SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Effects of botnets – a human-organisational approach

Zsolt Bederna[1], Tamás Szádeczky[2]

[1]bederna.zsolt@stud.uni-obuda.hu

https://orcid.org/0000-0003-0444-7275

Obuda University, Bécsi út 96/B, 1034 Budapest, Hungary

[2]szadeczky@mail.muni.cz

https://orcid.org/0000-0001-7191-4924

Masaryk University, Žerotínovo nám, 617/9, 601 77 Brno, Czech Republic

Abstract

Botnets, the remotely controlled networks of computers with malicious aims, have significantly affected the international order from Ukraine to the United States in recent years. Disruptive software, such as malware, ransomware, and disruptive services, provided by those botnets has many specific effects and properties. Therefore, it is paramount to improve the defences against them. To tackle botnets more or less successfully, one should analyse their code, communication, kill chain, and similar technical properties. However, according to the Business Model for Information Security, besides technological attributes, there is also a human and organisational aspect to their capabilities and behaviour. This paper aims to identify the aspects of different attacks and present an analysis framework to identify botnets' technological and human attributes. After researching the literature and evaluating our previous findings in this research project, we formed a unified framework for the human-organisational classification of botnets. We tested the defined framework on five botnet attacks, presenting them as case studies. The chosen botnets were ElectrumDoSMiner, Emotet, Gamover Zeus, Mirai, and VPNFilter. The focus of the comparison was motivation, the applied business model, willingness to cooperate, capabilities, and the attack source. For defending entities, reaching the target state of defending capabilities is impossible with a one-time development due to cyberspace's dynamic behaviour and botnets. Therefore, one has to develop cyberdefence and conduct threat intelligence on botnets using such methodology as that presented in this paper. This framework comprises people and technological attributes according to the BMIS model, providing the defender with a standard way of classification.

Keywords:

capabilities, botnet, cyberattack

Article info
Received: 7 April 2021
Revised: 1 June 2021
Accepted: 6 June 2021
Available online:1 July 2021
DOI: http://doi.org/10.35467/sdq/138588

Introduction

In cybersecurity, several actors operate with their own objectives, preferences, tools, and tactics. Since the actors behave according to their strategies and payoffs for actions, one can regard them as players who play a big game in cyberspace limited byresource constraints. There may well be some collaborators and some enemies of an actor in more layers, as a player may be a person or a group of people (Chukwudi, 2017, p. 45), to defend or attack a specific system. To achievetheir objectives, attackers and defenders apply some or even several tools to carry out their activities; and one of the most preferred tools of the attackers are botnets.

In fact, because "many areas of cybersecurity are also interconnected with national security" (Dobák, 2021), the essential services defined in the NIS Directive (European Union, 2016; *Directive (EU) 2016/1148 of the European Parliament and of the Council, 2016*) are frequently the targets of botnet attacks. Previous research (Bederna, Rajnai and Szadeczky, 2021) showed that criminals often use botnets against such services. Operators of digital infrastructure, financial and banking sectors were the victims of distributed denial of Services (DDoS), for example, by Mirai botnet's operation. Furthermore, criminals targeted the health, transport, and financial and banking sectors with ransomware attacks that halted operations for hours or even days. Not to mention that Governmental services also suffered from such an attack. However, criminals targeted them with the aim of espionage.

Although "most of the cyber-attacks against information systems, services or national information critical infrastructure originates fromdifferent networks […] made from infected end-points or network devices" (Bederna and Szadeczky, 2019, p. 45), botnets are "only" tools in attackers' hands, but quite complex ones. So, due to their functionalities and the types of attacks, ENISA (European Union Agency for Network and Information Security (ENISA), n.d.) has categorised botnets as the most dangerous threats. As Figure 1 shows, these 'tools' have been with us since the first Internet worm was created in 1988 with limited C&C capabilities, although thehistory of botnets started in 1999 with the Sub7 trojan and the Pretty Park worm. Since that time, botnets have evolved in the applied topologies and protocols, and threat actors have added important capabilities.

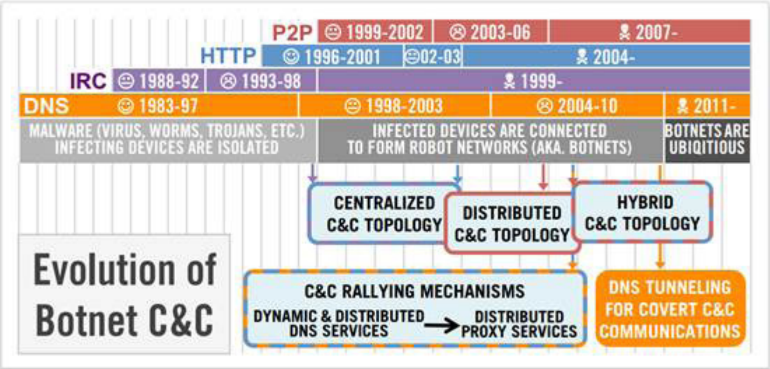
P2P ☺ 1999-2002 ☹ 2003-06 ☠ 2007-
HTTP ☺ 1996-2001 ☺02-03 ☠ 2004-
IRC ☺ 1988-92 ☹ 1993-98 ☠ 1999-
DNS ☺ 1983-97 ☺ 1998-2003 ☹ 2004-10 ☠ 2011-
MALWARE (VIRUS, WORMS, TROJANS, ETC.) INFECTING DEVICES ARE ISOLATED
INFECTED DEVICES ARE CONNECTED TO FORM ROBOT NETWORKS (AKA. BOTNETS)
BOTNETS ARE UBIQITIOUS
CENTRALIZED C&C TOPOLOGY
DISTRIBUTED C&C TOPOLOGY
HYBRID C&C TOPOLOGY
Evolution of Botnet C&C
C&C RALLYING MECHANISMS
DYNAMIC & DISTRIBUTED DNS SERVICES
DISTRIBUTED PROXY SERVICES
DNS TUNNELING FOR COVERT C&C COMMUNICATIONS

Figure 1. Evolution of botnets. Source: Cantón (n.d.).

From the defending perspective, the applied topology, protocols, and technical capabilities and attributes are inevitably important. However, if one wants to understand botnets' ecosystems, he or she should view botnets holistically, analysing technical and non-technical attributes. This paper aims to identify some essential technical and non-technical attributes that create a basic ontological model to facilitate such analyses, applying the information security perspective Business Model for Information Security (BMIS) model of ISACA (von Roessing, 2010). According to the BMIS, each organisation (attackers and defenders) comprises three essential (static) elements as (1) people, (2) process, and

(3) technology, distinguishing among entities' components the people, relevant processes, and tools and technology analysing the attackers in security games.In this context, botnets and their applicationshave various attributes. The paper first identifies the threat parameters of attackers and the possible technical effects of botnets on attacked entities to reach this target. Finally, in the case studies section, analysis of the five chosen botnets applies the pre-defined framework before the summary and the conclusion.

Threat parameters of botnets

All the technological elements of botnets serve the botmasters' will and behave according to their will. The whole or part of a botnet behaves according to its botmaster's (or botherder's) commands materialisingthe playing strategy. Regarding the BMIS model, thecommand and control (C&C) servers and the connected bots comprise the technology factor; and the botmaster,which is a person or a group of persons, is the human (people) factor.Therefore, there are various limitations in the operation of botnets. These boundaries include the various types of personal, organisational, or technical attributes, which are thebotmaster's motivation, the applied business model, willingness to cooperate, and human and technical capabilities. These parameters are discussed in the next subsections.

Motivation

With the application of botnets as tools, botmasters aim tocommit different types ofcybercrimes. Halder and Jaishankar (2012) describe cybercrimes as the "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet (networks including chat rooms, e-mails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".

Based on the definition, one can distinguish criminals' objectives according to the attacker's effectuate will.As information is becomingmore and more advantageous for individuals, businesses, and states, an attacker frequently aims to steal, leak, or destruct information processed by the targeted systems, or aims to disrupt operation due to anger, avenge, or for political reasons.

In effect, the motivation integrates the source of motives such as biological, social, and psychological needs, wants, or desires and the probable effects of any given action (Ryan and Deci, 2000). However, organisations or researchers may apply different categorisations. For example, Verizon (2020) distinguishes financial, espionage, and FIG (Fun, Ideology, and Grudges), despite the fact that one conducts espionage by political or even economic motivation.Therefore, applying espionage as motivation is not accurate, not to mention that espionage is a tool or action to get confidential data of the targeted entity. On the other hand, Gandhi *et al.* (2011), applied a methodology comprising political, socio-cultural, and economicmotivation as high-level factors; yet, the socio-cultural factor's elements they applied can belong to the FIG or political motivation.Accordingly, we apply the high-level categorisation for thebotmasters' motivation as (1) financial, (2) political, or (3) fun, ideology, and grudges (FIG).

Applied business models

It is beyond question that cybercrimes have evolvedoverthe last decade. Furthermore, today, there are highly sophisticated cybercrimes available as businesses. Cybercrime as a

Service is a business model forcybercriminals offering services, infrastructure, and knowledge to be rented (Manky, 2013), which incorporates (1) the Crimeware as a Service, (2) the Cybercrime Infrastructure as a Service, and (3) the Hacking as a Service.

In Crimeware as a Service, cybercriminals offer general or specifically targeted identified vulnerabilities and related exploits. For example, to this category, zero-day vulnerabilities, malware such as rootkits, ransomware belong, as well as droppers, keyloggers, and hiding tools (Szőr, 2005). However, they are the main building blocks for creating a botnet. Criminals offer infrastructural elements, specifically clients and servers under the aegis of the Cybercrime Infrastructure as a Service, making others ableto rent a botnet or typically a part of a botnet with a limited set of capabilities. Clients, as part of a botnet, are ready to process the renter's commands.Already in 2006, the Zeus botnet was the first that could-be rented quickly in Darknet. It arose with spyware capabilities, and overthe years, with version updates, some new features have been added to the original capabilities (Bederna and Szadeczky, 2019, p. 10). Hence, when planning a botnet, the botmaster can compare the income from renting with life-cycle costs such as acquiring malware, spreading, and maintenance (Putman, Abhishta and Nieuwenhuis, 2018, pp. 443–444).

Using Hacking as a Service solution, an attacker can outsource the complete attacking process to the "service provider" including planning and performing on-demand.

Cooperation willingness

Today's complex and comprehensive relations induce interactions between entities in any situation represented in a strategic form that describes players' action (Do *et al.*, 2017). In a security game, a player follows his or her strategy, which is the plan of actions-withthe payoff (Liang and Xiao, 2013). According to the noncooperative versus cooperative game-theoretic approaches, a critical aspect of a game is the players' cooperation behaviour. A noncooperative player chooses a strategy to optimise his or her interests. Contrarily, a cooperative player has a joint strategy for mutually achieving benefits with other players (Do *et al.*, 2017). However, the cooperation willingness can materialise in several layers in the technology and people factors of the BMIS model.

Creating and operating a botnet can be an easy and lonelytask if one is using pre-defined elements offered via Crimeware as a Service (Putman, Abhishta and Nieuwenhuis, 2018, p. 445). However, developing a comprehensive botfrom the beginning requires several actors to be involved, such as vulnerability analysts, exploit developers, bot collectors, bot maintainers, operators, remote personnel, developers, testers, sysadmins, and managers (Miller, 2010). So, individuals as players of the security games can commit a crime separately or in a groupthat hasthe same motivation. Furthermore, different threat actors may also cooperate. For example, in June 2016, "the US Democratic National Committee (DNC) announced that it had suffered a network compromise. Evidence proved two separate breaches, one carried outby APT28 and the other by another Russian group, APT29 (aka Cozy Bear)" (Bederna and Szadeczky, 2019). There is no information on whether the two groups cooperated or not, but in effect, at least, they did not work against each other.

However, in the technology factor, C&C servers may communicate and cooperate with bots belonging to another botnet. Collaboration (Chang *et al.*, 2015, pp. 648–649) may exist inter-family and intra-family botnet.On the other hand, noncooperative attacking players may take over the command centre's control (Cimpanu, 2019) or hijack or remove other botnets' agents (IBM Corporation, 2016, p. 11).

Capabilities

Capabilities incorporate the tools, tactics, and procedures (TTP) in the attacker's portfolio, which has changed tremendously over time, generally and in connection with botnets.In 1999, the Pretty Park contained only a limited number of competencies. It connected to a remote IRC server and reported basic system information as an operating system's version, login names, and e-mail addresses (Banday, Qadri and Shah, 2009, p. 2). Eight years later, when the Zeus botnet started its career, its main capabilities were (1) reporting system information, (2) stealing protected storage information, (3) stealing online credential information, and (4) contacting the C&C server for additional tasks to perform, as the agents' code had built-in commands waiting to be executed (Alzubaidy and Hatim, 2015, p. 123).

Today, as per ENISA (2019, pp. 130–131), botnets pose at being multi-staged and modular threats that have several features such as (1) self-propagation, (2) self-destruction, (3) anonymous communication, (3) persistent behaviour, (4) origin obfuscation, and (5) downloading payloads and installing themeven in the memory.Furthermore, one can distinguish botnet features according to their functionalities such as the (1) command module, (2) control module, (3) infection module, and (4) stealth module. The command module sends commands to the agents, and the control module controls the ownerships and relationships between the C&C and the bot. The infection module's task is to find vulnerable network nodes, such as servers, client machines, network devices, and the Internet of Things (IoT), and infect them. The stealth module has an essential role in hiding from antimalware services or even disabling their functionalities.

The commands that the command module carries determine the given botnet's capabilities that performattacking activities. The effectuated attack depends on the botmaster's motives. Such an attack is mainly one of the following: DDoS, phishing, spam and spim (spammed instant messages) sending, spyware, adware, ransomware cryptocurrency mining, fake news propagation, and more. The disruptionware simply overwrites or wipes the data stored on the infected device without any possibility of recovering it.

Used resources of attacked and utilised entities

Eventually, the botnets' capabilities determine the used or affected resources on the attacked entities and its operation's technical effects.As a botnet is acollection of its connected bots, which is an agent on infected nodes to tackle with the nodes' resources to perform given tasks, one can regarda botnet as a distributed system with separated resources for achieving a common goal in a certain sense. Hence, botnets tackle the infected computers' computational capacity, and networking, and process data to conduct an attack on the infected machines or targetfurther uninfected ones. The following subsections contain an analysis ofthe specifics of these parameters.

Computational capacity

As a botnet can be thought of as a distributed system with non-interactive workloads, it handles its bots' computational resource. Therefore, a botnet's computational capacity is the aggregated amount of its bots' capacity.The computational capacity (or performance) is the amount of valuable work accomplished by a computer system, which depends on response time, throughput, and the computer system's execution time. The response time is the time interval from the starting point to completing a task, which includes waiting for input or output and other processes, accessing disk and memory, and the time spent on execution time. The throughput is the total amount of computing tasks done in a given interval.

Networking

An attacker can use the network resources of the infected machines for attacking other entities. However, enterprises usually follow basic principles such as the hierarchical network model and modularity (Cisco, 2014a) in the planning, implementing, and operating of their network. This design method involves dividing the network into discrete layers, in which each layer in the hierarchy provides specific functions within the overall network (Cisco, 2014b). Nevertheless, the Internet is also a hierarchical network based on the autonomous systems (ASs) concept, which is routing domainscomprising a collection of routers under the same administration. The Interneten compasses several smaller and bigger Internet Service Providers (ISPs), Internet Exchange Points (IXPs), and Content Delivery Networks (CDNs) (Dey *et al.*, 2018).

This hierarchical approach of enterprise networks and the Internet is crucial as it gives limitations and opportunities for the attackers. The limitations originate from the fact that a bot has a restrained network bandwidth of the infected computer resources. Furthermore, the malicious traffic has to flow over aggregated connections, such as between the enterprise and the ISP, or between ISPs. However, on the other hand, the hierarchical structureallows the aggregating of the malicious traffic to achieve ahigher performance, e.g., for DDoS or spamming. Moreover, the attacked entity also has the limitationsa bot has; therefore, it is possible to get the desired effect with a lower performance from the attacker's viewpoint if the targeted systems have fewer available resources such as bandwidth or computational capacity.

Processed data

In every presence and in each status, data assets have theirconfidentiality, integrity, and availability parameters (Beckers, 2015). Confidentiality means only authorised users and processes can access or modify data; so, one has to protect processed data from unauthorised access and misuse. Integrity is the protection of data from unauthorised alteration; hence, a defender has tomaintain the data in a correct state,ensuring that nobody or no process canmodify it, either accidentally or maliciously improperly. According to the availability parameter, data has to be accessible promptly and uninterruptedly to authorised users and processes. An attack can therefore specifically affect at least one of its parameters such as confidentiality, integrity, or availability of specific data or a set of data depending on the botmaster's motivation and the botnet' capabilities.

Technical effects of botnets

Based on the previous chapter'sdiscussion about the effects on the processed data's confidentiality, integrity, or availability, the following subsectionsdiscuss the attack types mentioned in the Capabilities section, according to the attacked entity's main technical effects.

Confidentiality focus attacks

Spyware collects and shares personal and confidential information without the user's consent (Aycock, 2011). The information may include the company's proprietary data, computer, network data, personal data about the user, such as activities and behaviour from various applications as, e.g., browsers and instant messengers. Spyware can transfer all the information to the botmaster via its C&C server. The adware that is a particular category of spyware works as a tool for advertisingand collects the user information and behaviour for interested advertisers or other interested parties without their consent. It can display advertisements on the screen of a given user, most often within a web browser.

Phishing is the mechanism of crafting messages that use social engineering techniques to fraudulently attempt to obtain sensitive information from users (Khonji, Iraqi and Jones, 2013). It tricks the recipients into clicking on a link that points to an unsafe URL, hand over their credentials via legitimate-looking websites, online payment, and similar. It is typically carried out via e-mail spoofing or instant messaging. Spear phishing is directedat specific individuals or companies, while whaling attacks specifically senior executives and other high-profile targets.

Integrity focus attacks

Cryptocurrency mining (or cryptojacking) refers to the method that uses the processing power of the victim's device without his or her consent to mine cryptocurrencies. It may work with the installation of software on a user'sdevice that would run in the background or a browser aftervisiting a malicious website. The algorithm is about to generate units of a cryptocurrency that would go back into the attacker's wallet (Eskandari *et al.*, 2018). It wastes bandwidth and computational capacity. The user may noticea reductionin the speed and efficiency of legitimate computing workloads. The extra computation increases the power consumption causing direct costs. Furthermore, if the code runs on a mobile device, it also negatively affects its battery lifetime.

Fake news (or hoaxes; Tandoc, Lim and Ling, 2018) is not a new phenomenon; however, digitalisation has facilitated itsdiffusion via social media, making online visitorsmore susceptible to popularity indicators. Social bots (Siddiqui, Healy and Olmsted, 2018) can spread non-curated content using trending topics and hashtags. Their primary strategy is to reach a broader audience, which, in many cases, further helps the propagation of fake news by (1) tweeting fake news items or (2) replying or commenting on the postings of real social media users with false information.

Fake news delivery is also possible with spams and spims. Spam and spimare abusive uses of e-mail and instant messaging to flood unsolicited messages in bulk. Despite its low cost, spamming causes a massive waste of time and resources for recipients and service providers in network bandwidth and storage.

On the other hand, ransomware stops users from accessing the data they use, and it may freezetheir devices, too. For users to be able to release locked devices, an online payment ransom is demanded, typically in cryptocurrency (Youngblood, 2016). Criminals have committed ransomware attacks against a variety of organisations as victims paid the ransom in many cases. Nowadays, it has evolved from stand-alone attacks to campaigns. The victims of these attacks not only suffer financial losses, but also lose their credibility.

Availability focus attacks

Disruptionware is a particular category of malware that is designed to suspend operations within the targeted organisation. It aims to suspend operations and disrupt continuity; therefore, it is devastating in mission-critical systems and legacy systems that lack redundancy (Brichant and Eftekhari, 2019). Worms, file infectors, wipers, and even subcategories of ransomware belong to this category. A worm replicates itself over the network from device to device without the guidance of its creator. A file infector infects executable files by overwriting them or inserting infected code that disables them. A wiper deletes all the data stored on the infected device. In the case of disruptionware, the attacked and utilised entities are the same.

On the other hand, a DDoS attack attempts to disrupt the targeted entity's regular traffic or service behaviour by overwhelming the target or its surrounding infrastructure. In the case of a DDoS attack, the attacked and the utilised entities are distinct. A DoS attack occurs when an attacker makes the target machine local or network resource unavailable to its intended users temporarily or indefinitely. Such solutions as physical disruption, MAC, TCP, UDP, ICMP flood, and the routing protocol modification in the network infrastructures also belong to DoS.

According to the TCP/IP model (Ravali, 2013), there are (1) Internet layer attacks such as ICMP flood, smurf attack, and ping of death, (2) Transport layer attacks such as syn flood and UDP flood, and (3) Application layer attacks such as malformed SSL requests, and HTTP, telnet, FTP requests, andDNS attacks (Specht and Lee, 2004).

Case studies

The following subsections contain ananalysis of specific botnets according to the discussed attributes. The chosen botnets try to represent the most dangerous or spectacular ones from the last decade, specifically: (1) ElectrumDoSMiner, (2) Emotet, (3) Gamover Zeus, (4) Mirai, and (5) VPNfilter.

ElectrumDoSMiner

Threat actors have causedmany users of the Electrum Bitcoin wallet to be victims of phishing attacks, at least since December 2018, by tricking them into downloading a malicious version of the wallet by exploiting a weakness of the Electrum software. As a result, attackers were able to stealmany bitcoins from their owners. In February, the developers of Electrum decided to exploit the same flaw to force them to download the latest patched version to tackle this problem. In March, Electrum tried to exploit another vulnerability unknown to the public. Shortly after, criminals launched distributed DDoS attacks against Electrum servers. Theseattacks stopped legitimate Electrum servers dealing with legitimate requests meaningpreviously untouched clients turned to rogue servers which stole from other wallets (Malwarebytes Labs, 2019a).

Table 1presents the threat parameters of ElectrumDoSMiner, which applied Crimeware as Service tools such as the Smoke loader and the RIG exploit kit, stipulating its TTP, to conduct a DDoS attack. An interesting point is that by analysing the infected machines' geolocation, the largest concentration was in the Asia Pacific region (**Figure 2**).

Table 1. Threat parameters of ElectrumDoSMiner.

Motivation	Financial
Business model	The threat actor may have used Crimeware as a Service to apply the Smoke loader and the RIG exploit kit (Malwarebytes Labs, 2019b). The Smoke Loader (MITRE ATT&CK, 2019) has been able toload other malware since 2011, and the RIG exploit kit (FireEye, 2018) can be considered a repository or collection of various exploits.
Cooperation willingness	There is no information on whether it has taken over other bots or cooperatedwith other C&C servers or other criminals.
Capabilities	Its TTP is stipulated by the Smoke Loader and the RIG exploit kit.
Attack capabilities	DDoS attack

Used resources on attacked entities	Network resources and computational capacity of Electrum clients
Technical effects on attacked entities	The integrity of the Electrum clients and confidentiality of the Electrum valets
Used resources on utilised entities	Network resources of bots
Technical effects on utilised entities	The integrity of the system and availability of network

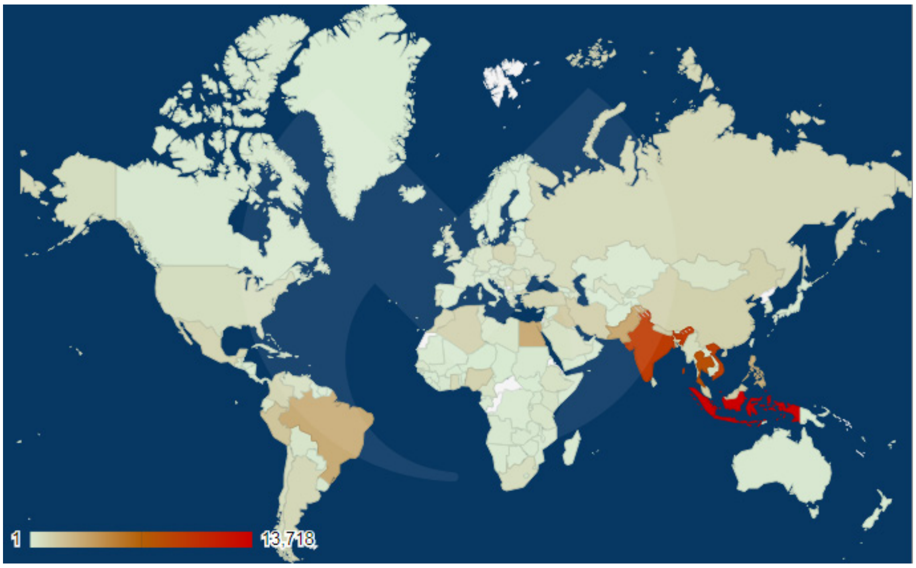

Figure 2. Presence of ElectrumDoS-Miner. Source: Malwarebytes Labs (2019b).

Emotet

Emotetwas initially a banking trojan. Its first detection in the wild was in 2014. However, it disappeared in 2016 and 2017. As seenlater, its operators had updated the trojan and reconfigured it to work primarily as a loader for other malware, e.g., spam as Trickbot and ransomware as Ryuk (Fortinet, 2019). Furthermore, in September 2019, it ran three separate botnets called Epoch 1, Epoch 2, and Epoch 3 to reducethe probability and the effect of a takeover or a takedown (Spamhouse, 2019).

Table 2 discusses the threat parameters of Emotet, which is a botnet offering a loader functionality for others as, e.g., Trickbot and Ryuk; it is in effect a Cybercrime Infrastructure as a Service tool. Therefore, some capabilities depend on the carried botnets. An examination of the presence of infections (**Figure 3**) reveals the most affected countries are Germany, the United States, India, the Russian Federation, and China.

Table 2. Threat parameters of Emotet.

Motivation	Financial		
Business model	With the reconfiguration, the threat actor behind Emotet has been offering the botnet as Cybercrime Infrastructure as a Service.		
Cooperation willingness	Due to the business model, it has delivered other malware, including Trickbot and Ryuk.		
Capabilities	Its TTP is described in (Security Boulevard, 2020).		
Attack capabilities	Emotet is a loader; therefore, the attack type depends on the delivered payload.		
	Spam (e.g., Trickbot)	Ransomware (e.g., Ryuk)	Further payload(s)

Used resources on attacked entity	Network and storage	Storage	Depending on the payload(s)
Technical effects on attacked entities	Availability and integrity of network and storage	The integrity of storage media on attacked entities	Depending on the payload(s)
Used resources on utilised entity	Network resources of bots	Network resources of bots	Depending on the payload(s)
Technical effects on utilised entities	The integrity of system and availability of network on the attacked entities	The integrity and the availability of system and availability of network on the attacked entities	Depending on the payload(s)

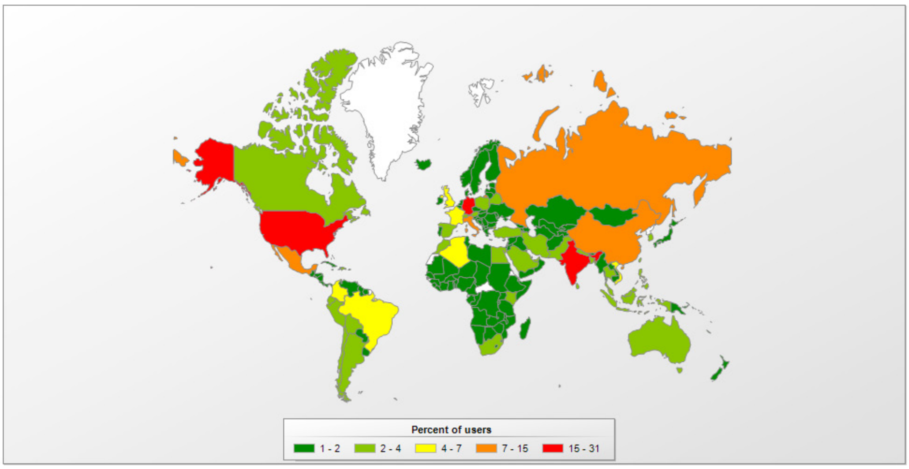

Figure 3. Presence of Emotet. Source: Kaspersky (2018).

Gameover Zeus

Gameover Zeus (GOZ) is a variant of the Zeus family, andwas identified in September 2011 using a decentralised peer-to-peer infrastructure of the compromised end-points. GOS utilised its P2P network for communicating commands, binary updates, or configuration and sent back stolen data in which it employed encryption to evade detection. Furthermore, GOZ was responsible for spreading Cryptolocker ransomware, spamming, data theft, and DDoS (Sandee, 2015). However, due tosuccessfulcooperation, law enforcement agencies were able to takedown GOZ in May 2014 (Europol, 2014).

Table 3 presents the threat parameters of GOZ, from which there are two interesting points: (1) there were a sophisticated cooperation of several threat actors working as a group, to create the botnet, which is explicitly known by security researchers, and (2) GOZ builders are not sold to individuals, showing less cooperation willingness. According to the geolocation attributes (Figure 4), the infected machines were mostly in the United States, India, and the United Kingdom.

Table 3. Threat parameters of Gameover Zeus.

Motivation	Financial motivation from stealing banking account details and a ransomware attack Political motivation because it conducted "searches for documents with certain levels of government secret classifications, and for specific government intelligence agency employees, and information about politically sensitive issues" (Sandee, 2015, p. 9)
Business model	N/A

Cooperation willingness	After the Zeus code became publicly available, the Zeus 2.1.0.X, used by the JabberZeuS group, morphed into GOZ. There were two leaders, a support crew, and several preferred suppliers to implement and troubleshoot certain features. There were also operators for the bots and the backend infrastructure (Sandee, 2015). “Gameover builders are not sold to individuals. Instead, they are privately operated which means only one Gameover botnet is running” (Trend Micro, 2014)			
Capabilities	“[…] the builder has a number of functions, one of which is to build updates with a number of configurable settings, and another is to communicate with the peer-to-peer network to interact with it in a number of ways, including distributing configurations and updates. For interaction with the peer-to-peer network, the builder needsa list of seed nodes, specified with the kbucket option […]” (Antonakakis *et al.*, 2017, p. 11) “The newer version of the builder came both with built in rootkit (Nercurs) and new options, which included crawling the peer-to-peer network, and the inclusion of support for creating signed plugins […]” (Antonakakis *et al.*, 2017, p. 12)			
Attack capabilities	DDoS	Spam	Ransomware	Spyware
Used resources on attacked entities	Network resources and computational capacity	Network and storage	Storage	Processed data
Technical effects on attacked entities	Availability	Availability and integrity of network and storage	The integrity of storage media on attacked entities	Confidentiality of files, documents, and any processed data
Used resources on utilised entities	Network resources of bots			Utilised and attacked entities are the same
Technical effects on utilised entities	Integrity of system and availability of network			Utilised and attacked entities are the same

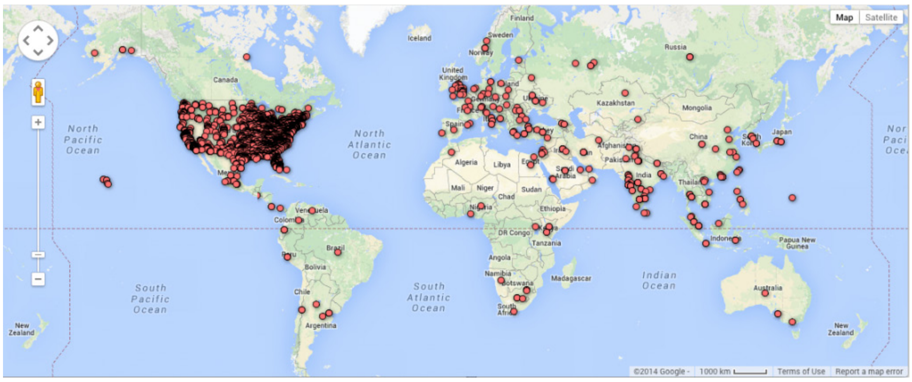

Figure 4. Presence of Gameover Zeus. Source: Ilascu (2014).

Mirai

Threat actors made Mirai, the infamous botnet, which was comprised of hundreds of thousands of thingbotsweaponising the Internet of things (IoT). Mirai started its DDoS attacks in August 2016. In early October, its developer released the Mirai source code as open-source. It infected more than 300,000 IoT devices, and soon after, it had more thana half-million thingbots. Mirai was in charge of attacks against Dyn DNS infrastructure, the French OVH datacentre and cloud provider, and the Deutsche Telekom infrastructure (Antonakakis *et al.*, 2017).

Due to its open-source nature, it has had several variants, such as Satori, Okiru, and Owari (Liu and Wang, 2018). Even Android smartphones were targets for bot-creation (Ullrich, 2018). However, one version of Satori, a variant of Mirai, changed the profile to crypto mining. After infecting, it switched the wallet to the attacker's wallet, resulting inall coins being generated for the attacker (Ashford, 2018).

According to the threat parameters of Mirai, depicted in Table 4, there was massive cooperation willingness among threat actors and business efforts from the botnet's operator(s), who had managed IoT devices-based bots worldwide (Figure 5).

Table 4. Threat parameters of Mirai.

Motivation	Financial for botmaster Possibly FIG for renter	Depending on the variant, e.g. it is usually the same as the original Mirai, but the cryptomining variant of Satori was created with clear financial gain in mind	
Business model	Its developer had made its code open-source on the Darknet, and thingbots may have been rented (Bing, 2016).	Probably the DDoS capable variants were alsorented (Liu and Wang, 2018).	
Cooperation willingness	There is no information about botnet takeovers or cross communications between Mirai variants or other bots.		
Capabilities	Its kill chain is described in (Manuel, 2018) and (Antonakakis *et al.*, 2017, pp. 2–3).	Due to the open-source nature of its source code, there are several variants with various capabilities, e.g. the OMG set up 3proxy on thingbots.	
Attack capabilities	DDoS	DDoS (e.g., Satori)	Cryptomining (e.g., Satori.miner variant)
Used resources on attacked entities	Network resources and computational capacity	Network resources and computational capacity	Computational capacity
Technical effects on attacked entities	Availability	Availability	The integrity of computer and wallets
Used resources on utilised entities	Network resources of bots	Network resources of bots	Utilised and attacked entities are the same
Technical effects on utilised entities	The integrity of the system and availability of network	The integrity of the system and availability of network	Utilised and attacked entities are the same

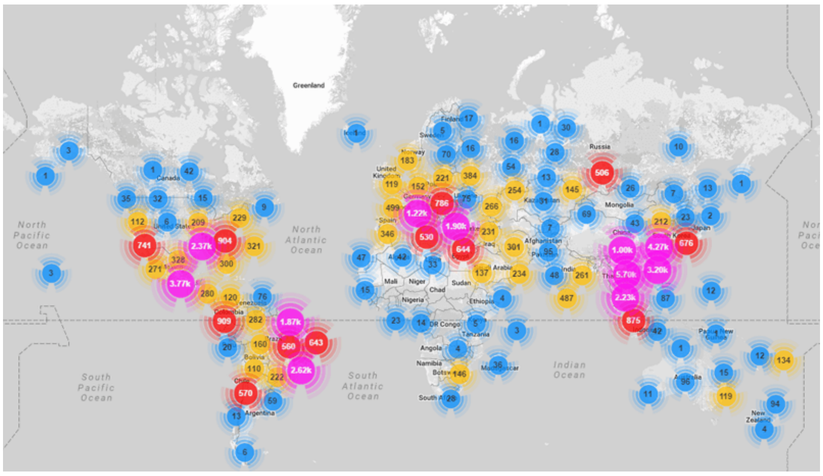

Figure 5. Presence of Mirai. Source: Montalbano (2018).

VPNFilter

VPNFilter initially attacked devices located in Ukraine, but it spread to other countries very quickly. In May 2018, one of the most extensive campaigns was reported as having composed around 500,000 bots. However, after the VPNfilter attack, Ukraine started developingcyber-defence capabilities (Vakulyk *et al.*, 2020).

The botnetapplied a multi-stage and modular infection. The first stage had the capability of boot persistence on devices; the second stage acted as a RAT, and the thirdstage included plugins to enhance functionalities. By the application of its RAT functions, it collected data, inspected local traffic, hijacked network data, communicated on the Tor network, and even wiped local firmware to destroy a specific device or all infected devices (Cisco Talos, 2018). Cisco Talos researchers found an interrelation between VPNFilter and BlackEnergy disruptionware that targeted the Ukrainian powergrid in the winter of 2015-2016 (Anomali, 2019). Both were the product of the APT28 group. There is no information about the business model and cooperation willingness, see Table 5; however, according to the conditional sponsorship of the Russian government, there must have been certain cooperation. Although the VPNfilter started mainly in Ukraine, its presence has changed worldwide (Figure 6).

Table 5. Threat parameters of VPNfilter.

Motivation	Political becauseit was the product of the APT28 group, which is “most probably sponsored by the Russian government. […] its primary interests are in the Caucasus, Eastern European Governments and Militaries, NATO and Other European Security Organisations including the European Defence Exhibitions” (Bederna and Szadeczky, 2019, p. 53).
Business model	N/A
Cooperation willingness	N/A
Capabilities	Its kill chain is described in ENISA (2019), and its TTP is in Cisco Talos (2018). It is a multi-stage and modular malware that has “the capabilities of an intelligence-collection platform, such as file collection, command execution, data exfiltration, and device management, and some versions possessed a self-destruct capability that overwrites a critical portion of the device’s firmware and reboots the device” (Bederna and Szadeczky, 2019, p. 57).
Attack capabilities	Spyware
Used resources on attacked entities	It utilised storage and accessed processed data
Technical effects on attacked entities	Confidentiality of any processed data The integrity of the infected end-points operation system Availability of processed data in the case of sanitisation
Used resources on utilised entities	Utilised and attacked entities are the same
Technical effects on utilised entities	Utilised and attacked entities are the same

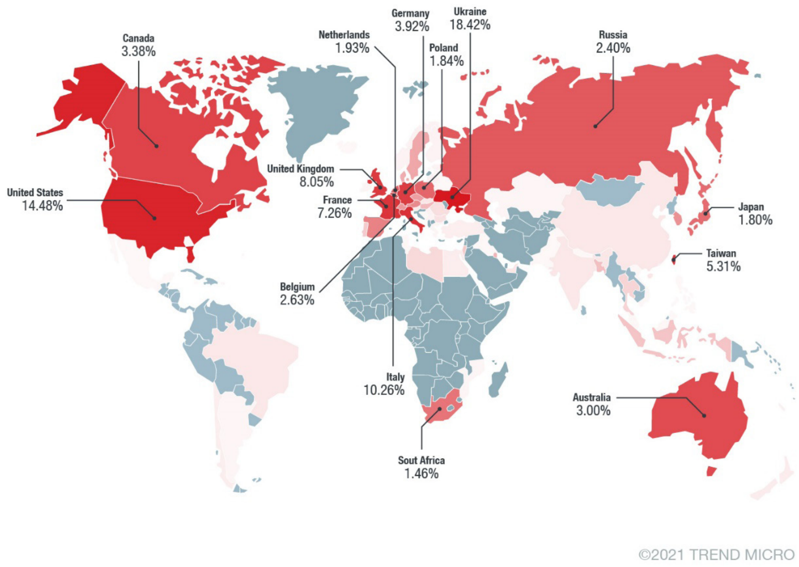

Figure 6. Presence of VPNfilter
Source: Trend Micro (2021).

Discussion

For analysing the attributes of botnets, this paper created a framework for a comprehensive review of the ecosystemof botnets, as shown in Figure 7. Botmasters as threat actors havethe motivation, evenchoosing a business model to operate, and may have (non-)cooperation willingness. As the technology factor of a botnet attack, they use the resources ofthe attacked and utilised entities, and technical effectssuch as confidentiality (C), integrity (I), and availability (A) define botnet behaviour.

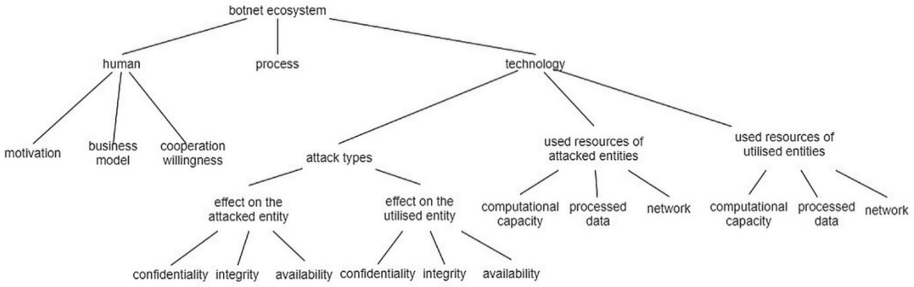

Figure 7. Identified attributes of the botnet ecosystem.

Based on the defined framework, this paper reviewed five botnets,the ElectrumDoS-Miner, Emotet, Gamover Zeus, Mirai, and VPNFilter. Utilising such a botnet, as Mirai was during its peak activity, has the potential to paralyse networks. Even another type of botnet, like VPNfilter is able to steal files, documents, and any processed data. Moreover, when a cyberattack hits an unprepared country as it did Ukraine through VPNFilter in 2018, the effect may be multiplied. However, Ukraine has learnt from the attack and started improving its cyber-defence capabilities, i.e. according to the BMIS elements. Table 6 displays these discussed parameters according to the created model.

Table 6. Comparison of the reviewed botnets.

		ElectrumDosMinter	Emotet		Gamover Zeus				Mirai	VPNFilter
Possible motivation	Financial	X	X	X	X				X	
	Political				X					X
	FIG								X	
Business model	Crimeware as a Service	X			?					?
	Cybercrime Infrastructure as a Service		X	X	?				X	?
	Hacking as a Service				?					?
Cooperation willingness	Cooperative	?	X	X	X					?
	Noncooperative	?								?
Capabilities		Described by TTPs								
	Attack	DDoS	Loader		DDoS	Spam	Ransomware	Spyware	DDoS	Spyware
			Spam (Trickbot)	Rans (Ryuk)						
Used resource of attacked entity	Comp. capacity	X			X					
	Networking	X	X		X	X			X	
	Storage		X	X		X	X			
	Processed data							X		X
Used resource of utilised entity	Comp. capacity									
	Networking	X	X	X	X	X	X			
	Storage									
	Processed data									
Technical effect on the	attacked entity	C,I	I,A	I,A	A	I,A	I	C,I	A	C,I,A
	utilised entity	I	I,A	I,A	I	I	I		I,A	

Conclusion

Without any doubt, botnets, as a beloved tool of attackers,have become more sophisticated in the last two decades. Indeed, attackers have been employing botnets with different motivations and capabilities; therefore, there are also differences in thetechnical effects. Furthermore, considering the advancements of information technology and the dependence of today's society on (critical) infrastructure, a botnet being deployed directly or indirectly on (critical) infrastructural elements canhave devastating effects.

For defending entities, achievingthe target state of defending capabilities is impossible with a one-time development due to cyberspace's dynamic behaviour and, hence, botnets. One's cyber-defence needs to be developed and threat intelligence on botnets carried out using themethodology discussed in this paper. This framework comprises people and technological attributes according to the BMIS model. The people factor encompasses motivation, business model, and cooperation willingness; and the technology factor covers some aspects of capabilities as the used resources ofthe attacked and the utilised entities, and technical effectssuch as confidentiality, integrity, andavailability define the behaviour of botnets. The application of the created model highlights important parts of the overall botnet ecosystems. In effect, the human attributes such as motivation, the applied business model, and cooperation willingness are most important. Based on the case studies, the applied business model and the cooperation willingness attributes can fundamentally affect the behaviour of botnets, although the current model does not handle this connection. Nevertheless, based on the case studies, the geolocation data can also serve as important data for a given botnet. Furthermore, the current processes are not detailed. According to the authors' opinion, this model can enhance the recognition of the botnets' ecosystem after the inclusion of the missing attributes and further important technological attributes outside the paper's scope.

Funding

This research was supported by the ERDF project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

Contributions

Writing, methodology, original draft preparation by ZB; conceptualization, writing, funding acqusition, validation by TS; All authors have read and agreed to the published version of the manuscript.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Alzubaidy, L. and Hatim, K. (2015) 'Analysis and detection of the Zeus Botnet crimeware', *International Journal of Computer Science and Information Security*, 13, pp. 121–135.

Anomali (2019) *APT28 timeline of malicious activity*. Available at: https://forum.anomali.com/t/apt28-timeline-of-malicious-activity/2019 (Accessed: 21 February 2019).

Antonakakis, M. April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K. and Zhou, Y. (2017) 'Understanding the Mirai Botnet', USENIX Security.

Ashford, W. (2018) *Next-gen Mirai botnet targets cryptocurrency mining operations*, Computer Weekly.com. Available at: https://www.computerweekly.com/news/450433414/Next-gen-Mirai-botnet-targets-cryptocurrency-mining-operations (Accessed: 21 April 2020).

Aycock, J. (2011) *Spyware and adware*. Switzerland AG: Springer. doi: 10.1007/978-0-387-77741-2.

Banday, M.T., Qadri, J.A. and Shah, N.A. (2009) 'Study of botnets and their threats to internet security', *Sprouts: Working Papers on Information Systems*, 9(24), 9–24.

Beckers, K. (2015) *Pattern and security requirements engineering-based establishment of security standards*. Switzerland AG: Springer. doi: 10.1007/978-3-319-16664-3.

Bederna, Z., Rajnai, Z. and Szadeczky, T. (2021) 'Attacks against energy, water and other critical infrastructure in the EU', in *2020 IEEE 3rd international conference and workshop on electrical and power engineering (CANDO-EPE)*, Óbuda, Hungary. doi: 10.1109/CANDO-EPE51100.2020.9337751.

Bederna, Z. and Szadeczky, T. (2019) 'Cyber espionage through botnets', *Security Journal*, 33, pp. 43–62. doi: 10.1057/s41284-019-00194-6.

Bing, C. (2016) *You can now buy a Mirai-powered botnet on the dark web, CYBERSCOOP*. Available at: https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web/ (Accessed: 21 April 2020).

Brichant, R. and Eftekhari, P. (2019) The rise of disruptionware. Available at: https://icitech.org/wp-content/uploads/2019/09/ICIT-Brief-The-Rise-of-Disruptionware.pdf (Accessed: 29 September 2019).

Cantón, D. (n.d.) *Botnet detection through DNS-based approaches*, INCIBE. Available at: https://www.incibe-cert.es/en/blog/botnet-detection-dns (Accessed: 1 August 2018).

Chang, W., Mohaisen, A., Wang, A. and Chen, S. (2015) 'Measuring botnets in the wild: Some new trends', in *ASIACCS 2015—Proceedings of the 10th* ACM *Symposium on Information, Computer and Communications Security*. doi:10.1145/2714576.2714637.

Chukwudi, A.E. (2017) 'Game theory basics and its application in cyber security', *Advances in Wireless Communications and Networks*, 3(4), pp. 45–49. doi: 10.11648/j.awcn.20170304.13.

Cimpanu, C. (2019) *Hacker takes over 29 IoT botnets*, ZDNet. Available at: https://www.zdnet.com/article/hacker-takes-over-29-iot-botnets/ (Accessed: 10 March 2020).

Cisco (2014a) *Cisco Networking Academy connecting networks companion guide: Hierarchical network design*. Cisco Press.

Cisco (2014b) *The Art of Network Architecture*. Cisco Press.

Cisco Talos (2018) *New VPN Filter malware targets at least 500K networking devices worldwide*. Available at: https://blog.talosintelligence.com/2018/05/VPNFilter.html (Accessed: 20 February 2020).

Dey, P.K. Canbaz M.A., Yuksel, M. and Gunes, M.H (2018) 'On correlating ISP topologies to their businesses', in *IEEE international conference on communications*. doi: 10.1109/ICC.2018.8422620.

Do, C.T., Tran, N.H., Hong, C., Kamhoua, C.A., Kwiat, K. A., Blasch, E. ... and Iyengar, S.S. (2017) 'Game theory for cyber security and privacy', *ACM Computing Surveys*, 50(2), pp. 1–37. Article No.: 30. doi: 10.1145/3057268.

Dobák, I. (2021) 'Many areas of cybersecurity are also interconnected with national security', *Security & Defence*, 33(1), pp. 75-85. doi: 10.35467/sdq/133154.

Eskandari, S., Leoutsarakos, A., Mursch, T. and Clark, J. (2018) 'A first look at browser-based cryptojacking', in *Proceedings of 3rd IEEE European symposium on security and privacy workshops, EURO S and PW 2018*. doi: 10.1109/EuroSPW.2018.00014.

European Union (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union', *Journal of the European Union*. Available at: http://data.europa.eu/eli/dir/2016/1148/oj.

European Union Agency for Network and Information Security (ENISA) (2019) *ENISA threat landscape report 2018*. doi: 10.2824/622757.

European Union Agency for Network and Information Security (ENISA) (n.d.) *Botnets*. Available at: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets (Accessed: 26 February 2020).

Europol (2014) *International action against 'Gameover Zeus' botnet and 'CryptoLocker' ransomware*. Available at: https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware (Accessed: 20 April 2020).

FireEye (2018) *Threat research—A deep dive into RIG exploit kit delivering grobios trojan*. Available at: https://www.fireeye.com/blog/threat-research/2018/05/deep-dive-into-rig-exploit-kit-delivering-grobios-trojan.html (Accessed: 20 April 2020).

Fortinet (2019) *New emotet report details threats from one of the world's most successful malware operations*. Available at: https://www.fortinet.com/blog/threat-research/emotet-playbook-banking-trojan.html (Accessed: 20 April 2020).

Gandhi, R.A., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., and Laplante, P. (2011) 'Dimensions of cyber-attacks: Cultural, social, economic, and political', *IEEE Technology and Society Magazine*, 30(1), pp. 28–38. doi: 10.1109/MTS.2011.940293.

Halder, D. and Jaishankar K. (2012) *Cyber crime and the victimization of women: Laws, rights, and regulations*. Hershey, PA: IGI Global. doi: 10.4018/978-1-60960-830-9.

IBM Corporation (2016) *The inside story on botnets*. Available at: https://www.ibm.com/downloads/cas/V3YJVYZX.

Ilascu, I. (2014) 'New gameover Zeus botnet forming, the US sees most infections', Sofpedia News. Available at: https://news.softpedia.com/news/New-Gameover-Zeus-Botnet-Forming-the-US-Sees-Most-Infections-455112.shtml (Accessed: 27 May 2021).

Kaspersky (2018) *Trojan-Banker.Win32.Emotet*. Available at: https://threats.kaspersky.com/en/threat/Trojan-Banker.Win32.Emotet/ (Accessed: 27 May 2021).

Khonji, M., Iraqi, Y. and Jones, A. (2013) 'Phishing detection: A literature survey', in *IEEE Communications Surveys and Tutorials*, 15(4), pp. 2091–2121. doi: 10.1109/SURV.2013.032213.00009.

Liang, X. and Xiao, Y. (2013) 'Game theory for network security', *IEEE Communications Surveys and Tutorials*, 15(1), pp. 472–486. doi: 10.1109/SURV.2012.062612.00056.

Liu, Y. and Wang, H. (2018) VB2018 paper: Tracking Mirai variants', *Virus Bulletin*. Available at: https://www.virusbulletin.com/virusbulletin/2018/12/vb2018-paper-tracking-mirai-variants/ (Accessed: 21 April 2020).

Malwarebytes Labs (2019a) *Electrum bitcoin wallets under siege*. Available at: https://blog.malwarebytes.com/cybercrime/2019/04/electrum-bitcoin-wallets-under-siege/ (Accessed: 20 April 2020).

Malwarebytes Labs (2019b) Electrum DDoS botnet reaches 152,000 infected hosts. Available at: https://blog.malwarebytes.com/cybercrime/2019/04/electrum-ddos-botnet-reaches-152000-infected-hosts/.

Manky, D. (2013) 'Cybercrime as a service: A very modern business', *Computer Fraud and Security*. doi: 10.1016/S1361-3723(13)70053-8.

Manuel, J. (2018) Searching for the reuse of Mirai code: Hide 'N Seek Bot. Available at: https://www.fortinet.com/blog/threat-research/searching-for-the-reuse-of-mirai-code--hide--n-seek-bot.html (Accessed: 10 March 2020).

Miller, C. (2010) 'Kim Jong-il and me: How to build a cyber army to attack the US', DEF CON 18.

MITRE ATT&CK (2019) *Smoke loader*. Available at: https://attack.mitre.org/software/S0226/ (Accessed: 20 April 2020).

Montalbano, E. (2018) *Mirai creators Cooperate with feds to avoid prison, the security ledger*. Available at: https://securityledger.com/2018/09/mirai-creators-cooperate-with-feds-to-avoid-prison/ (Accessed: 27 May 2021).

Putman, C.G.J., Abhishta, A. and Nieuwenhuis, L.J.M. (2018) 'Business model of a botnet', in *Proceedings of the 26th euromicro international conference on parallel, distributed, and network-based processing, PDP 2018*. doi: 10.1109/PDP2018.2018.00077.

Ravali, P. (2013) A comparative evaluation of OSI and TCP/IP models', *International Journal of Science and Research*, 4(7), pp. 514–521.

Ryan, R.M. and Deci, E.L. (2000) 'Self Determination Theory and the facilitation of intrinsic motivation, social development and well-being', *American Psychologist*, 55(1), pp. 68–78. doi: 10.1.1.529.4370.

Sandee, M. (2015) *GameOver ZeuS—Backgrounds on the Badguys and the backends*. Available at: https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends-wp.pdf.

Security Boulevard (2020) *Emotet attacks—A spike to start the year….* Available at: https://securityboulevard.com/2020/02/emotet-attacks-a-spike-to-start-the-year/ (Accessed: 20 April 2020).

Siddiqui, H., Healy, E. and Olmsted, A. (2018) 'Bot or not', in *12th International conference for internet technology and secured transactions, ICITST 2017*. doi: 10.23919/ICITST.2017.8356448.

Spamhouse (2019) *Estimating Emotet's size and reach*. Available at: https://www.spamhaus.org/news/article/791/estimating-emotets-size-and-reach (Accessed: 20 April 2020).

Specht, S.M. and Lee, R.B. (2004) 'Distributed denial of service: Taxonomies of attacks, tools and countermeasures', in *International workshop on security in parallel and distributed systems*, pp. 543-550.

Szőr, P. (2005) *The art of computer virus research and defense*. New Jersey: Pearson Education.

Tandoc, E.C., Lim, Z.W. and Ling, R. (2018) 'Defining "fake news": A typology of scholarly definitions', *Digital Journalism*. doi: 10.1080/21670811.2017.1360143.

Trend Micro (2014) *Gameover: ZeuS with P2P functionality disrupted*. Available at: https://www.trendmicro.com/en_us/research/14/f/gameover-zeus-with-p2p-functionality-disrupted.html (Accessed: 27 May 2021).

Trend Micro (2021) *VPNFilter two years later: Routers still compromised*. Available at: https://www.trendmicro.com/en_ca/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html (Accessed: 27 May 2021).

Ullrich, J.B. (2018) *Worm (Mirai?) exploiting android debug bridge (Port 5555/tcp), SANS ISC InfoSec forums*. Available at: https://isc.sans.edu/forums/diary/Worm+Mirai+Exploiting+Android+Debug+Bridge+Port+5555tcp/23856/ (Accessed: 21 April 2020).

Vakulyk, O., Petrenko, P., Kuzmenki, I., Pochtovyi, M. and Orlovskyi, R. (2020) 'Cybersecurity as a component of the national security of the state', *Journal of Security and Sustainability Issues*, 9(3), pp. 775–784.

Verizon (2020) *Data breach investigations report 2020*. Available at: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (Accessed: 23 March 2021). doi: 10.1016/S1361-3723(20)30059-2.

von Roessing, R. (2010) 'The ISACA business model for information security: An integrative and innovative approach', in *ISSE 2009 securing electronic business processes*. doi: 10.1007/978-3-8348-9363-5_4.

Youngblood, J.R. (2016) 'Ransomware', in *Business theft and fraud. Detection and prevention*. Boca Raton, FL: Routledge. doi: 10.4324/9781315380780-37.