Cyber espionage through Botnets

Zsolt Bederna & Tamas Szadeczky

Security Journal

ISSN 0955-1662
Volume 33
Number 1

Secur J (2020) 33:43-62
DOI 10.1057/s41284-019-00194-6

Security Journal (2020) 33:43–62
https://doi.org/10.1057/s41284-019-00194-6

ORIGINAL ARTICLE

Cyber espionage through Botnets

Zsolt Bederna[1] · Tamas Szadeczky[2,3]

Published online: 24 September 2019

Abstract

Botnets, the groups of illegally controlled infected devices on the Internet have had a history of two decades already. This history shows an evolution of the infection techniques, the scope of the target devices, and their usage. Thus, the new direction is the usage of sophisticated data leakage techniques by state-sponsored hacker groups. Our article analyses this evolution while focusing on Botnet usage for cyber espionage. We present the Botnet architecture in the context of network science research, lifecycle, applied network protocols, and capabilities. Next, we analyze two examples, the APT28 group activities and the VPNFilter Botnet, which demonstrate the real-life cyber espionage capability of this technique.

Keywords Botnet · Network science · Cyber espionage · APT28 · VPNFilter

Introduction

Creating and maintaining the security level expected by businesses is a complicated and cumbersome endeavor, which requires decisions on how to optimally use the available resources. Therefore, there is a need for precise inputs to make accurate outputs available when, where, and how to use them for which purpose. One of the essential mandatory tasks is to know threat agents, their capabilities, and applied tools, as they are the source of threats (and risks).

In the area of information security, risks happen in the physical and in the logical world, which may be in interrelation. Regarding this fact, threat agents may be categorized as (1) human, (2) environmental, (3) natural, and (4) artificial intelligence (abbreviated as AI). The various threat agents turn up as an attacker if a threat materializes. In the cyber world, threats always originate to humans as they create

✉ Tamas Szadeczky
szadeczky.tamas@uni-nke.hu; szadeczky@mail.muni.cz

[1] Doctoral School for Safety and Security Sciences, Obuda University, Budapest, Hungary

[2] Cybersecurity Research Institute, National University of Public Service, Budapest, Hungary

[3] Faculty of Law, Institute of Law and Technology, Masaryk University, Brno, Czech Republic

and use tools. However, as AI evolves, so turns to be a threat agent. Therefore, in cybersecurity, an attacker is a real person, a group of human beings or an AI entity who or which tends to cause damage by full or partial service disruption on a targeted system or to cause direct harm in the physical world (e.g., in industrial control systems) or to obtain unauthorized information.

From an organizational perspective, there are outsider and insider human threat agents who may be malicious (who act deliberately) or non-malicious (who act unintentional, e.g., as a cause of lack of knowledge).

As per Siciliano (2011), an IT security expert at McAfee who has classified technically qualified, malicious actors for the cyber world, there are (1) Black Hat Hackers, (2) Script Kiddies, (3) Hacktivists, (4) State-Sponsored Hackers, (5) Spy Hackers and (6) Cyber Terrorists. From now on, they are marked as attackers.

For an attacker, there is a choice to be made about which tool or tools he or she wants to use. There are tools available to use from simple ones to remarkably robust and professional ones. Due to a study created and published by Trend Micro (2012), there were already various possibilities for attackers in the black market on Darknet:

- Dedicated servers may have been rented with multiple capabilities and safeguard for different purposes (US$0.50–US$2.000) (Trend Micro 2012, p. 3),
- Targeted DDoS service (Distributed Denial of Service) was available for one day (US$30–US$70) or even for one-month (US$1.200) interval (Trend Micro 2012, p. 8),
- Sending spams in an email, SMS, ICQ and Skype for targets (e.g., “cheap email services” sent 1,000,000 emails for US$10) (Trend Micro 2012, p. 11),
- Botnet infrastructure’s capabilities may have been used, e.g., in the case of 2000 bots for US$200 (Trend Micro 2012, p. 12).

With the application of tools, one primal motive of threat agents is destruction. Inspecting the structure of the Internet (like most networks), it tends to represent the characteristics of scale-free networks (Barabási and Bonabea 2003). The main advantage of such network is to be robust to survive random failure as it is more likely to remain complete and not to fall apart, while its main disadvantage is to be more vulnerable to targeted attacks (Barabási 2001). If enough nodes with a high number of connected nodes are eliminated, the network falls into disjoint parts. These partitions may work onward, but the whole network ceases to operate as a functional unit. Due to these facts, targeted attacks may also take huge impacts at national critical information infrastructure to cause harm for a state or an international entity.

Beside destruction, another common aim of cyber-attacks is to obtain unauthorized information with a conventional technique applied by attackers to gather information for illegal, exploitative methods. The act of collecting classified information or trade secrets without the permission of the owner is called cyber espionage. Its purpose may be some beneficial gathering which can be martial, economic, financial, political, depending on its nature. There is a clear fact that stolen data may contain confidential technical information as well as personal data that is shown by a study created by Ponemon Institute, LLC and supported by IBM Security (Ponemon Institute LLC 2017). This kind of data is sellable on the black market, while a data breach causes a definitive loss for data controllers and data processors.

As per the European Union Agency for Network and Information Security's (ENISA) Threat Landscape Report 2018, "cyber espionage is more a motive than a cyberthreat. It has been maintained mainly because it unites almost all of the other cyberthreats" (ENISA 2019, p. 25). It "typically targets industrial sectors, critical and strategic infrastructures across the world including government entities, railways, telecommunication providers, energy companies, hospitals and banks" (ENISA 2019, p. 107).

Most of the cyber-attacks against information systems, services, or critical information infrastructure originates to different networks, the so-called Botnets, made from infected end-points or network devices. A Botnet tends to start various attacks like distributed denial of service (DDoS) and spamming for purposes like knock-out its target or cyber espionage.

For cyber espionage, various data exfiltration technics exist, like a keylogger, screenshot, camera-shot, adware, trojans, information stealing software and even cookies to capture (personal) data, nonetheless, which are perfect instruments. Capabilities provided by the before mentioned tools commonly controlled by Botnets. A wide range of platforms are affected by those risks: Microsoft Windows, Linux, Mac OS, even mobile environments and as well as network devices and Internet of Things (IoT) devices.

The primary objective of this study material is to analyze and categorize Botnets structure, capabilities in general and examine Botnets used for cyber-espionage. We aim to characterize specific parameters for those Botnets.

General review of Botnets

The infrastructure used by attackers is on a broad scale, between a fully manual alone system and a fully automated system that contains hundreds and thousands of nodes. Botnets are the latter, more precisely, they are groups of nodes (endpoints or network devices) on the Internet which use resources of the infected nodes without any knowledge or consent of their owners for illegal activities.

The advantage of the attackers' perspective is the fact that, if a malicious code makes the correspondent network entity part of a Botnet, its storage, computational capacity, processed data, and networking resources are available for the network. Furthermore, local network resources are potentially reachable through these nodes. Due to their functionalities and the type of the attacks, ENISA (European Union Agency for Network and Information Security) has categorized Botnets as the most dangerous threats (ENISA, n. d.). The aim of the application of such tools like Botnets, as well as the current technological capabilities, determine the architectural attributes of them.

Architecture

There are various elements in the structure, capabilities and technical implementation of Botnets that makes them almost unique, but in general, there is always a botmaster (or botherder), one or more Command and Control (C&C or C2) servers and at least one (but typically thousands or millions) controlled node (bot). A bot is an agent on infected nodes to perform received commands, while it tries to stay hidden from anti-malware protections.

The botmaster is the leader for the whole Botnet. In the case of Cybercrime Infrastructure as a Service, typically only a subpart of the Botnet's nodes may be partially controlled by a tenant. The command set available for the tenant tends to be a subset of the whole command set. Effectively, whoever controls the Botnet at a particular time, he or she is the real attacker.

C&C servers maintain the connection with bots, and they manage them. The way of the links between C&C servers and between C&C servers and bots specify the architecture of a Botnet. Considering the implementation of Botnets, there are centralized (or hierarchical), decentralized (or peer-to-peer, abbreviated as P2P) and hybrid Botnets (Table 1).

The knowledge of a Botnets' structure gives the possibility of more effective defensive capability, and even it gives the chance of targeted fightback and switch-off. There are four structures differentiated (Dagon et al. 2007): (1) Erdős-Rényi model, (2) Watts-Strogatz model, (3) Barabási scale-free model and (4) P2P model. It has been proved that some Botnets' structure is corresponding to the scale-free network structure (Dagon et al. 2007, p. 5). As stated in *Introduction*, the main disadvantage of the scale-free network is to be more vulnerable to targeted attacks, which may be utilized by active defending mechanism and during a switch-off action by agencies and telecoms.

Centralized

In the case of centralized Botnets, the control of bots has a static nature. This nature means a predefined number of C&C servers with predefined reachability and functionality. C&C servers may be found based on IP addresses or DNS queries by bots

Table 1 Botnets' architecture

Type	C&C servers
Centralized	Centralized Botnets have a fixed number of C&C server(s), as there may be one or more C&C servers in a flat array or a hierarchical arrangement In the case of hierarchical server arrangement, the number of layers increases complexity, while the number of servers in each layer influences load balancing and redundancy
Decentralized	There is no differentiated C&C server. Thus each bot may fill this role in the correspondent network
Hybrid	There are dedicated C&C servers which work in decentralized, peer-to-peer mode

Source Authors

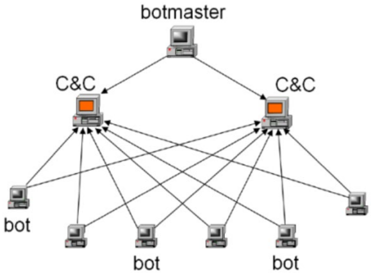

Fig. 1 Architecture of centralized Botnets. *Source* Wang et al. (2007)

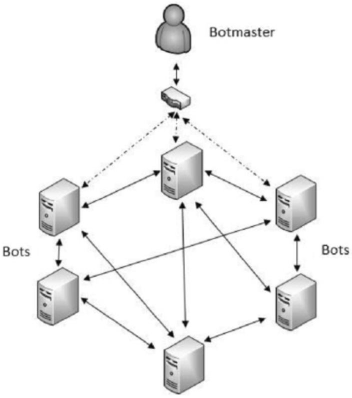

Fig. 2 Architecture of decentralized Botnets. *Source* Hyslip and Pittman (2015, p. 12)

which are hardcoded in agent's code. The most common client–server communication protocols are Hypertext Transfer Protocol (HTTP) and Internet Relay Chat (IRC). Bots may get new control information via the pull or push approach. Pull technology means that bots initiating requests to servers, while push technology means that servers are starting information updates to clients. Using centralized Botnet has a high risk of the identification of bots, C&C servers, or the correspondent botmaster.

A few examples for this category are AgotBot, RBot, and Zeus (Fig. 1).

Decentralized

In decentralized Botnets, there is no specific C&C server nominated. Therefore, such a Botnet works in P2P mode. Each bot registers the number of available bots in its surroundings, while it continually observes new bots, as well as it gets (pulls) and gives forward (push) the control information.

P2P functioning mode gives a high complexity for Botnets because of the application of dynamic routing methods to create and operate such a network. Distracting P2P protocols may cause the network to be partitioned or even to be completely non-functioning.

A few examples for this category are Storm, Nugache, and Conficker (Fig. 2).

Hybrid

Hybrid Botnets synthesize the advantages of the centralized and decentralized architecture of Botnets. This mixed architecture means that C&C servers have a structure of decentralized networks and bots connect to C&C servers in the way of a typical client–server model. With this implementation, the risk of identification and elimination of the whole Botnet reduced significantly. If a C&C server has been disqualified, only the controlled bots would be affected, which is only a subset of the entire network (Fig. 3).

Network protocols

In 2016, IBM X-Force® Research created a study in which IRC, HTTP, P2P, and Tor had been marked as the most often applied protocols (IBM Corporation 2016, p. 6). In contrast with solutions employed at the beginning of the Internet, cryptography is broadly used in the communication of Botnets, with the application of encryption and steganography algorithms. With their usage in various levels of the Transmission Control Protocol/Internet Protocol (TCP/IP) model, the efficiency of detection capabilities is brought down (Acarali et al. 2016, pp. 6–10). Furthermore, the dynamic nature in communication causes static IP reputation and blacklist-based defense solutions unusable. Fast flux is one way of the available technics to play these controls off (IBM Corporation 2016, p. 14).

Capabilities

Botnets may have one or more skills. The more important ones are the followings (IBM Corporation 2016, pp. 15–18):

- With DDoS attacks, the botmaster makes the target or targets unavailable to its intended users disrupting its or their services with regular or illegal requests attempting to overload systems and prevent some or all legitimate requests from being fulfilled;
- Botnets with spyware capability access to processed (stored, computed, communicated) data that may contain personal data on bots themselves or bots' local networks;

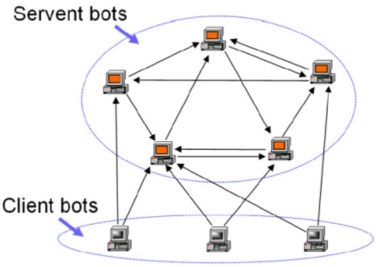

Fig. 3 The hybrid architecture of Botnets. *Source* Wang et al. (2007)

- Botnets may send unsolicited messages via email infrastructure (aka. spams), phone systems or any other messaging systems (aka spims);
- With fraud capability, fake services and their contents are served as it would be legitimate;
- Cryptocurrency mining (aka crypto-mining);
- Self-propagation.

All the attacking capabilities (spyware, spamming, crypto-mining, DDoS, etc.) are significant for botmasters. Apparently, the most spectacular is DDoS. In 2015, Akamai published its analysis about XOR DDoS Botnet in that the correspondent Botnet has 150+ Gbps aggregated network bandwidth (Akamai 2015).

Some attacking capabilities may be applied from the beginning, and some of them may be added with time with the update capability. Therefore update, self-propagation and self-preservation are essential features, too, and they concern each other.

In 2018, researchers defined the four-state SIRS (Susceptible-Infected-Recovered-Susceptible) model to describe the status of Botnets (Kudo et al. 2018, pp. 102–103) (Fig. 4).

Furthermore, they determined that Botnets with self-development characteristic has vulnerability identification and exploitation capability, which makes them more robust and resilient (Kudo et al. 2018, p. 109).

Multi-staged and modular threats, as per ENISA, has the following elements of known capabilities (ENISA 2019, pp. 130–131):

- Self-propagates,
- Self-destructs,
- Communicates anonymously,
- Behaves persistently,
- Obfuscates the origin,
- Downloads payloads and
- Installs payload in memory.

Grouping of Botnets

Considering the given parameters mentioned before, there are some Botnet grouping possibilities available. They may be grouped by architecture, protocols, and capabilities. Inspecting of the operating environments of Botnets, some more parameters

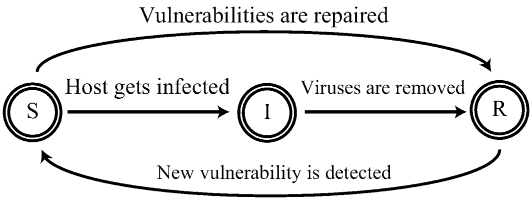

Fig. 4 SIRS model. *Source* Kudo et al. (2018, p. 103)

may be added as (1) effectiveness, (2) average available bandwidth, (3) efficiency and (4) robustness (Dagon et al. 2007, p. 2).

The following picture illustrates a possible way of grouping by architecture and protocols (Fig. 5).

Lifecycle

Considering the operational mechanism of Botnets, there are five phases differentiated (Feily et al. 2009, pp. 268–273):

1. Beginning of infection: The botmaster starts to infect network nodes via at least one attack vector with the exploitation of contained vulnerability or vulnerabilities.
2. Second injection: After successful infection, nodes start to download the agent's code.
3. Connection: Each agent connects to one of the C&C servers.
4. Command and Control: C&C servers relay the commands of the botmaster to bots, for example, to take part in an attacking campaign.
5. Updates and maintenance: Bug repairs and new features may be created and sent to bots which install updates. Sometimes botmaster activates sleeping mode temporarily or a complete switch-off status command for the whole or partial network.

Application of Botnets

In the phase of Command and Control of the lifecycle above, a Botnet may already be used as a tool to carry out attacks. Based on the model of cloud services, *Cybercrime as a Service* model is also available as a business model to make infrastructure, services, tools including Botnets available for attackers. Its main subcategories are (McAfee 2013):

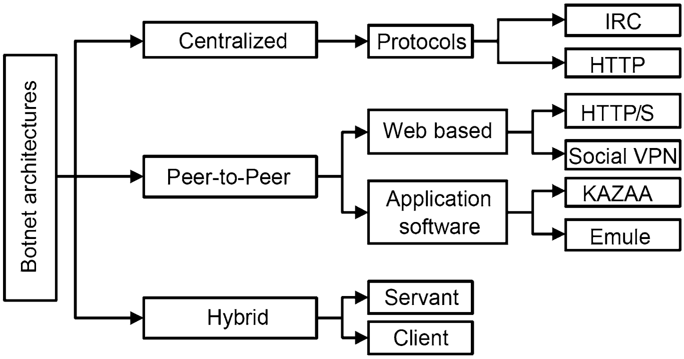

Fig. 5 Botnets grouped by architecture and protocols. *Source* Karim (2014)

- Crimeware as a Service is used for identification of vulnerabilities and to create an exploit specifically for them. There may be available such vulnerabilities which are not well-known publicly. Main tools available through this type of service are APTs (Advanced Persistent Threats), rootkits and ransomware, as well as droppers, keyloggers, and even hiding tools (e.g., cryptor, polymorphic solutions). There are tools for hardware attacks, too.
- Cybercrime Infrastructure as a Service makes infrastructure elements (clients and servers) available. Clients are used for various attacks (e.g., DDoS), while on servers, resources (including personal data) are achievable through pre-identified vulnerability.
- Hacking as a Service is a service model for the whole attacking process. Therefore it may be outsourced entirely. The "service provider" plans and performs attacks as clients' demands to disrupt specific service, process, or to gather information.

Considering this categorization, Botnets or part of Botnets may be rented, and in this case, they belong to the category of Cybercrime Infrastructure as a Service. Attackers may also use Botnets through Crimeware as a Service and Hacking as a Service type of activities, but it depends on their specific operations.

The applied architecture, network protocol, technical solutions, capabilities discussed in this chapter, and even the purpose of Botnets' usage has evolved through the years. In the following section, we discuss their advancement.

Evolution of Botnets

The first Internet worm was created in 1988 by one of the Cornell University's graduate students, namely Robert Morris, Jr. It has limited C&C capabilities which were self-propagation via a few attack vectors, and its agents were able only "to call home," i.e., to notify its C&C server. It was born without any malicious intent, but it caused an adverse effect in operation of affected computers. The Morris worm was followed by continuous development (Ferguson 2010) as we describe in the followings.

The history of Botnets starts in 1999 with the Sub7 trojan and the Pretty Park worm. They implemented a centralized architecture, applying the IRC protocol. In 2000, GTbot arose as a "further development" of mIRC client. In 2002, SDBot was already created in C++ and even it was sold by its creator(s) to gain financial benefits, while Agobot was the first to have a modular structure and it was able to launch an attack in phases (Fig. 6).

In 2003, Spybot was born. It had been created on the bases of SDBot with further capabilities included to make espionage available. It had the keylogging and data mining spyware capabilities, and it was able to send spammed instant messages or spims. Rbot was the first Botnet to launch DDoS attacks, and even it could use SOCKS proxy, while it was the first to apply of compressing and cryptographic algorithms to avoid detection.

In 2004, Polybot applied polymorph algorithms first to make its code dynamic. Due to the fact of "polymorphic viruses can mutate their decryptors to a high number

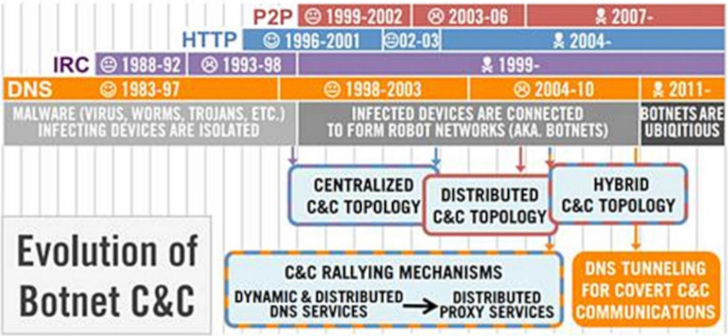
P2P
1999-2002
2003-06
2007-
HTTP
1996-2001
02-03
2004-
IRC
1988-92
1993-98
1999-
DNS
1983-97
1998-2003
2004-10
2011-
MALWARE (VIRUS, WORMS, TROJANS, ETC.) INFECTING DEVICES ARE ISOLATED
INFECTED DEVICES ARE CONNECTED TO FORM ROBOT NETWORKS (AKA. BOTNETS)
BOTNETS ARE UBIQITIOUS
CENTRALIZED C&C TOPOLOGY
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

Fig. 6 Evolution of Botnets. *Source* OpenDNS as cited in Cantón (2015)

of different instances that can take millions of different forms" (Szor 2005, p. 245), Polybot had many variants to mess up anti-malware protection. Botnets had finally turned to HTTP and ICMP protocols from IRC. Furthermore, they start to use the Secure Sockets Layer (SSL) protocol to communicate through an encrypted channel.

In 2006, Zeus arose with spyware capabilities, and through years, some version updates were applied, as well as some new features has been included. Even, Zeus was the first that may be rent easily in Darknet.

> Even though many criminal activities take place on this network, the Darknet is not criminogenic. Many of these activities can also exist outside of it (Mirea et al. 2019, p. 114)

Due to the static nature of C&C servers, defenders filtered them more efficiently based on IP reputation. As an answer, Cutwail in 2007 than Conficker in 2008 applied name generation technic for C&C servers. Conficker created 50,000 alternative names daily.

With times, technical abilities and motivation have changed from destruction to gathering financial or any other benefit. This had been realized in more and more data breaches in where personal data is affected (e.g., bank accounts, credit cards) increasingly, and, for example, crypto-mining without the consent of resource owners. Therefore, Gemini, as a revived Botnet in 2010, then AnserverBot in 2011, was able to use smartphones to run their agents. Likewise, in 2011, Ramnit was able to steal bank accounts without any difficulty (IBM Corporation 2016, p. 3). In the case of a smartphone, botmasters have to use agents' resource with caution, because their hardware resources like storage and processing are restricted, and excessive usage may quickly discharge the battery. Due to the hectic way of the Internet connection of the infected phones, C&C communication may also be a problem (Chen et al. 2017, pp. 270–271).

Utilizing possibilities given by social networks, socialbots are controlled by an independent, robust C&C server infrastructure offered by social networks via encrypted or steganographic messages (Boshmaf et al. 2013, p. 556).

In "The inside story on Botnets" report published in 2016 by IBM Corporation, the Internet of Things was mentioned at first in connection with Botnets as thingbots (IBM Corporation 2016, p. 3). In 2017, “The weaponization of IoT devices” report published by IBM Corporation again, the importance of thingbots had significantly increased. As a piece of evidence, Mirai started its amuck in 2016 (IBM Corporation 2017, p. 2).

In 2018, VpnFilter one of the multistage and modular Botnets received an update with seven new features, for example, network discovery and obfuscating the source of the attack. Furthermore, it had been proved that network devices were also affected. Initially, it targeted the Modbus protocol. Another Botnet, Hide and Seek (HNS), also received an update to reach out Android devices, while initially, focused on IP cameras (ENISA 2019, p. 60).

> Recent trends in multi-staged and modular malware attacks reveal how this type of attack is becoming increasingly sophisticated, versatile, and persistent. […] It uses different vectors, depending on a pre-assessment conducted to the victim’s infrastructure, to initiate the attack. (ENISA 2019, p. 130)

As information is valued higher and higher over time, so turn the destruction and espionage capabilities more and more critical. Considering the technological capabilities that Botnets own for a while, they are applied long ago to carry out sophisticated tasks. Regarding cyber espionage, (1) state espionage (when state actors are involved) and (2) industrial espionage (when commercial actors are concerned) may be differentiated as a high categorization (ENISA 2017, p. 7), while threat agents may be cybercriminals, insiders, states, corporations, hacktivists, cyber terrorists, and script-kiddies.

The APT28 group

From the operating cyber espionage actors, we have the APT28 codenamed group chosen. It owns some alternative designations as Swallowtail, Fancy Bear, Pawn Storm, Sofacy Group, Sednit, Strontium, and Tsar Team. This group has been active since at least January 2007 (Symantec 2018), and as a suspicion, it is most probably sponsored by the Russian government. The leading indicators are the consistent use of Russian Language and, the malware’s compile times corresponded to work days in Moscow’s time zone. Undoubtedly, as researchers have shown until 2014, its primary interests are in the Caucasus, Eastern European Governments and Militaries, NATO and Other European Security Organizations including the European Defense Exhibitions. In the Caucasus, its particular target is Georgia with the Georgian Ministry of Internal Affairs and the Georgian Ministry of Defense, and even, the journalist covering this area. In Eastern Europe, its targets were located in the Baltic, Poland, and Hungary (FireEye 2014).

In the following subsections, we will analyze APT28 group’s recent activities over the years. The group has carried out cyber espionage with various motives (e.g., political, martial), methods (e.g., phishing for injection) and tools (e.g., Botnets with different capabilities).

Operation Pawn Storm from 2004

It is believed that Operation Pawn Storm revealed by Trend Micro in 2014 is active from 2004 to nowadays. Its targets are some of the world's largest political organizations, such as the U.S. Senate and Democratic National Committee (DNC) (Anomali 2019).

Attack methods included spear-phishing utilization with creating fake Outlook Web Access (OWA) login pages for credential phishing, and even, XAgent variants iOS malware were created for espionage attacking mobile devices (Trend Micro 2016).

Through the operation, the targets were the NATO and the organization's member states, Government, Military and Media entities in the US, Government, Military and Media entities of US allies, Russian dissidents/political opponents of the Kremlin, Russian citizens across different civilian industries and sectors, Ukrainian Activists, Ukrainian Media, Ukrainian Military and Government, Governments in Europe, Asia and the Middle East (Trend Micro 2016).

In 2017, Trend Micro found that the group was targeting an unnamed Non-Governmental Organization (NGO) in the Netherland and even the United States Senate with phishing emails designed to steal user credentials (Trend Micro, 2018a, b).

Operation RussianDoll in 2015

In 2015, APT28 did a limited APT campaign by exploiting a zero-day vulnerability in Adobe Flash Player (CVE-2015-3043). Targeted users were required to click on a link leading to a group-controlled website. After a Windows privilege escalation vulnerability (CVE-2015-1701) was utilized to install malware. FireEye revealed it in April 2015 (Anomali 2019; FireEye 2015).

> This exploit delivers a malware variant that shares characteristics with the APT28 backdoors CHOPSTICK, and CORESHELL malware families [...] (which) uses an RC4 encryption key that was previously used by the CHOPSTICK backdoor. Moreover, the C2 messages include a checksum algorithm that resembles those used in CHOPSTICK backdoor communications. Also, the network beacon traffic for the new malware resembles those used by the CORESHELL backdoor. [...] The target firm is an international government entity in an industry vertical that aligns with known APT28 targeting. (FireEye 2015)

Operation Fancy Bear in 2015

In Summer 2016, CrowdStrike Intelligence analysts were investigating a suspicious Android Package (APK). "Initial research identified that the filename suggested a relationship to the D-30 122mm towed howitzer, an artillery weapon first manufactured in the Soviet Union in the 1960s but still in use today" (CrowdStrike 2016), therefore, they made in-depth reverse engineering with the following results:

- From late 2014 and through 2016, the XAgent was covertly distributed on Ukrainian military forums as a legitimate Android application developed by Ukrainian artillery.
- The original application aimed more rapid targeting process for the Soviet-era D-30 Howitzer employed by Ukrainian artillery forces.
- Probably, over 9000 artillery personnel had been using the application in the Ukrainian military.

Other operations in 2016

The group did a large-scale phishing campaign that targeted the US Democratic political party from March to November. In October and November, WikiLeaks published 34 instances of stolen email conversations. In June, the US Democratic National Committee (DNC) announced that it had suffered a network compromise. Evidence proved two separate breaches, one conducted by APT28 and the other by another Russian group, APT29 (aka Cozy Bear). During the DNC's breach, documents were stolen, which were later published by WikiLeaks, too (Anomali 2019).

In this year, the Organization for Security and Cooperation in Europe (OSCE) and Germany's Christian Democratic Union (CDU) also suffered breaches. In the case of CDU members, the objective was to steal account credentials with spear phishing emails which had a malicious, macro-based document. Infection was made by the custom Gamefish (Sednit) backdoor, and Responder open source tool to move laterally on the network (Anomali 2019). Even, the World Anti-Doping Agency (WADA) announced a network breach affected athlete medical data that had been accessed by APT28 (World Anti-Doping Agency 2016).

Operations in 2017

At the beginning of the year, multiple International Olympic Winter Sports Federations were targeted, for example, the European Ice Hockey Federation and the International Ski Federation, probably as a response to Russia being banned from the 2018 Winter Olympics (Anomali 2019).

In at least July, a campaign affected the hospitality sector with targeting individuals staying in hotels throughout Europe and the Middle East started. The group sent spear-phishing emails, and used the EternalBlue exploit, associated with the US National Security Agency (NSA), to move laterally on the network (FireEye 2017).

Operations in 2018

Since December 2017, its malware had been inside the "Informationsverbund Berlin-Bonn" (IVBB) network, and have present until the end of February 2018. This network is used by the German federal chancellery, the German parliament, federal ministries, the Federal Audit Office, and other security entities in Berlin and Bonn (Anomali 2019).

In early February 2018, Palo Alto Unit 42 researchers identified a new cyber espionage campaign of APT28 group targeting Ministries of Foreign Affairs with Microsoft Excel documents containing malicious macros distributed. The documents containing a loader trojan had been created with Luckystrike, an open source office document generating tool. The loader installed and ran the primary malicious variant of the group's custom Carberp (SofacyCarberp) backdoor. It gathered system information and sent it to a C&C server to be able to choose the appropriate payload to download (Palo Alto 2018).

In March, it continued the phishing emails with changed theme and malware. On March 12 and 14, distributed phishing emails to an unnamed European government agency were identified with infected Microsoft Word document titled "Defence & Security Conference Agenda" attachment, while in May, one of the most extensive campaigns reported about a Botnet consisting of approximately 500,000 devices as a result of VPNFilter malware infection. Cisco Talos researchers found interrelation between VPNFilter and BlackEnergy that targeted the Ukrainian power grid in the winter of 2015–2016 (Anomali 2019).

By June 2018, the group launched a new phishing campaign to distribute Zebrocy by malicious Microsoft Office attachments. Zebrocy is a loader with the capability of downloading different malware and has three components as (1) a Delphi downloader, (2) an AutoIt downloader, and (3) a Delphi backdoor. However, it is also capable of downloading DealersChoice platform. Then these first-stage droppers download the XAgent malware (Anomali 2019).

In August, Microsoft researchers had discovered to have registered domains associated with phishing campaigns by Microsoft researchers. One appeared similar to the domain name of the International Republican Institute (IRI), another impersonated the Hudson Institute, and the remaining for attempted to masquerade as domains that would be part of the US Senate's IT infrastructure (Microsoft 2018).

By September, it was clear that APT28 conducts the malicious activity with a new custom rootkit named LoJax after the anti-theft software LoJack. LoJax is unique in that it is the first rootkit observed in the wild to target the Unified Extensible Firmware Interface (UEFI) of a machine that connects software to the operating systems. In September, VPNFilter got updated features as third-stage modules with (Anomali 2019).

VPNFilter Botnet

From the many tools that are discussed in the previous chapter and behave as Botnets, we have chosen VPNFilter to be analyzed. In July 2018, security researchers described VPNFilter as sophisticated malware affecting 500,000 networking devices. Initially, it attacked Ukrainian hosts but spread over 54 countries very quickly (ENISA 2019, p. 131). It is a multistage and modular malware that "can steal and harvest information, intercept or block network traffic, monitor Supervisory Control and Data Acquisition (SCADA) protocols, and render infected routers inoperable" (Trend Micro 2018a, b).

As per Cisco Talos researchers (Cisco Talos 2018), VPNFilter had three stages, which are shown in the following kill chain diagram create by ENISA (2019) consequently Installation, Command & Control and Actions on Objectives (Fig. 7).

As Cisco Talos (2018) researchers had found, in stage one, it infected a device and gained persistence with the primary purpose to enable the deployment of the phase two malware. Multiple redundant command and control (C2) mechanisms were utilized that made it "extremely robust and capable of dealing with unpredictable C2 infrastructure changes" (Cisco Talos, 2018). As per Sophos' investigation (2018), stage one relied on connecting either to one of twelve hardcoded Photobucket URLs, or the Toknowall website. From a chosen image an encoded form of the command-and-control server's IP address was fetched from the image's EXIF metadata.

> Most of the Photobucket galleries used by the malware authors were named after famous female entertainer. […] The malware code indicated that it should query for its command-and-control server address every 10 to 19 seconds, but we observed that it performed an HTTP HEAD request against various pages on Photobucket at a much slower rate, with a random delay of 2 to 20 minutes between the attempts. If the Photobucket URLs fail, it tries to reach Toknowall C2 website. (Sophos 2018)

The stage two malware had the capabilities of an intelligence-collection platform, such as file collection, command execution, data exfiltration, and device management, as well as some versions possessed a self-destruct capability that overwrites a critical portion of the device's firmware and reboots the device.

There were multiple stage three modules as plugins for stage two malware with additional functionality, such as packet sniffer and communications module allowing communication over Tor.

The following picture shows the progression (Fig. 8).

As researchers found, VPNFilter's additional modules were (Trend Micro 2018a, b):

- htpx: Redirect and inspect unencrypted traffic traversing through compromised devices.

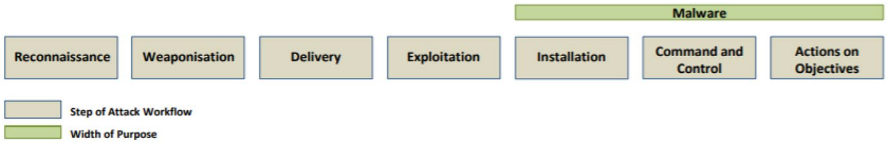

Fig. 7 VPNFilter kill chain. *Source* ENISA (2019, p. 131)

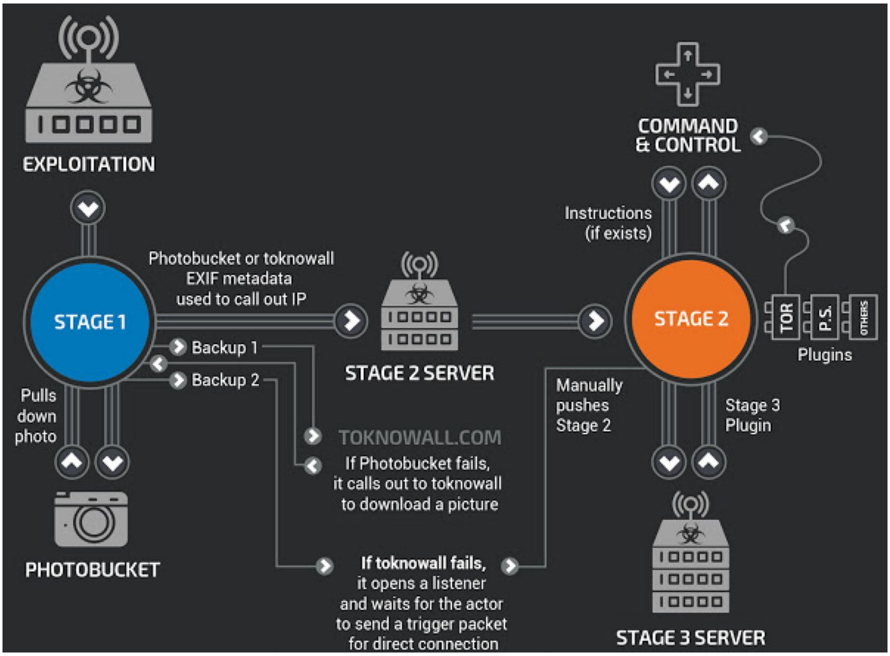
EXPLOITATION
COMMAND & CONTROL
Instructions (if exists)
Photobucket or toknowall EXIF metadata used to call out IP
STAGE 1
STAGE 2 SERVER
STAGE 2
TOR
P.S.
OTHERS
Plugins
Backup 1
Backup 2
Pulls down photo
Manually pushes Stage 2
Stage 3 Plugin
TOKNOWALL.COM
If Photobucket fails, it calls out to toknowall to download a picture
PHOTOBUCKET
If toknowall fails, it opens a listener and waits for the actor to send a trigger packet for direct connection
STAGE 3 SERVER

Fig. 8 VPNFilter's workflow. *Source* Cisco Talos (2018)

- ndbr: Enable remote access to the device, turn it into a Secure Shell (SSH) client or server. It can transfer files via Secure Copy (SCP) protocol and to perform as a network scanner to identify hosts and services on a network.
- nm: Perform reconnaissance via a network-mapping and port-scanning tool with searching for specific routers to compromise.
- netfilter: Carry out denial of service by blocking IP addresses related to specific services and applications.
- portforwarding: Redirect traffic from the compromised device to an attacker-specified network.
- socks5proxy: Turn a compromised device into a virtual private network (VPN) server to be able to communicate in an encrypted channel.
- tcpvpn: Enable remote access to internal networks of compromised devices to export data and remote C&C.

Several indicators of compromise (IOC) had been recognized, such as URLs, IPs, and file hashes, as well as Snort rules had been created (Cisco Talos, 2018). Finally, the Federal Bureau of Investigation (FBI) managed to shut down a C&C server used by VPNFilter (Trend Micro 2018a, b).

Conclusion

According to recent statistics and reports from anti-malware companies, the usage of infected computers as attack agents (Botnets) has become more sophisticated in the last two decades. The objectives of the Botnets have become more varied and now include not only destruction purpose, but data leakage, as well as cyber espionage.

In connection with business security and espionage, Mendell (2011) wrote in his book about three paradoxes. The first one is about attitude and limited resources available to security operation. The second paradox "arises from the structure of the information commodity itself. […] Electronic information […] prone to subtle manipulation" (Mendell 2011, p. 4). The third paradox originates to the dynamic nature of today's businesses, as all the environment, economy, clients are changing almost fluently.

Considering the fact of each paradoxes, victims' systems are also more diverse nowadays than 10 years before. In addition to traditional desktop and mobile computers with all sorts of operating systems, smartphones, IoT devices, and any "smart" device can also be infected and used for the goals of the botherders or the tenants. Therefore, the set of attack vectors has firmly grown, and it will probably grow in the future, too.

With this technical advancement affecting critical infrastructure, like banking, public services and similar, with the growth of the value of information, the motives of the attacker have also evolved through the years. From the many influential attacker groups, we have shown the well-documented recent activities of the APT28 group. We have introduced the crucial activities of the group and its VPNFilter Botnet, which proves that even state-controlled (or state-sponsored) cyber espionage is actively using this technique and achieves political, military and economic success with such sophisticated tools like Botnets.

It must be pointed out that the phenomenon is not new, as the traces show, the intelligence agencies are just utilizing modern tools to conduct espionage operations. However, recognizing Botnets' activities is a hard task, and tracing the communication back to their C&C servers and even back to tenants and botmasters is almost impossible in many cases. Without tighter international, private and public sector cooperation, they may do their job fluently.

Acknowledgements This article was supported by ERDF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822). The authors appreciate the encouragement of the network science research group at the National University of Public Service.

Glossary

Advanced Persistent Threat (APT) An advanced persistent threat is an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives

	by using multiple attack vectors (e.g., cyber, physical, and deception) (NIST SP 800-39)
Bot	Computers that are compromised after hackers install malware that give them complete control over the infected machine (Rege 2014)
Botherder or botmaster	An assemblage of bots that have been compromised weeks or months before an attack and can be remotely controlled by the attacker. Cybercriminals then herd the bot network, or issue orders to their bots, directing them to send bogus messages simultaneously to targeted websites, resulting in a DDoS attack (Rege 2014)
Distributed Denial of Service (DDoS)	An attack created by amassing a Botnet to disrupt a targeted site's traffic bandwidth capability, and consume all disk space or CPU time. The site is thus overwhelmed with requests and is slowed down to a crawl, resulting in a DDoS attack (Rege 2014)
Indicators of compromise (IOC)	A technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred (NIST SP 800-150)
Threat	An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss (NIST SP 800-160)
Threat agent or threat source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability (FIPS 200)
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (FIPS 200)
Zero-day vulnerability	A previously unknown hardware, firmware, or software vulnerability (CNSSI 4009-2015)

References

Acarali, D., M. Rajarajan, N. Komninos, and I. Herwono. 2016. Survey of approaches and features for the identification of HTTP-based Botnet traffic. *Journal of Network and Computer Applications* 76: 1–15.

Akamai, 2015. *XOR DDoS Botnet Launching 20 Attacks a Day From Compromised Linux Machines, Says Akamai.* https://www.akamai.com/us/en/about/news/press/2015-press/xor-ddos-botnet-attacking-linux-machines.jsp. Accessed 15 July 2018.

Anomali, 2019. *APT28 Timeline of Malicious Activity.* https://forum.anomali.com/t/apt28-timeline-of-malicious-activity/2019. Accessed 21 February 2019.

Barabási Albert László, 2001. The physics of the web. *Physics World*, pp. 33–38.

Barabási Albert László és Eric Bonabea, 2003. http://barabasi.com/f/124.pdf. Accessed 02 May 2013.

Boshmaf, Y., I. Muslukhov, K. Beznosov, and M. Ripeanu. 2013. Design and analysis of a social Botnet. *Computer Networks* 57: 556–578.

Cantón, D., 2015. *Botnet detection through DNS-based approaches.* https://www.certsi.es/en/blog/botnet-detection-dns. Accessed 01 Aug 2018.

Chen, W., et al. 2017. CloudBot: Advanced mobile Botnets using ubiquitous cloud technologies. *Pervasive and Mobile Computing* 41: 270–285.

Cisco Talos, 2018. *New VPNFilter malware targets at least 500 K networking devices worldwide.* https://blog.talosintelligence.com/2018/05/VPNFilter.html. Accessed 20 Feb 2019.

CrowdStrike, 2016. *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units.* https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/. Accessed 19 Feb 2019.

Dagon, D., G. Gu, C.P. Lee, and W. Lee. 2007. *A Taxonomy of Botnet Structures.* http://faculty.cs.tamu.edu/guofei/paper/Dagon_acsac07_botax.pdf. Accessed 21 June 2018.

ENISA, 2017. *ENISA overview of cybersecurity and related terminology.* https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology. Accessed 17 Feb 2019.

ENISA, 2019. *ENISA Threat Landscape Report 2018.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport. Accessed 17 Feb 2019.

ENISA, n.d. *Botnets.* https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets. Accessed 15 July 2018.

Feily, M., A. Shahrestani, and S. Ramadass. 2009. *A Survey of Botnet and Botnet Detection.* Washington, DC, USA, s.n.

Ferguson, R., 2010. *The Botnet Chronicles A Journey to Infamy.* http://www.trendmicro.co.kr/cloud-content/us/pdfs/security-intelligence/white-papers/wp_botnet-chronicles.pdf. Accessed 10 May 2018.

FireEye, 2014. *APT28: A Window into Russia's Cyber Espionage Operations?* https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf. Accessed 18 Feb 2019.

FireEye, 2015. *Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack.* https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html. Accessed 22 Feb 2019.

FireEye, 2017. *APT28 Targets Hospitality Sector, Presents Threat to Travelers.* https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html. Accessed 23 Feb 2019.

Hyslip, T., and J. Pittman. 2015. A survey of Botnet detection techniques by command and control infrastructure. *Journal of Digital Forensics, Security and Law* 10 (2): 7–26.

IBM Corporation, 2016. *The Inside Story on Botnets.* https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03086USEN&appname=skmwww. Accessed 23 May 2018.

IBM Corporation, 2017. *The Weaponization of IoT Devices.* https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03128USEN&appname=skmwww. Accessed 04 May 2018.

Karim, Ahmad. 2014. Botnet detection techniques: review, future trends, and issues. *Journal of Zhejiang University-Science C* 15 (11): 943–983.

Kudo, T., et al. 2018. Stochastic modeling of self-evolving Botnets with vulnerability discovery. *Computer Communications* 124: 101–110.

McAfee, 2013. *Cybercrime Exposed—Cybercrime-as-a-Service.* http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf. Accessed 01 March 2016.

Mendell, R.L. 2011. *The quiet threat: Fighting industrial espionage in America*, 2nd ed. Springfield, IL: Charles C Thomas Publisher Ltd.

Microsoft, 2018. *We are Taking New Steps Against Broadening Threats to Democracy.* https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/. Accessed 23 Feb 2019.

Mirea, M., V. Wang, and J. Jung. 2019. The not so dark side of the darknet: A qualitative study. *Security Journal* 32: 102–118.

Palo Alto, 2018. *Sofacy Attacks Multiple Government Entities.* https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/. Accessed 23 Feb 2019.

Ponemon Institute LLC, 2017. *2017 Cost of Data Breach Study.* https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN. Accessed 15 Jan 2018.

Rege, A. 2014. Digital information warfare trends in Eurasia. *Security Journal* 4: 27.

Siciliano, R. 2011. *7 Types of Hacker Motivations.* http://blogs.mcafee.com/consumer/identity-theft/7-types-of-hacker-motivations. Accessed 23 July 2012.

Sophos, 2018. *VPNFilter Botnet: a SophosLabs Analysis, Part 2.* https://news.sophos.com/en-us/2018/05/27/vpnfilter-botnet-a-sophoslabs-analysis-part-2/. Accessed 23 Feb 2019.

Symantec, 2018. *APT28: New Espionage Operations Target Military and Government Organizations.* https://www.symantec.com/blogs/election-security/apt28-espionage-military-government. Accessed 18 Feb 2019.

Szor, P. 2005. *The Art of Computer Virus Research and Defense*. Hagerstown, MD: Addison Wesley Professional.

Trend Micro, 2012. *Trend Micro Inc., Russian Underground 101 (Research Paper 2012).* https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf. Accessed 15 Jan 2018.

Trend Micro, 2016. *Operation Pawn Storm: Fast Facts and the Latest Developments.* https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts. Accessed 21 Feb 2019.

Trend Micro, 2018a. *Internet-of-Things (IoT) Security: Developments in VPNFilter and Emergence of Torii Botnet.* https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/internet-of-things-iot-security-developments-in-vpnfilter-and-emergence-of-torii-botnet. Accessed 23 Feb 2019.

Trend Micro, 2018b. *Update on Pawn Storm: New Targets and Politically Motivated Campaigns.* https://blog.trendmicro.com/trendlabs-security-intelligence/update-pawn-storm-new-targets-politically-motivated-campaigns/. Accessed 22 Feb 2019.

Wang, P., et al. 2007. *An Advanced Hybrid Peer-to-Peer Botnet.* http://static.usenix.org/event/hotbots07/tech/full_papers/wang/wang_html/. Accessed 10 Oct 2012.

World Anti-Doping Agency, 2016. *WADA Confirms Attack by Russian Cyber Espionage Group.* https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-attack-by-russian-cyber-espionage-group. Accessed 23 Feb 2019.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.