Agent-whistleblower Technology for Secure Internet of Things

Vladimir Eliseev, Anastasiya Gurina

***Abstract*— The paper investigates the causes of widespread use by cybercriminals of the Internet of Things for organizing network attacks and other illegal use. An analysis of existing approaches and technologies for protecting networked computer devices is presented, as well as the main factors that prevent their use in the world of Internet of Things. An approach is suggested that ensures the integration of protective mechanisms directly into the composition of Things. Various variants of technology implementation are considered. Key aspects and potential ways of implementing the proposed approach are noted.**

***Tóm tắt*— Bài báo nghiên cứu về các phương thức được tội phạm mạng sử dụng rộng rãi trong Internet vạn vật (IoT), để tổ chức các tấn công mạng và các hành vi bất hợp pháp khác. Bài báo phân tích các phương pháp và công nghệ hiện có để bảo vệ các thiết bị kết nối mạng, cũng như các yếu tố chính để ngăn chặn việc sử dụng chúng trong IoT. Cách tiếp cận được đề xuất là đảm bảo việc tích hợp các cơ chế bảo vệ trực tiếp vào cấu trúc của IoT. Bài báo cũng xem xét các biến thể khác của việc thực hiện công nghệ này. Từ đó, đưa ra lưu ý về các khía cạnh chính và cách thức cài đặt tiềm năng để thực hiện phương pháp được đề xuất.**

***Keywords*— security agent; lightweight intrusion detection; anomaly detection; distributed network attack; DDoS attack; Internet of Things; smart things.**

***Từ khóa*— tác nhân bảo mật; phát hiện xâm nhập nhẹ; phát hiện bất thường; tấn công mạng phân tán; tấn công DDoS; internet vạn vật, sản phẩm thông minh.**

This manuscript is received on September 12, 2018. It is commented on November 1, 2018 and is accepted on November 14, 2018 by the first reviewer. It is commented on November 16, 2018 and is accepted on December 16, 2018 by the second reviewer.

I. INTRODUCTION

In recent years, considerable attention has been paid by computer security specialists to the Internet of Things (IoT). Researchers note a significant level of threat from the widely spread Smart Things both in terms of privacy and in the organization of large-scale botnets. The cause of the phenomenon, already called the rise of machines [1] and the Internet of Vulnerabilities [9], was a combination of factors previously considered separately: the lack of knowledge of users about the risks of using simple and default passwords, the presence of vulnerabilities in the firmware, and the inability to update the patched firmware from the manufacturer.

As early as 2014 it was discovered that numerous web cameras installed around the world and transmitting video to their owners via the Internet were completely unprotected from use by outsiders [2]. However, this only affected the violation of the privacy of private life. In the summer of 2016, there is appeared evidence of the formation of botnets based on IoT devices [3]. In the fall of 2016, the first significant use of the Mirai IoT botnet took place to organize a DDoS attack [4]. After that, it was reported about the signs of creating other large botnets based on the devices of the Internet Things and attacks with their help [1]. Despite the considerable attention attracted to this problem, it is still not clear how to deal with [5]. Simple recommendations for the protection of devices connected to the Internet, such as those listed in [6], have been known for a long time, but this does not have a significant effect for dealing with the problem that has arisen.

Authoritative specialists in the field of information security note that the scale of the problem becomes national and even worldwide and calls for strengthening state regulation to make Internet of Things more secure [5]. In these proposals, there is a certain sense, but it seems impossible to reverse the situation with the malicious use of the Internet of Things only through the adoption of laws and the creation of state control entities. The Internet is a cross-border infrastructure and it is unlikely that the problem of IoT-botnets, as well as other equally important problems, can significantly change the rules of the game on the Internet.

II. BACKGROUND

IoT devices which are most often attacked for inclusion in a botnet (DVR, routers), in terms of their computer architecture, are servers based on embedded Linux [9]. Technologies for creating botnets based on such devices have been known for more than 10 years. Let's list the ways of penetration into the system via the Internet:

- Default and weak passwords
- Configuration errors
- Software vulnerability
- Insufficient control by staff

Servers, personal computers and even mobile devices are systematically protected by firewalls, intrusion detection and prevention systems, antiviruses, security scanners, monitoring systems (SIEM) and Threat Intelligence. Most importantly, the security of conventional computer systems is always under the control of a human user, a system administrator or a security officer.

IoT devices due to their compactness, numerousness and narrow functional specialization, as a rule, they are not considered as computer equipment. When installing such devices in most cases, computer security specialists are not involved. However, the standard computer architecture used makes the Things vulnerable enough. In particular, typical software and hardware solutions lead to the emergence of typical vulnerabilities [7]. Well-researched approaches to penetration into Linux network servers prove to be successfully applied to IoT devices [8].

At the same time, the minority of the computer component in IoT devices is manifested in the limited opportunities for administration, software updates, usually represented by monolithic firmware, and the lack of free computing resources. A detailed description of typical properties of computer architectures used in IoT devices is given in [9]. Thus, it turns out that the owner of the IoT device, even if there is a qualification in the field of information security, does not have the ability to monitor the operation of the device, install patches for individual software components, and to strengthen the protection of the device by installing additional programs, for example, antivirus software. Manufacturers of IoT devices do not include advanced security features in the firmware, such as antivirus and network IDS/IPS, because the computing resources of the device are quite scarce. Therefore, the detection of penetration and subsequent malicious use of the device always go unnoticed.

The attacker is not limited in resources and can use the whole arsenal of tools for hacking the device, including identification of the versions of programs installed in the firmware, the selection of passwords, the use of known exploits and fuzzing for the development of new ones. Since IoT is based on typical computer architectures, penetration methods are also typical [9].

Let's consider the task of developing a technology that would allow the massive introduction of IDS/IPS into the Things and at the same time would be effective to prevent massive DDoS attacks from IoT botnets.

III. ANALYSIS

A. Anatomy of the IoT botnet attack and its prevention

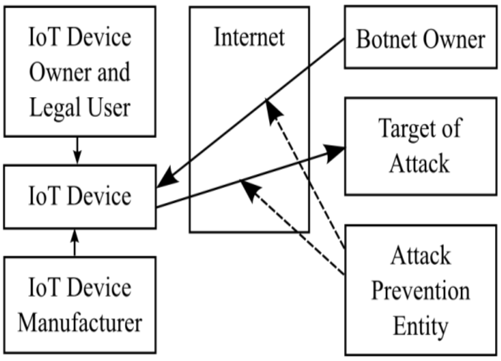

Fig 1. Subjects of attack using a botnet based on IoT

We list the main actors directly or indirectly involved in the process of creating a botnet, conducting an attack with it and countering this attack (Fig 1).

The indirect participation of the device manufacturer is due to the responsibility for the manufacture of the firmware containing certain vulnerabilities. The device owner and user configure the device and enforce security policies. His (her) errors lead to the possibility of intrusion and operation of the device in the botnet. As a rule, special organizations - telecom operators (ISP), CDN-providers and companies providing information security services, are engaged in preventing attacks.

The specificity of network attacks on the Internet is that the devices from which the attack is directed, the manufacturers of these devices, the owner of the botnet and the target of the attack, are usually distributed geographically and are in different jurisdictions. This greatly complicates the development of an effective set of measures, for example, forcing IoT device owners to implement the necessary security policy. Manufacturers of IoT devices do not always produce corrected firmware for devices with detected vulnerabilities and making them do this is not always possible. For example, the device can be officially withdrawn from support, but is still widely used. If the manufacturer supplies the device firmware automatic update tool from your site, this is considered by some countries as a possible problem with the violation of privacy, and even national security information, because it allows to arbitrarily change the functionality of the device after the sale.

Thus, the development of an acceptable technology for combating IoT-botnets must take into account the interests of all involved parties affected by the attack.

B. Intrusion detection and prevention considerations

In [10], clear definitions of IDS and IPS are given. Let's pay attention to the following aspects, which we will consider separately:

1. Monitoring of events.
2. Allocation of relevant events.
3. Analysis of events for signs of incidents.
4. Attempt to prevent a possible incident.

We list the main types of violations mentioned in [10] with regard to intrusion detection systems:

- Computer security policies
- Acceptable use policies
- Standard security practices

Let's pay attention to the fact that violation of security practices and policies regarding computer systems and IoT devices in particular takes place quite a long time, but only a massive violation of the policy of permissible use made the problem of IoT-botnets so important.

A. *Technologies for detection and protection from DDoS attacks*

Consider the technological aspects of detecting and preventing attacks. Typical schemes for including network IDS and IPS are shown in Fig 2.

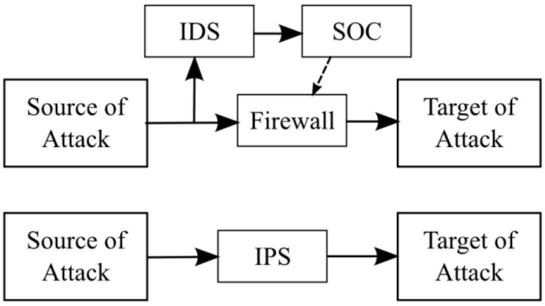

Fig 2. Typical schemes for including IDS and IPS in the network infrastructure

The IoT device acts during the formation of the botnet first as the target of the attack, and then as the source. Consider the possibilities of protection against attacks on these phases separately.

During the first phase, during the formation of the botnet, the vulnerabilities of the IoT device are exploited either by brute-forcing a password that gives access to the installation of programs or by injecting code that provides a similar possibility. Implementing the protection of an IoT device using the built-in complex of IDS and Firewall is generally not possible, since the mandatory in this case the Security Management Center (SOC) is not provided in the very ideology of the Internet of Things.

The use of built-in IPS is theoretically possible, but the following practical limitations hamper the implementation of this protection scheme:

- The need to regularly update the database with attack signatures and rules for their prevention. This service is usually paid, which will significantly increase the cost of the device.
- Significant resource consumption of IPS technology, which significantly increases the power consumption and cost of the IoT device.
- Non-zero probability of false positives increases the risk of inability to perform normal operations with the device.

Consider the second phase, when malicious penetration into the device successfully took place. When the command is received from the center, the botnet program starts an attack against the specified target. Traffic from many IoT devices arrives at the point of attack and causes a denial of service (Fig 3). Avoiding an attack near its target requires considerable resources to identify and filter the attacking traffic.

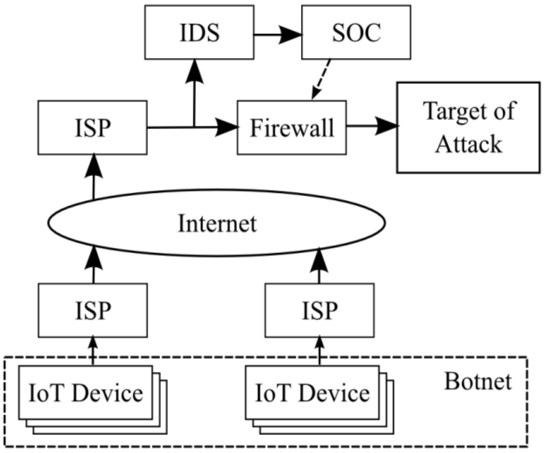

Fig 3. Scheme of DDoS attacks using the IoT botnet and the traditional protection scheme from it

The filtering task would be much easier if we could identify the attacking traffic directly where the infected devices connect to the Internet. However, the use of Dynamic NAT technology in Internet networks based on IPv4 makes it difficult to trace from the target of the attack to its many sources.

Consider the task of detecting an attack in the source. Technologies of network IDS are divided into two large types: signature based and anomaly based. The methods of signature analysis are aimed at detecting in the traffic flow the signs of network attacks and the consequences of the penetration of malicious code into the system. The accuracy of signature methods for known attacks is close to 100%, however, they can not be used to identify an attacker of network traffic in the source. Signatures do not allow detecting attacking DDoS traffic since it uses high-power factor, and does not use specific vulnerabilities in the implementation of the protocol stack. Identifying the control traffic of the botnet command centers is also difficult, since attackers in recent years often use cryptographic protocols.

The methods for detecting anomalies are very numerous [11,12], but they all have the following general properties:

- Require training on the source data for the purpose of constructing a classifier.
- Have in practice a precision that does not reach 100% and a non-zero level of false positives.

The main advantages of these methods, unlike signature ones, include an implicit way of extracting rules for detecting attacks from training data. In addition, training on normal data allows you to build a classifier that detects previously unknown anomalies – "zero-day" attacks.

IV. IDEA DESCRIPTION

A. Statement of the problem to be solved

We set as the main task the protection of Internet resources from botnet attacks based on IoT. At the same time, we will not solve the problem of protecting the IoT devices themselves from malicious influence. To do this, we will offer an approach that allows you to detect an attack in its source on the IoT device. For the purpose of protection from attack, a method will be proposed to inform the telecom operator about the source of the attack.

B. Detection of attack in source

Let's pay attention to three features of the devices of the Internet of Things essentially distinguishing them from usual servers:

- Fixed functionality for the entire lifetime.
- Identity of devices of the same model - they differ only in the serial number.
- Limited specific functionality.

Fixed functionality includes unchanged network protocols, input and output data formats, as well as basic working scenarios (sequence of actions). Limited functionality is due to the purpose of a particular device, for example, a DVR with control over the Internet.

It is possible to build a classifier that recognizes on the basis of analysis of incoming and outgoing network traffic, whether it is normal, corresponding to the main working scenarios, or not. If an anomaly is detected, it can be argued that the device is not being used for the intended purpose.

The methods used to construct the classifier can be different: from systems of formal rules and statistical methods to decision trees and artificial neural networks. The space of features involved in the classification can be quite simple. For example, a well-known list of network protocols and directions of opening connections during normal operation will easily reveal a DDoS type attack using unfamiliar protocols. A simple analysis of data packets (for example, using regular expressions) is possible, which makes it possible to distinguish normal protocol packets from unfamiliar, and therefore potentially related to attacking traffic.

The task of constructing such a classifier for the manufacturer of the IoT device is trivial, because in a compact form it reflects the specifications for the product. This classifier should be integrated into the firmware of the device for the purpose of independent monitoring of incoming and outgoing network traffic.

Identity of devices with the same firmware provides replicability of the developed classifier. Due to the fixed functionality of the device, the classifier does not require regular updates, similar to the signature based network IDS . When updating the firmware with the adjustment of functionality, the classifier must also be adjusted accordingly.

We call a complex from the classifier of normal operation and the method of signaling about the detected anomaly by the agent-whistleblower (Agent WB). The schema of the device with the agent-whistleblower is shown in Fig 4. If an abnormal traffic is detected, for example, on an infected device, the agent signals an anomaly (Fig 5). An anomaly alarm should include the address of the device, and also protect the message from spoofing.

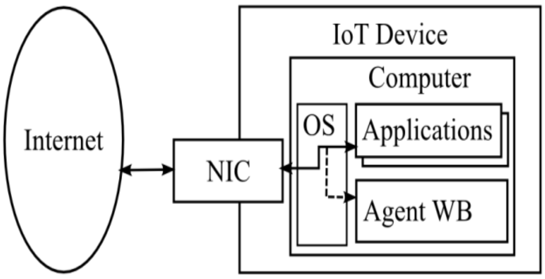

Fig 4. Structure of the secure IoT device

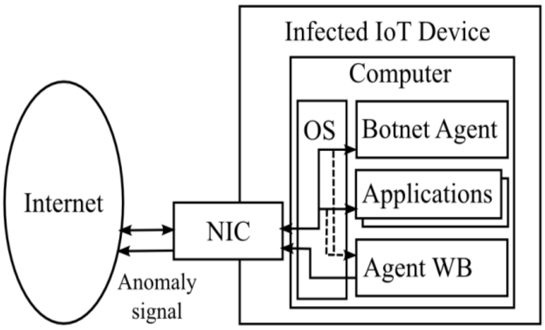

Fig 5. Anomaly detection on the infected IoT device

C. Preventing an attack near the source

Detecting an anomaly in the network traffic of the device can be a false positive, so the agent-whistleblower should not interfere with the functioning of the IoT device in which it is embedded. However, signals sent by agents on IoT devices when anomalies are detected must be processed in the telecom operator's infrastructure through which they connect to the Internet. The telecom operator, using event correlation tools, will be able to easily recognize whether the anomalies signals on individual IoT devices are disjointed or are a sign of a beginning DDoS attack. Since agents in their signals reveal the address of their device, the telecom operator can easily filter out the traffic of infected devices by blocking the Internet connection. A diagram showing the main elements of the system is given in Fig 6.

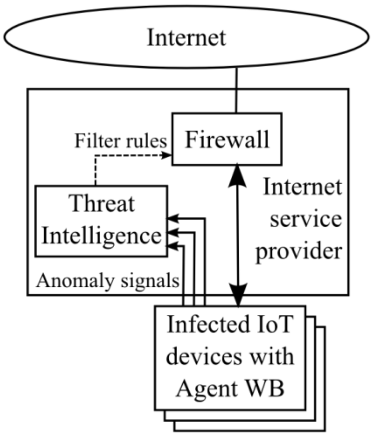

Fig 6. ISP infrastructure to process anomaly signals and block attacking traffic

It should be noted that for the wide use of this technology, the format of signals from agents of different IoT devices and different manufacturers should be unified. It is advisable to develop a standard in the form of RFC for this purpose. It is also possible to develop means for exchanging data on anomalies between telecom operators, which will increase the sensitivity and reliability of the entire system on a global scale.

V. REGULATION AND INCULCATION OF THE TECHNOLOGY

The proposed approach allows implementing the technology of detecting and preventing attacks from IoT devices, however, in order to obtain meaningful results, it is necessary to widely implement this technology. To do this, it's needed to:

- Develop compact embedded implementations of an agent-whistleblower in the distributed in the world of IoT computational modules of ARM, MIPS and x86 architectures.
- Provide signal processing on the side of telecom operators.
- Ensure that IoT devices manufacturers are forced to use the described technology by means of state regulation and certification of devices supplied to national markets.

The introduction of this technology does not require the transfer of user data in any, even anonymous, form. It is not required to provide special access to devices from telecom operators. National interests are also taken into account in cross-border shipments of IoT devices, since they are completely controlled in national jurisdictions by local telecom operators.

VI. DISCUSSION

The proposed technology for its full requires considerable coordination of efforts and synchronized actions of states that are technological leaders of the world economy. This may seem excessive, but experts note an extraordinary level of threat to the communication infrastructure of all countries in the world - from technological leaders such as Germany, to small ones such as Liberia [5].

Building a classifier for a specific IoT device can look like a complex task, requiring laborious analysis of specifications. However, the methods of machine learning make it possible to build a similar classifier for the traffic of the device obtained in the process of exhaustive release testing.

It can be noted that the agent-whistleblower can be disabled or deceived on the infected IoT device. To prevent disconnection, it is advisable to implement the agent at the level of the most protected components of the operating system or using technologies of a trusted computing environment, such as ARM TrustZone.

Deceit of the agent-whistleblower is possible in the event that the botnet agent program can disguise its traffic as normal. However, this masking requires knowledge of classifier rules for a particular IoT device. Adaptation of the botnet programs to a wide range of devices makes the task of creating a botnet too expensive, and therefore, economically unprofitable.

Infected IoT devices equipped with whistleblower agents may lose functionality during the attack time, as their traffic will be blocked completely or partially by the telecom operator. However, after a decease of the attack, the connection to the devices must be restored.

Since the correlation of anomalous events usually implies a certain threshold of insensitivity, it is possible to have single attacks passed by telecom operators to the Internet. However, the power of such attacks will be extremely small and will not cause a denial of service for the attacked resource.

VII. CONCLUSION

A comprehensive analysis of the problem of botnets based on Internet devices has been carried out. An approach is presented that describes the main elements and the introduction of technology for the implementation of the concept of secure Internet of Things through distributed analysis of anomalies and blocking of attack traffic close to the source.

REFERENCE

[1]. "The Rise of the IoT Botnet: Beyond the Mirai Bot" (April 12, 2017). [Online]. Available: http://resources.infosecinstitute.com/rise-iot-botnet-beyond-mirai-bot. [Accessed: 15-Jun- 2017]

[2]. Ms. Smith, "Peeping into 73,000 unsecured security cameras thanks to default passwords", (November 6, 2014). [Online]. Available: http://www.networkworld.com/article/2844283/microsoft-subnet/ peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html. [Accessed: 15-Jun- 2017]

[3]. Pierluigi Paganini "Sucuri spotted a large botnet of CCTV devices involved in DDoS attacks" (June 28, 2016). [Online]. Available: http://securityaffairs.co/wordpress/48807/cyber-crime/cctv-devices-ddos.html. [Accessed: 15-Jun-2017]

[4]. Brian Krebs "KrebsOnSecurity Hit With Record DDoS" (September 16, 2016). [Online]. Available: https://krebsonsecurity.com/2016/09/ krebsonsecurity-hit-with-record-ddos. [Accessed: 15-Jun- 2017]

[5]. Bruce Schneier, "Security and the Internet of Things", (February 1, 2016). [Online]. Available: https://www.schneier.com/blog/archives/ 2017/02/security_and_th.html. [Accessed: 15-Jun- 2017]

[6]. Joel Lee "Hack Attack: How To Keep Your Webcam Secure From Online Peeping Toms", (September 17, 2013). [Online]. Available: http://www.makeuseof.com/tag/hack-attack-how-to-keep-your-webcam-secure-from-online-peeping-toms. [Accessed: 15-Jun- 2017]

[7]. Rotem Kerner "Remote Code Execution in CCTV-DVR affecting over 70 different vendors" (March 22, 2016). [Online]. Available: http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html [Accessed: 16-Jun- 2017]

[8]. Richard Chirgwin "Dishwasher has directory traversal bug" (March 26, 2017). [Online]. Available: https://www.theregister.co.uk/2017/ 03/26/miele_joins_internetofst_hall_of_shame. [Accessed: 16-Jun- 2017]

[9]. Kishore Angrishi "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets" (February 17, 2017). [Online]. Available: https://arxiv.org/pdf/1702.03681.pdf. [Accessed: 16-Jun- 2017]

[10].Karen Scarfone, Peter Mell "Guide to Intrusion Detection and Prevention Systems (IDPS)" Special Publication (NIST SP) - 800-94, February 20, 2007.

[11]. Chandola, V., Banerjee, A., and Kumar, V. "Anomaly detection: A survey" ACM Comput. Surv. 41, 3, Article 15, July 2009.

[12]. Hodge, V.J., Austin, J. "A survey of outlier detection methodologies". Artificial Intelligence Review, 22(2), pp. 85–126 (2004).

ABOUT THE AUTHORS

Vladimir Eliseev

Workplace: JSC Infotecs, MPEI university

Email: EliseevVL@infotecs.ru

The education process: He is a Chief of Research and Development Center at JSC InfoTeCS and associate professor in Moscow Power Engineering Institute (MPEI). He received his Master's degree in information processing and control in technical systems from Moscow State Technical University named after Bauman in 1997. He defended his PhD thesis, devoted to neural networks for optimal control, at MPEI in 2012.

Research today: His research interests include information security, quantum cryptography applications, intrusion detection systems, neural networks and machine learning.

Anastasiya Gurina

Workplace: JSC Infotecs

Email:Anastasia.Gurina@infotecs.ru

The education process:She is a Researcher of Research and Development Center at JSC InfoTeCS. She received her Master's degree in management and informatics in technical systems from Moscow Power Engineering Institute in 2018. Since October 2018, she is a post-graduate student in system analysis, control and information processing in MPEI.

Research today: Her research interests include information security, intrusion detection systems, neural networks and machine learning.