Chapter 8
Botnet Defense System and White-Hat Worm Launch Strategy in IoT Network

Shingo Yamaguchi
Yamaguchi University, Japan

Brij Gupta
National Institute of Technology, Kurukshetra, India

ABSTRACT

This chapter introduces a new kind of cybersecurity system named botnet defense system (BDS) that defends an IoT system against malicious botnets. This chapter consists of two parts. The former part describes the concept and design of the BDS. The concept is "fight fire with fire." To realize the concept, the BDS uses bot technology. The BDS builds a white-hat botnet on the IoT system by itself and uses it to exterminate the malicious botnets. The white-hat botnet autonomously spreads over the IoT system and thus drastically increases the defense ability. The latter part explains the strategy of the BDS. The white-hat botnet is a so-called double-edged sword. It defends the IoT system against malicious botnet but wastes the system's resources. Therefore, the BDS should strategically use the white-hat botnet. Some strategies have been proposed. Their characteristics are discussed through the simulation with the agent-oriented petri nets.

INTRODUCTION

Internet of Things (IoT) aims everything including humans to interact and to create new values from sharing information. IoT has enriched our lives while gives rise to a new risk on cybersecurity. IoT devices are explosively increasing, and the number is predicted to reach 30 billion by 2023 (Cisco, 2020). The problem is that most of them are vulnerable. This is because they do not have resources to run security functions and their vendors may sacrifice security in the price competition and/or their rush to market. In September 2016, that risk became reality. IoT was used as a springboard of giant distributed denial-

DOI: 10.4018/978-1-7998-7789-9.ch008

Copyright © 2022, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

of-service (DDoS) attacks, which struck many of the world's biggest sites such as Netflix and Twitter (O'Brien, S.A.,2016). These attacks were brought about by malware called Mirai. Mirai infects IoT devices and turns them into bots. Those bots form a network (botnet) that can be used for DDoS attacks. For the detail of Mirai, refer to (Sinaović, H., & Mrdovic, S., 2017) and (Yamaguchi, S. & Gupta, B., 2019). Mirai's DDoS attacks have a tendency to be large-scale and disruptive. This is because IoT devices are characterized by large-volume, pervasiveness, and high vulnerability (Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J., 2017). Mirai has spread to emerging markets and developing countries (Nakao, K., 2018). In early October 2016, Mirai infected over 300,000 IoT devices in 164 countries (Devry, J., 2016). To make matters worse, Mirai's authors published the source code (Bonderud, D., 2016). It gave rise to many variants of Mirai such as Satori (360 netlab., 2017) and Okiru (Arzamendi, P., Bing, M. & Soluk, K., 2018). Even now after five years since Mirai appeared, Mirai and variants continue to rage all over the world (Milić, J., 2019).

Some techniques have been proposed against Mirai's threat. The United States Computer Emergency Readiness Team (US-CERT) showed rebooting the infected device can clear Mirai (US-CERT, 2016). This is because Mirai penetrates only to the dynamic memory of the device. However, Moffitt, T. (2016) reported that Mirai can reinfect the device within minutes unless the vulnerability is patched. The other techniques can be roughly divided into three categories: detection, mitigation, and spread prevention. The following are typical examples.

Detection Techniques: Bezerra, V.H., da Costa, V.G.T., Barbon, J., Miani, R.S., & Zarpelão, B.B. (2019) have proposed a host-based approach to detect IoT botnets called IoTDS (Internet of Things Detection System). IoTDS monitors a device and collects its CPU use and temperature, memory consumption, and the number of processes. If the device detects any anomaly from the data, an alert of botnet detection is sent to the central server.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018) have proposed a network-based anomaly detection method for the IoT called N-BaIoT. N-BaIoT extracts behavior snapshots of the network and uses deep autoencoders to detect anomalous network traffic from compromised IoT devices.

Mitigation Techniques: Some of this category include both detection and mitigation (Jaramillo, L.E.S., 2018) and (Alomari, E., Manickam, S., Gupta, B. B., Anbar, M., Saad, R. M., & Alsaleem, S., 2016). Manso, P., Moura, J., & Serrão, C. (2019) have proposed a Software-Defined Intrusion Detection System. This system can automatically detect several DDoS attacks. Once the IDS detects an attack, it notifies a software-defined networking controller to control devices. Therefore, it timely enables to detect a botnet exploitation, to mitigate malicious network traffic, and to protect normal network traffic.

Ceron, J.M., Steding-Jessen, K., Hoepers, C., Granville, L.Z., & Margi, C.B. (2019) have proposed a network layer that adapts itself to mitigate the network traffic generated by malware. It can modify the traffic at the network layer based on the actions performed by the malware.

Spread Prevention Techniques: Gopal, T.S., Meerolla, M., Jyostna, G., Eswari, L., Reddy, P., & Magesh, E. (2018) have proposed a whitelisting based solution to prevent Mirai from spreading. They showed the successful blocking of Mirai malware through the experiment.

Frank, C., Nance, C., Jarocki, S., & Pauli, W. E. (2018) have proposed two scripts executable on actual devices to protect devices from becoming Mirai bots. They show that the hardening script was shown to be successful in preventing the initial Mirai infection on the device and the detection script was successful in recognizing and stopping an already existing infection in a controlled test environment.

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/botnet-defense-system-and-white-hat-worm-launch-strategy-in-iot-network/292235

Related Content

Using SAML and XACML for Web Service Security&Privacy
Tuncay Namliand Asuman Dogac (2008). *Securing Web Services: Practical Usage of Standards and Specifications (pp. 182-205).*
www.irma-international.org/chapter/using-saml-xacml-web-service/28519

Intelligent Video Monitoring and Analysis System for Power Grid Construction Site Safety Using Wireless Power Transfer
Xinyuan Liuand Hongyang He (2024). *International Journal of Information Security and Privacy (pp. 1-21).*
www.irma-international.org/article/intelligent-video-monitoring-and-analysis-system-for-power-grid-construction-site-safety-using-wireless-power-transfer/347878

Hexa-Dimension Code of Practice for Data Privacy Protection
Wanbil William Lee (2019). *Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics (pp. 237-248).*
www.irma-international.org/chapter/hexa-dimension-code-of-practice-for-data-privacy-protection/213654

The Electronic Surveillance of Public Assemblies: Political Privacy & Public Anonymity in Greece
Haralambos Anthopoulos (2011). *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices (pp. 59-68).*
www.irma-international.org/chapter/electronic-surveillance-public-assemblies/50408

Information Security Management Systems Cybernetics
Wolfgang Boehmer (2012). *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions (pp. 223-244).*
www.irma-international.org/chapter/information-security-management-systems-cybernetics/63092