirus software or related security tools, these infections went unnoticed by their owners and users. As a result, attackers were able to compromise the devices using a malware variant called Mirai, which was then used to engage in a massive DDoS attack in 2016 (Krebs, 2016b). This malware, called Mirai, targeted cybersecurity authors and service providers for websites like GitHub, Twitter, Netflix, AirBnB and many other major groups. The size of the botnet and the power leveraged by the IoT devices enabled attackers to knock portions of the East Coast of the US offline for several days (Newman, 2016).

The IoT includes home appliances and technologies, as well as durable goods and infrastructure such as Internet-connected and autonomous, or self-driving, vehicles (Dimitrakopoulos 2011; Lu et al. 2014). The production of the so-called CAVs (Connected and Autonomous Vehicles), whether cars or trucks, includes the existing functionality of modern vehicles and replaces their underlying systems with electric-mechanical hybrids, guided by webs of interlinked microchips and electronics. Additionally, the adaptation of wireless technology and the development of integrated communications and enter-

tainment systems that link to mobile devices have turned cars into repositories for huge amounts of data and have created new forms of user interfaces (Gerla, Lee, Pau & Lee 2014). In fact, the production of smart vehicles is an essential underpinning of connected autonomous vehicles that will depend on Internet connectivity to share real-time information with other vehicles and transport-related infrastructure, such as GPS resources and road service systems (Gerla et al. 2014).

The emergence of CAVs and the cyber-enabled systems to support vehicle functioning have opened doors to new threats that did not exist with the mechanical and closed-loop electrical connections that used to define automobile systems. Of great concern are threats emanating from cyberattacks by computer hackers on a vehicle's computerized systems, control functions and data repositories, which represent a clear and present danger to vehicles, their occupants and society (Greenberg 2015; 2016; 2017). Vehicle-related cybersecurity risks also threaten the intellectual property of vehicle manufacturers and their supplier partners, as well as consumers' privacy.

Example of vehicle-related cybersecurity

At present, a typical sedan is estimated to use between 50 and 70 independent computer modules or Electronic Control Units (ECUs), and to rely upon approximately 100 Megabytes of embedded binary code (Larson and Nilsson 2008).

The computerization of modern cars has brought forth major advances in vehicle system capabilities, as well as certain levels of control over vehicle operations and advanced user features designed to enrich the driving experience. Many of these features –such as adaptive cruise control, lane management systems, collision avoidance systems and parking assistance– also help to increase the levels of vehicle safety. These and other features require continual communication among the many interconnected onboard computer modules, as well as communication with external entities such as GPS systems and telematics providers (e.g., Onstar, HondaLink).

Some of these technologies were initially integrated into vehicles in the late 1990s and the early 2000s, though it was not possible to externally access them via Internet connectivity. Instead, an actor would have to gain physical access to the vehicle's internal systems through a hardware connection at the OBD-2 (On-Board Diagnostics) port. The growth of CAV technologies and the development of high-speed wireless Internet connectivity created opportunities for virtual access to the systems, which in turn enables attackers to attempt to shift the exploits and existing cybercrime techniques to vehicle platforms.

To date, no incidents of cyberattacks on vehicles that appear to have affected consumers have been documented (e.g., Upstream 2019). Instead, the current crop of attacks seem to be demonstrations or experiments to see if a potential compromise could be achieved in controlled settings, such as a lab or managed roads and tracks. However, attacks have been performed against wireless vehicle keyfobs that enable access to the vehicle via remote locking, starting and alarm controls. The signal between the keyfob and the vehicles can be captured in various ways, and then cloned by an attacker to ensure access. In fact, several theft incidents that involved using keyfob information have been documented in the US and UK in the first half of 2019 alone (Upstream,

2019). As a result, there is a need to carefully consider how vehicle-related technologies can be impacted by criminals and generally used for economic and property-based crimes.

3. Nation-State Cyberattacks and Economic Threats

In addition to the broader landscape of criminal threats, there is no doubt that nation-states will continue to engage in cyberattacks against government and industry targets.

The potential impact that a nation-state can have against its perceived rivals through cyberattacks is unparalleled. A nation can use hacking techniques not only to affect another country's operational and economic security, but also to diminish its citizens' perception of their government's ability to ensure the security of their information (see Andress & Winterfeld, 2013; Rid, 2013).

This was exemplified in a recent set of ransomware attacks that have been attributed to North Korean actors (Newman, 2017).

Wannacry

The incident actually originated in part from the US National Security Agency (NSA), where a number of previously unidentified vulnerabilities in common Microsoft software products were identified. The NSA did not release this information to Microsoft, and kept it secret in order to use the vulnerability to their own advantage for offensive attacks (Ablon & Bogart, 2017; Newman, 2017). The vulnerability was made public due to a hack of the NSA by a group who called themselves the ShadowBrokers and sold a cache of sensitive, secret information and hacking tools produced by the Agency (Newman, 2017).

Microsoft was able to release patches for the vulnerability, though many systems had not completely implemented the security updates. As a result, a large number of systems across the globe were vulnerable to attack. In May 2017, a form of ransomware began to circulate in Asian nations, infecting systems and encrypting user data while demanding $300-$600 payments in bitcoin (Newman, 2017). The tool quickly spread across the world, and it affected a total of 150 nations and over 200,000 individual systems (Bossert, 2017).

Wannacry was particularly effective in harming health services in England and Scotland, as well as manufacturers across Europe. As a result, Wannacry was estimated to have caused $4 billion losses in damages and system down time (Bossert, 2017). The ransomware was not well configured and created numerous errors, including the fact that some of the people who paid did not get their files decrypted. In addition, its errors enabled security researchers to find ways to mitigate the attacks, leading Wannacry to be negated within a few days of its initial appearance (Bossert, 2017).

The reason why North Korea would have launched this attack is not entirely clear, but money could be one immediate motivation, as the funds raised via Bitcoin would be difficult to trace, thus ensuring money could be available for clandestine and illegal activities (Bossert, 2017). In addition, the economic and operational harm caused to global computer systems would help demonstrate that North Korea, while being small, has the ability to hobble other nations. Thus, such an attack may have a general deterrent value and help increase the perceived strength of the nation (Andress & Winterfeld, 2013; Rid, 2013).

Nation-states are also increasingly developing the ability to target modern critical infrastructure in order to cause systemic economic and social harm via cyberattacks.

NotPetya

For instance, a series of ransomware attacks was observed in June 2017 against several western countries, with a particularly large impact on computers and systems in Ukraine. In fact, over 80% of the infections observed were found in Ukraine, suggesting that this nation may have been specifically targeted (Greenberg, 2018). The malware, called NotPetya, seemed to target power companies, transportation systems, and smart systems that supported the electrical grid (Greenberg, 2018). It also had an impact on a range of industry and home user systems, causing a massive shutdown of critical infrastructure and systems.

The malware used a similar structure to that of a known ransomware tool called Petya, but differed from its code in major ways. First, the program used the same Microsoft vulnerability identified and used in the Wannacry attacks, which was not present in Petya (Greenberg, 2018). Second, the program displayed a ransomware message like Petya, but did not actually decrypt systems once a ransom was paid. NotPetya did not only encrypt the hard drive of the device it infected, but also damaged parts of the software to render it unusable (Greenberg, 2018). As a result, researchers began to call it NotPetya because of the similarities and differences between the two. Third, the NotPetya malware was autonomous in nature, similar to a worm (see Chapter 2). Lastly, security firms noted that initial infections were spread through the use of a software programme called MeDoc, used by Ukrainians to pay their taxes (Greenberg, 2018). This targeted attack method reinforced the idea that this malware was different from Petya, as the creators apparently sought to directly harm Ukrainian targets.

The scope of the damages caused by NotPetya should not be underestimated, as it seriously damaged any computerized system it infected, and spread across networks in seconds. Substantial disturbances were caused to hospitals, shipping and logistics providers, financial institutions, governments and industrial control systems in Ukraine and other nations (Greenberg, 2018). In fact, some estimates place the global economic losses associated with NotPetya at over $10 billion. This is by far one of the most extreme examples of nation-state attacks, and most attribute its use to Russia, which has been in a protracted cold and hot conflict with Ukraine over the last few years. Some speculate that the goal of causing such extreme damages was to send a message to other nations, implying that what happened in Ukraine could happen anywhere (Greenberg, 2018). Additionally, some suggest that the catastrophic damage caused to systems may have been intentional so as to delete evidence of other Russian hacking activities and hinder any further attribution to this nation. Finally, there is little reason to believe that an individual or a group of individuals acted on their own, as no financial profit was obtained by using the the ransomware (Greenberg, 2018). Thus, this may be the most serious example of nation-state sponsored hacking to date, and demonstrates the terrible potential economic toll of such attacks.

4. The challenge to policy-makers globally

This chapter has explored some patterns of crime and criminality that we may expect in the near future, which may be a function of technology and prior patterns of cybercrime in general. How policy makers and industry sectors may respond in order to proactively or reactively deal with these threats in the near future remains unclear. Governments around the world have created new agencies and organizational features within their current departmental structures to investigate and deter attacks (Andress & Winterfeld, 2013).

UK example

For instance, over the last decade the UK has repeatedly revised and restructured the number of agencies within their police structure to take complaints and investigate cybercrime and online fraud (Holt, Bossler, & Burruss, 2019).

However, the governmental response to cybercrime is only as useful as industry efforts to produce secure software and tools to be used in the market (Holt & Bossler, 2016; Rid, 2013). As noted in the nation-state examples above, products by major software vendors have vulnerabilities that can be exploited by attackers. Depending on the market share of a product, these threats could cause unparalleled harm for businesses and consumers alike, through no fault of their own. This is particularly evident in the number of vulnerabilities that have been identified in major Internet protocols and tools used to secure online communications and personal data over the last decade.

Drown

For instance, researchers identified a novel attack method in 2016. They called it DROWN, or Decrypting RSA with Obsolete and Weakened eNcryption (Higgins, 2016). The attackers were able to compromise an older application in the OpenSSL (Secure Socket Layer) library used in Internet communications to encrypt sensitive data as they are transferred between systems (Higgins, 2016). Attackers were thus able to break the encryption system used and obtain the content of communications between web browsers, email servers and VPN sessions. Given the kind of information that may be secured through SSL, such as financial information, this is a serious threat to individual privacy and confidentiality. Whereas a patch was made available for this vulnerability, it should be noted that more than one third of all servers using OpenSSL could have been compromised.

This example, and the Microsoft vulnerability mentioned in the nation-state attacks above, demonstrate that the security of the Internet is highly dependent on the practices of industry and software developers. No system can guarantee to be completely hack-proof, but software producers can take more efforts to cautiously identify vulnerabilities and software/hardware flaws at all points in a product's lifecycle (Rid, 2013). The more care a producer takes in order to minimize the likelihood of their products being hacked (not only before they reach the market, but also after they are sold), the less likely are these products to be effectively hacked by individuals in the wild. Such efforts are thought to be too costly for developers and would slow their ability to release products on the market.

To increase the likelihood of products being made more secure by design and remaining secure over time, industry bodies have emerged to encourage the consistent use of cybersecurity protocols that improve overall security for a variety of devices. Many of these groups operate as non-profit organizations with direct ties to industrial and government bodies.

US example

For instance, the ISA Security Compliance Institute (ISCI) in the US has developed multiple compliance specifications related to securing critical infrastructure and Internet-enabled devices used in electrical and water grid management (Andress & Winterfeld, 2013). They also operate a certification program for hardware and software used in the field to ensure it is secured to industrial standards (Andress & Winterfeld, 2013). Similar entities exist to promote system security standards and compliance for industrial sectors ranging from defense contractors to the automotive industry across the world. As a result, they provide a means to establish basic security guidelines, encourage compliance and identify regulatory and policy strategies that can be implemented when industry standards fall short.

In addition, industrial sectors are becoming more heavily involved in the investigation and management of various forms of cybercrime. Many Internet Service Providers, software developers and computer security firms have access to sensitive information about ongoing active threats and may be able to observe attacks in real time (Wall, 2007). Some firms, such as Crowdsrike, are actively hired to investigate and remediate active attacks, which gives them insight into sensitive networks maintained by high-profile government and industry targets (Leopold, 2017). Many of their investigations stem from attacks originating from nation-states like Russia and China, and they frequently publish information on their results so as to inform the broader field of cybersecurity. Corporations such as Microsoft and Google have also established several working groups with law enforcement and industry partners to investigate and take down different cybercrime groups (Adhikari, 2013).

Finally, industry associations like the Financial Coalition Against Child Pornography (FCACP), which includes ISPs, financial institutions, and non-governmental non-police agencies such as the International Center for Missing and Exploited Children work together to disrupt wrongdoing (International Center for Missing and Exploited Children, 2017). For instance, the FCACP was created in 2006 to reduce the use of legitimate financial payment providers in sending and receiving payments related to the production and distribution of child sexual exploitation content by offenders (National Center for Missing and Exploited Children, 2017). By banding together as an industry, payment service providers were able to identify behavioral markers for illegal payments and block specific customers and transactions from completion (International Centre for Missing and Exploited Children, 2017).

Summary

Taken as a whole, the transformative nature of technology use has dramatically impacted the world and how we as humans live and interact within it. The manifest benefits of technology have, however, created new opportunities for deviance and crime that impact individuals, organizations and governments. As a consequence, we must now carefully consider how our acceptance of, and willingness to use technologies may simplify the process of crime, or create new paths for offenders to gain access to sensitive data. Otherwise, we run the risk of enabling crimes and increasing our personal risk of victimization for the foreseeable future.

Bibliography

Ablon, L.; Bogart, A. (2017). *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and their Exploits* [online]. Santa Monica, CA: RAND. <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf>

Adhikari, R. (2013, December 9). «Microsoft's ZeroAccess Botnet Takedown No "Mission Accomplished"» [online]. *TechNewsWorld*. <http://www.technewsworld.com/story/79586.html>

Andress, J.; Winterfeld, S. (2013). *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners* (2nd ed.). Waltham, MA: Syngress.

Bossert, T. P. (2017, December 19). «It's Official: North Korea Is Behind WannaCry». The Wall Street Journal.

Cannarella, J.; Spechler, J. A. (2014). «Epidemiological modeling of online social network dynamics».

CBS (2017, February 24). «Major data breach exposed Uber, Fitbit, & OKCupid Info» [online]. *CBS Boston*. <https://boston.cbslocal.com/2017/02/24/cloudflare-bug-uber-fitbit-okcupid-passwords-breach/>

Collins, J. D.; Sainato, V. A.; Khey, D. N. (2011). «Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors». *International Journal of Cyber Criminology* (vol. 5, nº 1).

Constine, J. (2018, April 17). «A flaw-by-flaw guide to Facebook's new GDPR privacy changes» [online]. *TechCrunch*. <https://techcrunch.com/2018/04/17/facebook-gdpr-changes/>

Cunningham, A. (2016, August 25). «Apple releases iOS 9.3.5 to fix 3 zero-day vulnerabilities» [online]. *Ars Technica*. <https://arstechnica.com/apple/2016/08/apple-releases-ios-9-3-5-with-an-important-security-update/>

Curtis, S. (2013, August 2). «Home invasion 2.0: How criminals could hack your house» [online]. *The Telegraph*. <www.telegraph.co.uk/technology/internet-security/10218824/Home-invasion-2.0-how-criminals-co uld-hack-your-house.html>

CVE. «Common Vulnerabilities and Exposures» [online]. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5786>

Dimitrakopoulos, G. (2011, August). «Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges». En: ITS Telecommunications (ITST). *2011 11th International Conference on* (pp. 145-151). IEEE.

Drury, F. (2015, June 10). «FBI investigation into leaked naked celebrity photos focuses on man who "lives alone with parents" as they say many more famous people may have been hacked» [online]. *Daily Mail*. <https://www.dailymail.co.uk/news/article-3118070/FBI-investigation-leaked-naked-celeb-photos-focuses-man-lives-parents.html>

Duggan, M.; Ellison, N. B.; Lampke, C.; Lenhart, A.; Madden, M. (2015). «Demographics of key social networking platforms» [online]. *Pew Charitable Trust*. <https://www.pewinternet.org/2015/01/09/demographics-of-key-social-networking-platforms-2/>

Franceschi-Bicchierai, L. (2016, October 3). «The Internet of Things sucks so bad even "amateurish" malware is enough» [online]. *Vice Motherboard*. <https://www.vice.com/en_us/article/jpgb7y/internet-of-things-malware-mirai-ddos>

Gerla, M.; Lee, E.-K.; Giovanni, P.; Lee, U. (2014, March). «Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds». *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 241-246). Seoul: IEEE.

Greenberg, A. (2015, July 21). «Hackers remotely kill a jeep on the highway with me in it» [online]. *Wired*. <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

Greenberg, A. (2016, September 27). «Tesla responds to Chinese hack with a major security upgrade» [online]. *Wired*. <https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/>

Greenberg, A. (2017, August 16). «A deep flaw in your car lets hackers shut down safety features» [online]. *Wired*. <https://www.wired.com/story/car-hack-shut-down-safety-features/>

Greenberg, A. (2018, August 22). «The untold story of Notpetya, the most devastating cyberattack in history» [online]. *Wired*. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

Guynn, J. (2018, April 11). «After Facebook hearings, users want to know: Who is protecting my data?» [online]. *USA Today*. <https://www.usatoday.com/story/tech/2018/04/11/after-facebooks-mark-zuckerberg-hearings-users-want-know-who-protecting-my-data/505791002/>

Hansen, T. (2017, July 21). «Drobpox named a leader in 2016 Garnter Magic Quadrant for EFSS» [online]. *Dropbox Business Blog*. <https://blogs.dropbox.com/business/2016/07/gartner-enterprise-file-sync-and-share-efss/>

Higgins, K. J. (2016, March 1). «SSL "DROWNs" in yet another serious security flaw» [online]. *Dark Reading*. <http://www.darkreading.com/attacks-breaches/ssl-drowns-in-yet-another-serious-security-flaw/d/d-id/1324521>

Holt, T. J.; Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge.

Holt, T. J.; Burruss, G. W.; Bossler, A. M. (2019). «An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents» [online]. *Policing and Society*. doi: 10439463.2018.1450409

International Center for Missing and Exploited Children (2017). «Commercial childpornography: A brief snapshot of the Financial Coalition Against Child Pornography» [online]. <https://www.icmec.org/wp-content/uploads/2016/09/FCACPTrends.pdf>