FEATURE

Cybersecurity Takedowns

A Primer for Success

Information security programs are not easy or totally successful on a global scale. In fact, performing a takedown—that is, successfully removing or blocking malware implemented on a vast scale and/or stopping malicious individuals or organizations that create and disseminate it—is very difficult for many reasons. Examining several cybersecurity response programs, evaluating their levels of success and describing various common malware programs can help reveal methods to help combat cyberincidents.

Malware Response Programs and Operations

World authorities, vendors and many countries have been working together to fight cybercrime and the spread of malicious software with limited success.

Botnet Takedowns

Botnets are malicious software that spread to vulnerable computing devices including desktops, laptops, smartphones, tablets, servers and Internet of Things (IoT) devices. They infect tens of thousands of computing devices and perform a variety of malicious activities—for example, spamming, stealing credentials, redirecting users to alternative websites, spreading malware and conducting click fraud (in which a host is paid when users click the host's ad)—all without the device owner's knowledge.

Figure 1 contains samples of botnet takedowns and provides insight into their levels of success. The takedowns were not all fully successful. In some cases, the malicious actors (i.e., hackers, botnet creators and/or administrators) received leniency because they cooperated with authorities. In one instance, the bot creator was freed because of a loophole in the law (i.e., he did not attack his own country).[1]

Cybercriminal Marketplace Takedowns

A cybercrime marketplace is a place where criminals such as thieves buy and sell stolen goods. It is also a place where malware is sold, software vulnerability information is provided, personal identity information is sold and much more. The Internet has also been used to coordinate many types of cyber-related crimes. Some criminal marketplace takedowns include:

- AlphaBay cybercriminal marketplace had 200,000 users, 40,000 vendors and 250,000 listings of illegal documents, counterfeit goods, malware, computer hacking tools, firearms and fraudulent services.[2,3] The takedown required months of planning and involved the US Federal Bureau of Investigation (FBI), Europol, and law enforcement authorities in Canada, France, Lithuania, the Netherlands, Thailand and the United Kingdom. The site's creator and administrator was Alpha02 (aka Admin), a 25-year-old Canadian citizen living in Thailand. He and his wife amassed numerous high-value assets, including luxury vehicles, residences and a hotel in Thailand. They possessed millions of US dollars in cryptocurrency (which has been seized).

Larry G. Wlosinski, CISA, CRISC, CISM, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL V3, PMP
Is a senior consultant at Coalfire Federal with more than 20 years of experience in IT security and privacy. Wlosinski has been a speaker on a variety of IT security and privacy topics at US government and professional conferences and meetings, and he has written numerous articles for magazines, journals and newspapers.

Figure 1—Botnet Takedowns and Their Success

Botnet	Botnet Description	Takedown Participants	Evaluation of Takedown
ZeroAccess	• Created in 2011 • Included a peer-to-peer (P2P) network • 49 domains were suspected of association with the botnet • Included 18 IP addresses in Europe • Had a command and control (C&C) backup mechanism	FBI, European Cybercrime Center, several high-tech companies including A10 Networks	Partially successful: Authorities took down only 40 percent of its infrastructure, and the takedown affected unsuspecting security monitoring researchers.
Avalanche	• Used to manage mass global malware attacks and money mule recruiting campaigns • Estimated to cause hundreds of millions of euros in damages worldwide • 180 countries were affected	Germany, US Department of Justice, FBI, Europol, Western District of Pennsylvania and global partners	Successful: Five individuals were arrested, 37 premises were searched and 39 servers were seized. Two hundred twenty-one servers were taken offline via abuse notifications. 800,000 domains were seized, sink holed or blocked.
Gamarue/Andromeda	• Distributed 80 malware species to an average of 1 million machines per month • More than 1,500 domain names were seized • Seven C&C servers were sink holed • 223 countries and more than 2 million devices infected	FBI, Germany, Europol, J-CAT, Eurojust and private-sector partners	Partially successful: Charges were dropped after the bot creators helped authorities understand and catch other cybercriminals. The criminals returned US$5,400.
Mirai	• Hijacked millions of IoT devices (including security cameras, home routers, DVRs) • Many sites/devices were forced offline	FBI	Partially successful: Variations exist. Because three bot creators helped the authorities, they received five years' probation, 2,500 hours of community service and were forced to return US$127,000.

Source: Based on Adhikan, R.; "Microsoft's ZeroAccess Botnet Takedown No 'Mission Accomplished'," *TechNewsWorld*, 9 December 2013, *https://www.technewsworld.com/story/79586.html*; Europol, "'Avalanche' Network Dismantled in International Cyber Operation," 1 December 2016, *https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation*; Microsoft Security, "Microsoft Teams Up With Law Enforcement and Other Partners to Disrupt Gamarue (Andromeda)," 4 December 2017

- Hansa marketplace facilitated the sale of illegal drugs, toxic chemicals, malware, counterfeit identification documents and other illegal services. This takedown resulted in the arrest of hundreds of people and was done at the same time as the AlphaBay takedown.[4] The Netherlands National High-Tech Crime Unit (NHTCU) was credited with this successful takedown. The police seized more than 2,500 bitcoins, along with details of over 26,000 transactions. Hundreds of arrests followed because of the information gathered.
- Russian Anonymous Marketplace (RAMP) dealt in all sorts of illegal products (primarily drugs). Russian authorities were able to take this marketplace down, but a clone surfaced a few days later. The clone died out for unknown reasons. A new service called RuTor was advertised as an alternative marketplace.[5]
- The "In Fraud We Trust" marketplace was a partially successfully shut down. Authorities failed to arrest everyone involved. It had 10,901 registered members. The shutdown was led by the FBI, but many other countries were involved. Of the 36 indicted, only 13 were arrested. The marketplace sold credit card numbers, taxpayer numbers, compromised accounts and material to create counterfeit cards.[6]

Today, multiple marketplaces remain to be taken down, but, in some cases, authorities have acted against them.[7] The frustrating part for law

enforcement authorities is that because there are so many criminal organizations, any void opened by takedowns is generally quickly filled by other perpetrators. It is an ongoing challenge for law enforcement around the world.

Other Cyberresponse Successes

Aside from bots, botnets and criminal marketplaces, there are other types of malicious activity on the Internet. The following information details other ways that criminals misuse the Internet for personal gain and why it is important to address cybercriminal activity. Instances of malicious cybersoftware and corresponding takedowns include the following:

- In December 2016, 34 teenagers were arrested by the FBI, Europol and law enforcement in 12 European nations for conducting distributed denial of service (DDoS) attacks for fun.[8] The teenagers paid for software that would flood websites and servers with massive amounts of data that left them inaccessible to users.
- In April 2017, Interpol, working with countries (China, Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam) and private organizations (Booz Allen Hamilton, British Telecom, Cyber Defense Institute, Fortinet, Kaspersky Labs, Palo Alto Networks, Trend Micro), took down 270 websites and about 8,800 command and control (C&C) servers that hosted malware, launched DDoS attacks and more.[9] Three suspects were arrested in Spain and two were arrested in the United Kingdom.
- In May 2017, Russia's Ministry of Internal Affairs with the help of the Group-IB (a vendor of threat intelligence) arrested the Cron gang of 20 for running a mobile Cronbot, a banking trojan, and fake apps and websites. Their malware infected more than 1 million Android devices to make transfers and intercept bank text messages. The gang opened more than 6,000 accounts and made more than US$890,000.[10]
- In July 2017, two Latvian citizens were arrested by the US Department of Justice (DOJ) and the FBI for running the "VisuTotal-for-Crooks" services, which included a software tool (Scan4You) that checked malware for visibility to antivirus software.[11, 12, 13] The results of this crime service were the theft of 40 million credit and debit card numbers, approximately 70 million addresses, phone numbers, and other personal information. It caused one retailer US$292 million in losses. The software was also used in the development of Citadel. The hackers were sentenced to 14 years in prison.
- In August 2017, technology organizations (Akamai, CloudFlare, Flashpoint, Google, Oracle Dyn, RiskIQ, Team Cymru and others) took down the WireX Android botnet that was hosted by the Google Play store. The malware that was associated with approximately 300 applications (apps) was hidden in media players, ringtones and storage managers.[14, 15] The botnet had spread to users in more than 100 countries.

> "THE FRUSTRATING PART FOR LAW ENFORCEMENT AUTHORITIES IS THAT BECAUSE THERE ARE SO MANY CRIMINAL ORGANIZATIONS, ANY VOID OPENED BY TAKEDOWNS IS GENERALLY QUICKLY FILLED BY OTHER PERPETRATORS."

Key Problem Areas

Despite these successes, challenges persist and often prevent or deter complete success, e.g., in the areas of people (and organizations), enforcement, processes and techniques, and technology. There are some problems/challenges associated with taking down bots, botnets and cybercrime marketplaces.

Bots and Botnets

Challenges in taking down bots and botnets are numerous and include:

- **Inadequate coordination among software vendors or Internet malware researchers**—It is better to stop bad behavior than let it propagate out of control. To that end, there should be specially focused groups dedicated to consistency in providing software solutions.
- **Failure to update antivirus (AV) software in a timely manner or consistently across vendors**—Because updating AV signatures is a never-ending task, system owners find it tedious and unprofitable. However, patching system software and updating AV systems in a timely manner is critical, especially if there are zero-day vulnerabilities.

- **Keeping up with alerts and commercial software patches**—Not all organizations are committed to staying informed about security alerts and implementing software security patches. This lax attitude may leave an enterprise open to system compromises, malware infections, data breaches, etc.
- **Number of hackers**—The number of hackers continues to grow because malware tools have become easy to use, and hackers provide each other with training and assistance.
- **Threat of DDoS attacks**—Because Internet service providers (ISPs) provide services to many customers, attacking ISPs (e.g., via DDoS attacks) may affect the productivity, reputation and profit of all users who share common services (e.g., cloud products and platforms).
- **Failure to take down malware completely or thoroughly**—Online malware takedowns may miss devices that are not powered on or not included by activity analysis, thereby leaving unremedied devices. Follow-up takedowns are needed to increase the percentage of eradication.
- **Compromised computer systems**—Content management systems (CMSs) (e.g., WordPress) are common targets for hackers because these websites are easily created but not always maintained (i.e., updated or patched).
- **Cyberthreats on the IoT**[16]—Devices considered to be in the category of IoT are often developed with almost no thought to security. Many devices have been compromised and are used as part of a botnet for DDoS attacks. IoT technology has introduced new threats to personal privacy and sometimes enterprise information.
- **Device configuration complexity and evolving technology**—Computing devices have changed in terms of capabilities and features and, consequently, their complexity has grown. Support staff need continual/periodic training to keep pace with the threats. This makes for an uneven target environment in which some targets are weaker than required. It only takes one vulnerability to gain access to a network.
- **Weaponized artificial intelligence (AI)**—Weaponized AI is a new and growing threat vector that enables hackers (and bots) to find and compromise systems quickly.
- **Inadequate infection and detection tools**—Intrusion detection systems (IDS) and intrusion prevention tools (IPS) may not be quick enough to stop zero-day and AI-driven attacks. Information security professionals must be vigilant to new threats and tools that can help them protect the organization.

“WEAPONIZED AI IS A NEW AND GROWING THREAT VECTOR THAT ENABLES HACKERS (AND BOTS) TO FIND AND COMPROMISE SYSTEMS QUICKLY.”

Cybercrime Marketplaces

Cybercriminal marketplaces allow criminals and associated organizations to conduct business and, thus, constitute a worldwide problem. Some of the challenges in taking down the cybercrime marketplaces include:

- Developing countries that are often challenged with weak economies and labor markets are ripe for the growth of cybercriminal activity. This continues to be a problem because Internet access is expanding in many developing countries.
- Hackers can adapt. Weak economies often encourage criminal endeavors, including fraud, malware, identity theft, data theft, etc. Having readily available tools, services and buyable information makes data and identity protection a big challenge.
- Criminals share malicious software tools, tricks (e.g., phishing) and techniques (e.g., poisoned domains and web services) with one another.

The criminal underground includes many cybermarketplaces where criminals buy and sell information, identities, services, tools/malware, etc., all of which make preventing attacks a daunting task for law enforcement.

- Growing cybercriminal trends such as spear phishing and ransomware are the latest ways criminals obtain/steal money. Because the tools are so ubiquitous, they are difficult to eliminate.
- The sharing of malware source code (i.e., variations) is a growing threat because perpetrators often do not fear capture or criminal consequences. New malware and source code proliferate easily across the dark web and cybercriminal marketplaces.
- Advanced software development tools often eliminate the need for coders. Malware programmers do not have to be numerous because tools are readily available in the underground to construct code easily.
- Illicit software testing tools and services ensure that malware evades detection. Quality check programs available in the cybercriminal marketplace are used to test and confirm that malware cannot be found by AV software.

Many key challenges cut across bots, botnets and cybercriminal marketplaces:

- If coders are not caught, there is no deterrent. Takedowns often apply only to equipment and software and, thus, produce only partial solutions if the originators and participants are not caught.
- Monetary gains are often not tracked or recovered. More work needs to be done to recapture the spoils of malicious activity. Whenever criminals can hide their gains for later use, they win.
- Penalties for cybercriminals are often light, and many loopholes exist—for example, perpetrators may not be prosecuted if they cause no harm within their own countries. Nevertheless, the damage can be devastating, not only to individuals and small organizations, but also to some large enterprises. Penalties should be standardized across countries, and monetary gains should be uniformly recovered from cybercriminals.
- Bots, botnets and criminal cybermarketplaces can be replaced quickly. Takedowns are often only temporary, because other bad actors rush in to take the place of the original perpetrators.
- Malware backups ensure continuity. Cybercriminals follow best practices and often recover systems from backups. Additionally, to be competitive, new market entrants copy the code and the setup of existing criminal marketplaces.

> “REGARDLESS OF SIZE, CYBERHYGIENE SHOULD BE STANDARD PRACTICE ACROSS ALL ORGANIZATIONS WITH DIGITAL PROCESSING ENVIRONMENTS.”

Cyberhygiene

Good cyberhygiene is often not ingrained in the practices of small- and medium-sized enterprises, which tend to grow with relatively little thought devoted to data security. Practicing good cyberhygiene helps keep data safe and well protected against theft and outside attacks. All organizations need to implement safeguards that prevent the unauthorized release of their data and their possible corruption. Without the knowledge or expertise to secure computing devices and environments, the organization is at risk. Regardless of size, cyberhygiene should be standard practice across all organizations with digital processing environments.

Perimeter

Protecting the perimeter is the first area of concern because it is the connection to the Internet and the doorway into the digital environment. Not implementing the safeguards results in a risk to the confidentiality, integrity and availability of data. Security teams should protect the perimeter by

defining boundaries, assigning ownership and creating accountability, implementing boundary firewalls and Internet gateways, and establishing an inventory of hardware and software. This inventory can help ensure that nothing is missed when performing vulnerability scans and that unauthorized software and hardware can be recognized and removed.

Network

The network should be protected by installing appropriate tools and/or applying appropriate techniques. Segmentation with enhanced controls to protect sensitive and confidential information exists should be assured. Additionally, user-access controls are necessary. These controls include minimizing administrative accounts, applying the principle of least privilege and using multifactor authentication.

Software and systems (e.g., antivirus software, patch management systems and network monitoring tools [such as IDS]) can also help protect the network. Event log monitoring systems and centralized monitoring dashboards may also be useful tools in protecting the network. Enterprises should also consider scanning incoming email, periodically scanning devices for vulnerabilities, and controlling wireless and remote access.

Devices

Devices include servers, workstations, laptops, tablets, smartphones, etc. Acquisition, configuration, maintenance, encryption and operational policies need to be implemented and enforced for all devices. Configuration standards need to be defined and implemented for all digital devices. Individual devices should be protected by implementing secure configurations to harden the devices, maintaining mobile devices, and monitoring and controlling permitted/approved software/apps. Organizations need to have a process in place to ensure that only approved software is loaded onto their devices. If safeguards are not in place, organizations risk allowing malware onto the devices and into their network, providing an authorized access point for hackers, breaking copyright laws and more.

Data

Data protection software and techniques (including data minimization and real-time scanning for sensitive data movement) should be used to protect data. Encryption for data at rest and in transit should be used wherever possible. Data should be backed up regularly and tested so that they can be restored in an emergency in the event of data corruption, system crash or a ransomware event. Despite taking all precautions, security breaches may happen, so establish and regularly test the organization's incident response plan.

Third Parties

Third parties can be partners, online information suppliers, Internet and CSPs, and any organization that provides or shares data with an organization. They can even be hardware vendors. These third parties must be secured by using them in a secure manner (e.g., encrypted traffic, data minimization) and mandating suitable security controls (e.g., device configurations, background checks, limiting building access) in any service and/or interconnection agreements. Without security safeguards, organizations risk exposure of their data (be they sensitive, confidential, personal, etc.), the organization's reputation and its future.

Supply Chain

The supply chain should be protected by requiring security reviews and/or assessments and enforcing uniform levels of security across the supply chain. Examples of enforcement that can be conducted include inspections and random visits that test access and authentication controls, building security, and incident response and contingency plans and procedures.

Recommendations to Reduce Risk

To reduce risk of data breaches (and many other types of malicious activity) on a global scale, enterprises, vendors and regulatory authorities should take the following actions, in addition to those presented previously.

Handling Bots and Botnets

Enterprises can perform many activities to prevent malware (e.g., bots and botnets) from gaining a

foothold in their infrastructures. They can reduce the enterprise's cyberattack surface by:

- Minimizing open ports, protocols, devices with access, and wireless access and accounts
- Implementing hidden backups to thwart ransomware
- Using vendor-provided security-as-a-service to enhance defensive programs and delegate prevention to experts
- Implementing a defense-in-depth strategy (including, for example, multiple barriers and network segmentation) to provide a more secure environment, especially for large organizations whose protective measures were initially developed in response to a specific compromise
- Performing frequent penetration testing of the organization's network to determine the strength of cyberdefenses and remediate vulnerabilities
- Enhancing network protection by using AI to combat botnet attacks

Detecting bots and botnets requires enterprises to monitor their infrastructure software for unauthorized changes (e.g., in executable file sizes, in hash values).

Responding to cyberinfections includes restoring original access rights and any affected device configurations, followed by cleaning infected systems and files. To recover quickly, enterprises must have secure baseline configurations for network, server and other devices ready at all times.

In addition to enterprises, authorities also can help combat the risk associated with bots and botnets. Authorities can detect bot and botnet infection attempts by running cybertakedowns repeatedly to clean affected devices. They should also coordinate evidence gathering and response efforts by implementing more Internet traffic monitoring centers. Authorities should seek to stop bots early so that the sheer volume of infected devices does not prohibit comprehensive takedowns.

Vendors also can coordinate preventive activities and products, such as:

- Developing malware profiles to keep antivirus software vendors more current and effective against new attack vectors and threats

"RESPONDING TO CYBERINFECTIONS INCLUDES RESTORING ORIGINAL ACCESS RIGHTS AND ANY AFFECTED DEVICE CONFIGURATIONS, FOLLOWED BY CLEANING INFECTED SYSTEMS AND FILES."

- Implementing services that help enterprises and software vendors detect vulnerabilities specific to given business sectors (e.g., hotel, airline, retail or pharmaceutical industries)
- Providing testing services (beyond scanners) to weed out program vulnerabilities
- Conducting bug bounty programs, a contest in which cyberpractitioners try to infect the sponsoring organization's network infrastructure to flush out network and software weaknesses

Vendors could also facilitate detection by using AI technology to isolate and track cyberanomalies and report them to the proper authorities. Vendors could develop IoT recognition systems or devices to enhance continuous monitoring and facilitate computer inventory and risk analysis.

Enterprises whose users have infected computers may consider implementing a trade-in policy that reduces the number of malicious/infected devices and simultaneously provides replacements with more secure and/or up-to-date systems.

Addressing Cybercriminal Marketplaces
Government/country law enforcement authorities need to monitor the cyberactivity of criminals as diligently and comprehensively as they monitor the good guys (e.g., via audits and assessments). One possibility is to use imposter criminal marketplaces to identify criminals. Another is to increase the number of sensors on the Internet to obtain information about the source(s). This information could be used to minimize the spread of malware, improve cyberresponses, establish new controls and find the attackers.

Handling Both Botnets and Criminal Cybermarketplaces

Authorities can offer rewards for information leading to arrests (especially in other countries) of those associated with malicious cyberactivity. Authorities should develop a search engine to identify devices with certain patterns and/or signatures and register them for future action (perhaps one potential application of AI). Authorities should leverage the efforts of vendors and researchers who routinely monitor network traffic to help narrow search areas and pinpoint the source of malware or botnet attacks. They should develop and test scenario-based response plans on a multi-country basis and share information regarding malicious activity among authorities and across borders—first to establish and then to optimize a coordinated response plan.

> "AS A BEST PRACTICE, AUTHORITIES SHOULD IMPLEMENT MALICIOUS CYBERACTIVITY DETECTION TOOLS AND TECHNIQUES ACROSS ALL LAW-ENFORCEMENT ORGANIZATIONS."

To detect botnets and cybercriminal marketplaces, authorities should work with other countries (i.e., United Nations [UN] partnerships)[17] to find and arrest "Cyber's Most Wanted."[18] All countries need to arrest those who commit cybercrimes, no matter their countries of origin. As a best practice, authorities should implement malicious cyberactivity detection tools and techniques across all law-enforcement organizations.

Finally, authorities should make more arrests worldwide and hold countries accountable via penalties. Penalties must be stiff to deter future activity effectively and encourage local governments to take action.

Conclusion

Malicious cyberactivity has gotten out of control. Cybercrime can be anonymous, quick and does not require a lot of research, given the ubiquity and easy access of cybercrime marketplaces. Enterprises, vendors and government authorities need to do more. The current standard information security posture—namely, responding to problems after the fact rather than striving to prevent big, costly and uncontrollable crises in advance—must change. Implementing the recommendations herein may help turn the tide by teaching cybercriminals to fear reprisals—not only takedowns, but also repossession of ill-gotten gain and lengthy prison time.

Endnotes

1 Cimpanu, C.; "Adromeda Botnet Operator Released With a Slap on the Wrist," BleepingComputer, 27 August 2018, *https://www.bleepingcomputer.com/news/security/andromeda-botnet-operator-released-with-a-slap-on-the-wrist/*

2 Federal Bureau of Investigation, "Darknet Takedown: Authorities Shutter Online Criminal Market AlphaBay," 20 July 2017, USA, *https://www.fbi.gov/news/stories/alphabay-takedown*

3 Department of Justice, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," 20 July 2017, USA, *https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down*

4 Greenberg, A.; "Operation Bayonet: Inside the Sting That Hijacked an Entire Dark Web Drug Market," *Wired*, 8 March 2018, *https://darkwebnews.com/darkwebmarkets/inside-the-operation-that-brought-down-hansa-market/*

5 Cimpanu, C.; "Russian Authorities Announce Takedown of RAMP Dark Web Marketplace," BleepingComputer, 19 September 2017, *https://www.bleepingcomputer.com/news/security/russian-authorities-announce-takedown-of-ramp-dark-web-marketplace/*

6 Vaas, L.; "'In Fraud We Trust'—Cybercrime Org Bust Shows We're Fighting Pros," *Naked Security*, 26 February 2018, *https://nakedsecurity.sophos.com/2018/02/26/in-fraud-we-trust-cybercrime-org-bust-shows-were-fighting-pros/*

7 Swinhoe, D.; "Dark Web Takedowns Make Good Headlines, Do Little for Security," *CSO*, 8 July 2019, *https://www.csoonline.com/article/3406319/dark-web-takedowns-make-good-headlines-do-little-for-security.html*

8 Howell O'Neill, P.; "DDoS-Happy Teenagers Arrested in International Cybercrime Bust," Cyberscoop, 12 December 2016, *https://www.cyberscoop.com/ddos-europol-arrest-december-2016/*

9 Cimpanu, C.; "Interpol Identifies 8,800 C&C Servers Used for Malware, Ransomware, Others," BleepingComputer, 24 April 2017, *https://www.bleepingcomputer.com/news/security/interpol-identifies-8-800-candc-servers-used-for-malware-ransomware-others/*

10 Vaas, L.; "Police Swoop on Gang That Planted Banking Trojan on 1m Phones," *Naked Security*, 24 May 2017, *https://nakedsecurity.sophos.com/2017/05/24/police-swoop-on-gang-that-planted-banking-trojan-on-1m-phones/*

11 Cimpanu, C.; "Owners of 'VirusTotal-for-Crooks' Service Arrested," BleepingComputer, 6 July 2017, *https://www.bleepingcomputer.com/news/security/owners-of-virustotal-for-crooks-service-arrested/*

12 Cimpanu, C.; "Hacker Gets a Whopping 14 Years in Prison for Running Scan4You Service," *ZDNet*, 22 September 2018, *https://www.zdnet.com/article/hacker-gets-a-whopping-14-years-in-prison-for-running-scan4you-service/*

13 Howell O'Neill, P.; "Latvian National Convicted of Running 'VirusTotal-for-Criminals' Malware Scanner," Cyberscoop, 16 May 2018, *https://www.cyberscoop.com/scan4you-ruslan-bondars-convicted-malware-scanner/*

14 Thomson, I.; "Tech Firms Take Down WireX Android Botnet," *The Register*, 28 August 2017, *https://www.theregister.co.uk/2017/08/28/tech_firms_take_down_wirex_android_botnet/*

15 Cochran, J.; "The WireX Botnet: How Industry Collaboration Disrupted a DDoS Attack," The Cloudflare Blog, 28 August 2017, *https://new.blog.cloudflare.com/the-wirex-botnet/*

16 Wlosinski, L. G.; "The IoT as a Growing Threat to Organizations," *ISACA® Journal*, vol. 4, 2019, *www.isaca.org/archives*

17 ITU, "Global Partnership," *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-partnership.aspx*

18 Federal Bureau of Investigation, "Cyber's Most Wanted," USA, *https://www.fbi.gov/wanted/cyber*