ЗАЩИТА УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ ОТ MIRAI-ПОДОБНЫХ ВИРУСНЫХ ПРОГРАММ-ЧЕРВЕЙ

В работе проанализированы вредоносное программное обеспечение (ПО) ботнета Mirai и его модификации. Приведена история развития ботнета Mirai с момента первого обнаружения в августе 2016 года. Выделены основные составные части ботнета: бот, загрузчик, сервер управления и контроля, сервер отчетов. Описан процесс заражения вирусной программой-червем Mirai от перебора паролей на заражаемом устройстве до получения команды на начало DDoS атаки на целевой сервер. Рассмотрены отличительные следы вирусной программы-червя в трафике сети (шаблоны пакетов и коммуникации с серверами ботнета), которые позволяют определить наличие зараженного устройства в сети. Описаны модификации Mirai, использующие как открытый исходный код ботнета, так и только основные методики заражения и контроля ботов. Исследованы уязвимости устройств Интернета вещей (IoT) перед вирусной программой-червем Mirai и ее модификациями, сформулированы методы их обнаружения и защиты устройств IoT.

Ключевые слова: DDoS атака, ботнет, вирусная программа-червь, Интернет вещей (IoT).

Bukharev D. A., Vagin S. V., Sokolov A. N.

INTERNET OF THINGS DEVICES PROTECTION FROM MIRAI-LIKE WORM-VIRUSES

The paper analyzes the malicious software of the Mirai botnet and its modifications. The history of Mirai development since the first discovery in August 2016 is considered, the main components of the botnet are highlighted: bot, loader, command and control server, report server. The process of infection with worm-virus Mirai from brute force passwords on the device to receive a command to start a DDoS attack on the target server. The distinctive traces of the worm-virus in the network traffic (patterns of packets and communication with botnet servers), which allow to determine the presence of an infected device in the network, are considered. The article describes the modifications of Mirai, using both open source botnet and only the basic methods of infection and control of bots. Vulnerabilities of Internet of things (IoT) devices to the Mirai and Mirai-like worm-viruses are investigated, methods of its detection and protection of IoT devices are formulated.

Keywords: DDoS attack, botnet, worm-virus, Internet of things (IoT).

Развитие технологий Интернета вещей (Internet of Things, IoT) привело к появлению новых возможностей злоумышленников по реализации кибератак. Устройства IoT постоянно подключены к сети Интернет и имеют множество уязвимостей, которые позволяют злоумышленникам проводить атаки типа «Распределенный отказ в обслуживании» (Distributed Denial of Service, DDoS).

Последними примерами таких атак являются атаки ботнета (вирусной программы-червя) Mirai. Впервые этот ботнет был идентифицирован группой исследователей в области информационной безопасности MalwareMustDie в августе 2016 года [1]. Mirai (с яп. «будущее»), его множественные вариации и имитаторы послужили двигателем для реализации одних из самых крупных DDoS-атак в истории: в сентябре 2016 года веб-сайт консультанта по информационной безопасности Брайана Кребса был подвержен DDoS-атаке, трафик которой в пике составил около 620 Гб/с, что сделало ее одной из самых крупных DDoS-атак [2]. Приблизительно в то же время была произведена еще более крупная атака с помощью ботнета Mirai с трафиком в пике 1,1 Тб/с, нацеленная на поставщика облачных услуг OVH [3].

Через некоторое время после публикации в открытом доступе исходного кода Mirai его создателем [4], злоумышленники стали предлагать в аренду ботнеты на 400 тыс. одновременно зараженных устройств. Наиболее заметная по последствиям атака, которая привела к массовым проблемам доступа пользователей к популярным ресурсам, таким как Amazon, PayPal, GitHub, Twitter и др. [5], осуществлена в октябре 2016 года и была нацелена на известный DNS-провайдер Dyn.

Устройства Интернета вещей оказались наиболее уязвимым звеном в современных компьютерных сетях. Заражение вирусной программой-червем Mirai начинается с таких устройств как веб-камеры, цифровые видеорегистраторы и маршрутизаторы, работающие с использованием набора UNIX-утилит для встраиваемых операционных систем BusyBox. После этого вирусная программа-червь заражает другие незащищенные IoT устройства путем подбора стандартных логина и пароля администратора из небольшого словаря.

В настоящее время вариации Mirai генерируются ежедневно. Поскольку базовые механизмы безопасности в устройствах Интернета вещей, как правило, не реализованы,

вполне очевидно, что различные вариации Mirai продолжают наносить ущерб сетевой инфраструктуре, используя методы вторжения, подобные оригинальной версии Mirai [6].

В большинстве случаев Mirai приводит к DDoS-атаке, направленной на целевой список серверов путем своего внедрения в слабозащищенные IoT устройства. Можно выделить пять основных причин, которые делают устройства Интернета вещей приоритетной целью злоумышленников:

1. Работа устройств 24/7. В отличие от стационарных персональных компьютеров (ПК) и ноутбуков, от устройств IoT требуется бесперебойное круглосуточное функционирование.

2. Слабая защита устройств IoT. Приоритетной задачей большинства производителей, как правило, является обладание долей рынка устройств IoT, а не создание их защитных механизмов.

3. Недостаточная поддержка устройств IoT. Многие устройства IoT устанавливаются по принципу «включил и забыл», после чего пользователи и администраторы сети забывают об их обслуживании.

4. Генерация значительного объема трафика. Современные устройства IoT являются достаточно производительными устройствами, чтобы генерировать объемы трафика при DDoS атаке, сравнимые с объемами генерации трафика обычными современными ПК.

5. Неинтерактивный пользовательский интерфейс устройств IoT. Устройства IoT не требуют частого внимания пользователя, поэтому заражение, как правило, проходит незамеченным. Из-за недостаточных возможностей конфигурации устройства IoT пользователю тяжело исправить ситуацию при обнаружении заражения.

Коммуникация и организация ботнета Mirai

Ботнет Mirai состоит из четырех основных частей. Бот является вредоносной программой, которая заражает устройства [7]. Ее двойное предназначение заключается в распространении заражения на незащищенные устройства и атаке целевого сервера при получении соответствующей команды от лица, контролирующего бота, или ботмастера (лицо, контролирующее весь ботнет). Сервер управления и контроля (command and control, C&C) предоставляет ботмастеру интерфейс централизованного управления для проверки состояния ботнета и проведения

целевых DDoS-атак. Обычно вся коммуникация с другими частями сети происходит через анонимную сеть Tor. Сервер-загрузчик (loader) обеспечивает распространение вредоносной программы-червя, нацеливаясь на другие аппаратные платформы (18 платформ, включая ARM, x86, MIPS) путем прямой коммуникации с новыми жертвами. Сервер отчетов, к которому, как правило, обращаются инфицированные устройства, наполняет базу данных деталями о всех устройствах в ботнете.

В момент, когда вредоносное ПО Mirai пытается получить доступ к новым устройствам IoT, проверяются произвольные публичные IP-адреса на портах протокола TCP 23 или 2323. При этом некоторые адреса государственных служб, компаний General Electric и Hewlett-Packard исключены из проверяемого списка, предположительно для того, чтобы не привлекать внимание государственных органов. На рис. 1 показаны ключевые шаги организации и коммуникации ботнета Mirai.

Рис.1. Ключевые шаги организации и коммуникации ботнета Mirai

Рассмотрим процедуру заражения и атаки пошагово.

Шаг 1. Бот пытается получить контроль над слабозащищенными IoT устройствами путем перебора логина и пароля. Словарь для перебора прописан в программном коде Mirai и содержит 62 стандартные пары пользователь:пароль.

Шаг 2. После успешного подбора и запуска удаленной командной оболочки бот передает серверу отчетов различные характе-

ристики скомпрометированного устройства через другой порт TCP.

Шаг 3. Посредством сервера управления и контроля ботмастер регулярно проверяет наличие новых потенциальных жертв для заражения, а также текущий статус ботнета, посылая запрос серверу отчетов, обычно через анонимную сеть Tor.

Шаг 4. После определения потенциально уязвимых устройств ботмастер подает серверу-загрузчику команду на заражение с указанием всей необходимой информации: IP-адрес, аппаратную архитектуру, операционную систему и т.д.

Шаг 5. Сервер-загрузчик удаленно входит в целевую систему, загружает и запускает бинарную версию вредоносной программы при помощи утилиты Wget или по протоколу TFTP. После заражения вирусная программа-червь пытается защитить устройство от других вредоносных программ путем закрытия возможностей удаленного подключения к устройству, таких как Telnet или SSH. Зараженное

устройство начинает связываться с сервером управления и контроля для получения инструкций для атаки. Это происходит путем разрешения доменного имени cnc.changeme.com (в оригинальной версии Mirai), которое прописано в программном коде вирусной программы-червя, не используя статический IP-адрес. Таким образом, ботмастер имеет возможность по своему желанию изменять IP-адрес сервера управления и контроля с течением времени, не прибегая к изменению

бинарного файла вредоносной программы на зараженных устройствах.

Шаг 6. Ботмастер указывает всем ботам в сети атаковать определенный сервер путем выполнения простой команды на сервере контроля и управления с указанием типа DDoS атаки, ее длительности, списка IP-адресов ботов и целевых серверов.

Шаг 7. Боты после получения приказа атакуют сервер одним из 10 возможных типов DDoS атак, включая DDoS атаки TCP SYN-флуд, HTTP-флуд и DDoS атаку, использующую протокол GRE.

Модификации Mirai

Появление в открытом доступе исходного кода Mirai не только не привело к быстрому появлению механизмов защиты от него, но и позволило создать новые модификации Mirai. Через два месяца после публикации исходного кода Mirai количество ботов в сети увеличилось с 213 тыс. до 493 тыс. [1]. Модификации Mirai используют те же уязвимости устройств IoT, что и оригинальная версия ботнета Mirai.

Как правило, заражения Mirai проходят через порты TCP 23 и 2323. Модификации Mirai, обнаруженные в ноябре 2016 года, используют для заражения другие порты TCP, например, порт 7547, который используется интернет-провайдерами для удаленного управления широкополосными маршрутизаторами клиентов. Одна из таких модификаций привела к отключению от сети около миллиона пользователей Deutsche Telekom [8]. В феврале 2017 года очередная модификация Mirai запустила 54-часовую DDoS атаку на сайт колледжа в США [9]. В марте 2017 года появилась новая модификация с функцией добычи криптовалюты Bitcoin. Учитывая малые вычислительные мощности устройств IoT, злоумышленники не получили от очередной модификации значительных выгод [10].

Очередной модификацией вредоносного ПО Mirai стал ботнет Persirai [11], открытый в апреле 2017 года исследователями компании Trend Micro и названный из-за своего, предположительно, иранского происхождения (Persian Mirai). Механизм работы Persirai предполагает получение доступа к веб-камерам определенного производителя через порт TCP 81. Если доступ удастся, вирусная программа-червь пытается проникнуть в маршрутизатор, к которому подключено само устройство через уязвимости набора протоколов UPnP. После этого на маршрути-

затор загружается вредоносный бинарный файл, который удаляется после запуска. Для доступа к устройствам Persirai использует не простой перебор паролей, а задокументированные уязвимости первого дня для получения файла с паролем. Это становится возможным, поскольку пользователи, как правило, не обновляют программное обеспечение устройств IoT в процессе эксплуатации.

В сети все чаще появляются новые ботнеты, использующие все те же базовые принципы заражения устройств, но более продуманные механизмы сокрытия и распространения.

Ботнет IoT, написанный на языке программирования Lua, был обнаружен группой MalwareMustDie в конце августа 2016 года [12]. Большинство устройств, вошедших в ботнет, были модемы с процессорами архитектуры ARM и операционными системами Linux. Вредоносная программа использует шифрованное соединение с сервером контроля и управления и особый список правил фаервола iptables для защиты зараженных устройств.

Ботнет Hajime, обнаруженный в октябре 2016 года специалистами компании Rapidity Networks [13], использует метод заражения, схожий с Mirai. Однако механизм сокрытия ботнета Hajime предполагает вместо централизованной архитектуры использование децентрализованных механизмов связи при помощи протоколов BitTorrent DHT (для поиска пиров) и µTP (для передачи данных). Каждое сообщение, отправляемое отдельным ботом, шифруется и подписывается ассиметричным протоколом RC4. При этом своими действиями вирусная программа-червь закрывает все порты доступа к устройству IoT, которые используются Mirai-подобными ботнетами.

Другой ботнет, основанный на работе с набором утилит BusyBox – BrickerBot был обнаружен группой исследователей Radware в апреле 2017 года [14]. Путем получения удаленного доступа по SSH, используя стандартные пары логин-пароль, вредоносная программа производит атаку типа «Постоянный отказ в обслуживании» (PDos) путем перезаписи системной прошивки, удаления всех файлов во встроенной памяти и реконфигурации параметров сетевого подключения.

Методы защиты от вредоносного ПО Mirai

В отличие от другого вредоносного ПО, Mirai не пытается избежать обнаружения. Во всех стадиях заражения, вирусная программа-

червь оставляет следы, которые можно обнаружить даже при простом анализе трафика в сети. Трафик в сети с устройством, зараженным Mirai, может включать в себя:

- последовательную проверку данных для входа по определенному порту;
- отсылку отчетов, имеющих различимый шаблон;
- скачивание бинарного кода определенного типа;
- обмен keep-alive сообщениями;
- получение команд от удаленного сервера на атаку, которые имеют определенную структуру;
- генерацию трафика с очень малым числом произвольных компонентов.

Таким образом, зараженное устройство можно определить по четко различимому шаблону, который формируется типами сообщений, размерами пакетов и последовательностью отправки.

При первоначальном заражении Mirai производит перебор логинов и паролей из встроенного в программный код словаря, который содержит 62 стандартных и самых популярных пар. Поэтому для защиты от заражения Mirai рекомендуется предпринять следующие действия:

1. Разработчикам устройств IoT необходимо:

- предоставить пользователю возможность изменения логина и пароля для входа в устройство при первоначальной настройке;
- предоставить пользователю возможность генерации нового логина и пароля с использованием криптографически стойких генераторов псевдослучайных чисел;
- реализовать технологию проверки подлинности исполняемого кода с целью исключения возможности выполнения вредоносного неподписанного кода вирусной программой-червем на устройстве [15].

2. Пользователям и администраторам сети с устройствами IoT необходимо:

- изменить стандартный логин и пароль для входа при первоначальной настройке устройства IoT;
- запретить доступ к IoT устройству из внешней сети, если в этом нет необходимости;
- все устройства IoT объединить в отдельную подсеть путем физического разделения сети или с использованием VLAN.

Реализация предложенных рекомендаций позволит закрыть возможности проник-

новения вирусной программы-червя Mirai и его вариаций в устройства IoT и внутреннюю сеть.

Для обнаружения возможности заражения устройств Интернета вещей, находящихся во внутренней сети, можно воспользоваться бесплатным ресурсом Mirai Vulnerability Scanner [16], которое осуществляет проверку на предмет наличия уязвимых устройств и уведомляет пользователя, если таковые устройства были найдены. При наличии уязвимых устройств следует воспользоваться предложенными ранее методами устранения уязвимостей и реализовывать новые проверки до тех пор, пока сканер не сообщит об отсутствии уязвимых устройств.

Для обнаружения уже зараженных устройств во внутренней сети можно воспользоваться бесплатной утилитой для диагностики сети Wireshark [17] и специальными аппаратными перехватчиками трафика (network TAP), устанавливаемыми внутри сети. Wireshark позволяет «прослушивать» трафик в сети в реальном времени, либо читать уже заготовленные pcap-файлы с записанным трафиком. В утилите Wireshark необходимо отфильтровать ранее записанный трафик и оставить только те пакеты, которые отправляются устройствами Интернета вещей. Для этого следует использовать фильтр «ip.dest == X.X.X.X», где X.X.X.X – IP-адрес проверяемого устройства.

После фильтрации трафика необходимо его проанализировать. Проверяемое устройство IoT можно считать зараженным, если оно в течение 10-15 минут отправляет пакеты на различные IP-адреса сети Интернет или внутренней сети, которые содержат:

- запросы на авторизацию по telnet, SSH, http;
- DNS-запросы по доменному имени sps.changeme.com, так как это доменное имя принадлежит серверу управления и контроля Mirai.

При обнаружении зараженного устройства следует провести сброс устройства к заводским настройкам и установить на нем новые логин и пароль для входа [18].

На рис. 2 представлена общая схема алгоритма обнаружения и устранения угроз заражения устройств Интернета вещей вирусной программой-червем Mirai и его модификациями.

Выводы

Ущерб, причиненный атаками ботнета

Рис. 2. Схема алгоритма обнаружения и устранения угроз заражения устройств Интернета вещей вирусной программой-червем Mirai и его модификациями.

Mirai, его модификациями и подражателями указывает на уязвимости, которыми обладают устройства Интернета вещей. Самые обычные подходы к получению несанкционированного доступа к таким устройствам позволяют злоумышленникам объединять устройства в большие группы, которые могут использоваться для DDoS атак. В работе описана структура и характеристики ботнета Mirai и его модификаций, приведены причины, которые делают устройства Интернета вещей приоритетной целью для атак злоумышленников. К этим причинам относятся:

- слабая защита устройств IoT;
- недостаточная поддержка со стороны производителя;

- малые возможности пользовательской конфигурации устройств IoT;
- большой вычислительный потенциал большого числа IoT устройств, объединенных в одну сеть.

Для реализации противодействия атакам на IoT устройства рассмотрен типовой процесс их заражения и предложены рекомендации по защите от ботнета Mirai и его модификаций как для разработчиков устройств Интернета вещей, так и для конечных пользователей и администраторов сетей.

Статья выполнена при поддержке Правительством РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

1. Блог «MalwareMustDie» [Электронный ресурс]. – Режим доступа: <http://blog.malwaremustdie.org/2016/08/mmd-0054-2016-pnscan-elf-worm-that.html>, свободный (дата обращения: 13.10.2018).
2. Блог «KrebsonSecurity» [Электронный ресурс]. – Режим доступа: <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos>, свободный (дата обращения: 13.10.2018).
3. Сайт компании ArsTechnica [Электронный ресурс]. – Режим доступа: <https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/>, свободный (дата обращения: 13.10.2018).
4. Исходный код вирусной программы-червя Mirai [Электронный ресурс]. – Режим доступа: <https://github.com/jgamblin/Mirai-Source-Code>, свободный (дата обращения: 13.10.2018).
5. Британский новостной сайт «The Register» [Электронный ресурс]. – Режим доступа: https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/, свободный (дата обращения: 15.10.2018).
6. Tuptuk N., Hailes S. Security of smart manufacturing systems // Journal of Manufacturing Systems. – 2018. – № 47. – С. 93–106.
7. Багай Д.И. Угроза Интернету вещей: ботнет Mirai // Современные технологии: актуальные вопросы, достижения и инновации: сборник статей XIV Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение». – 2018. – С. 69–72.
8. Блог «KrebsonSecurity» [Электронный ресурс]. – Режим доступа: <https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/>, свободный (дата обращения: 15.10.2018).
9. Сайт веб-сервиса мониторинга и защиты от DDoS атак Imperva Incapsula [Электронный ресурс]. – Режим доступа: <https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html>, свободный (дата обращения: 15.10.2018).
10. Сайт компании SecurityIntelligence [Электронный ресурс]. – Режим доступа: <https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/>, свободный (дата обращения: 16.10.2018).
11. Блог компании SecurityIntelligence [Электронный ресурс]. – Режим доступа: <https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/>, свободный (дата обращения: 16.10.2018).
12. Блог «MalwareMustDie» [Электронный ресурс]. – Режим доступа: <http://blog.malwaremustdie.org/2016/09/mmd-0057-2016-new-elf-botnet-linuxluabot.html>, свободный (дата обращения: 19.10.2018).
13. Статья S. Edwards and I. Profetis, 16 Окт. 2016; [Электронный ресурс]. – Режим доступа: <http://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf>, свободный (дата обращения: 19.10.2018).
14. Сайт группы исследователей Radware [Электронный ресурс]. – Режим доступа: <https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/>, свободный (дата обращения: 19.10.2018).
15. Маслова М.А. Принципы безопасности интернета вещей // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 3(29). – С. 38–42.
16. Mirai Vulnerability Scanner [Электронный ресурс]. – Режим доступа: <https://www.incapsula.com/mirai-scanner/>, свободный (дата обращения: 17.11.2018).
17. Утилита Wireshark [Электронный ресурс]. – Режим доступа: <https://www.wireshark.org/>, свободный (дата обращения: 17.11.2018).
18. Коновалова С.Б., Миронов А.Н. Вопросы информационной безопасности Интернета Вещей // ИТ-Стандарт. – 2016. – № 9. – С. 37–39.

References

1. Blog «MalwareMustDie» [Elektronnyy resurs]. – Rezhim dostupa: <http://blog.malwaremustdie.org/2016/08/mmd-0054-2016-pnscan-elf-worm-that.html>, svobodnyy (data obrashcheniya: 13.10.2018).
2. Blog «KrebsonSecurity» [Elektronnyy resurs]. – Rezhim dostupa: <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos>, svobodnyy (data obrashcheniya: 13.10.2018).
3. Sayt kompanii ArsTechnica [Elektronnyy resurs]. – Rezhim dostupa: <https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/>, svobodnyy (data obrashcheniya: 13.10.2018).
4. Iskhodnyy kod virusnoy programmy-cherveya Mirai [Elektronnyy resurs]. – Rezhim dostupa: <https://github.com/jgamblin/Mirai-Source-Code>, svobodnyy (data obrashcheniya: 13.10.2018).
5. Britanskiy novostnoy sayt «The Register» [Elektronnyy resurs]. – Rezhim dostupa: https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/, svobodnyy (data obrashcheniya: 15.10.2018).

6. Tuptuk N., Hailes S. Security of smart manufacturing systems // Journal of Manufacturing Systems. – 2018. – № 47. – С. 93–106.
7. Bagay D.I. Ugroza Internetu veshchey: botnet Mirai // Sovremennyye tekhnologii: aktual'nyye voprosy, dostizheniya i innovatsii: sbornik statey XIV Mezhdunarodnoy nauchno-prakticheskoy konferentsii. – Penza: MTSNS «Nauka i Prosveshcheniye». – 2018. – С. 69–72.
8. Blog «KrebsonSecurity» [Elektronnyy resurs]. – Rezhim dostupa: <https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/>, svobodnyy (data obrashcheniya: 15.10.2018).
9. Sayt veb-servisa monitoringa i zashchity ot DDoS atak Imperva Incapsula [Elektronnyy resurs]. – Rezhim dostupa: <https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html>, svobodnyy (data obrashcheniya: 15.10.2018).
10. Sayt kompanii SecurityIntelligence [Elektronnyy resurs]. – Rezhim dostupa: <https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/>, svobodnyy (data obrashcheniya: 16.10.2018).
11. Blog kompanii SecurityIntelligence [Elektronnyy resurs]. – Rezhim dostupa: <https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/>, svobodnyy (data obrashcheniya: 16.10.2018).
12. Blog «MalwareMustDie» [Elektronnyy resurs]. – Rezhim dostupa: <http://blog.malwaremustdie.org/2016/09/mmd-0057-2016-new-elf-botnet-linuxluabot.html>, svobodnyy (data obrashcheniya: 19.10.2018).
13. Stat'ya S. Edwards and I. Profetis, 16 Okt. 2016; [Elektronnyy resurs]. – Rezhim dostupa: <http://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf>, svobodnyy (data obrashcheniya: 19.10.2018).
14. Sayt gruppy issledovateley Radware [Elektronnyy resurs]. – Rezhim dostupa: <https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/>, svobodnyy (data obrashcheniya: 19.10.2018).
15. Maslova M.A. Printsipy bezopasnosti interneta veshchey // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2018. – № 3(29). – С. 38–42.
16. Mirai Vulnerability Scanner [Elektronnyy resurs]. – Rezhim dostupa: <https://www.incapsula.com/mirai-scanner/>, svobodnyy (data obrashcheniya: 17.11.2018)
17. Utilita Wireshark [Elektronnyy resurs]. – Rezhim dostupa: <https://www.wireshark.org/>, svobodnyy (data obrashcheniya: 17.11.2018)
18. Konovalova S.V., Mironov A.N. Voprosy informatsionnoy bezopasnosti Interneta Veshchey // IT-Standart. – 2016. – № 9. – С. 37–39.

БУХАРЕВ Дмитрий Александрович, магистрант кафедры вычислительной математики и высокопроизводительных вычислений высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: needleinspace@gmail.com

ВАГИН Сергей Владиславович, магистрант института спорта, туризма и сервиса ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: vaginserg.96@mail.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

BUKHAREV Dmitrii, student of the Department of computational mathematics and high-performance computing of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: needleinspace@gmail.com

VAGIN Sergey, student of the Institute of sport, tourism and service FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: vaginserg.96@mail.ru

SOKOLOV Alexander, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru