3. Howser G., McMillin B. A Modal Model of Stuxnet Attacks on Cyber-physical Systems: A Matter of Trust // Eighth Int. Conf. on Soft. Sec.and Reliability (SERE), San Francisco, CA. – 2014. – Pp. 225-234.

4. Margelis G., Piechocki R., Kaleshi D., Thomas P. Low throughput networks for the iot: Lessons learned from industrial implementations. In Internet of Things (WF-IoT) // 2015 IEEE 2nd World Forum. – 2015. Pp. 181-186.

5. Detken K., Rix T., Kleiner C., Hellmann B., Renners L. SIEM approach for a higher level of IT security in enterprise networks // IEEE 8th Int. Conf. on Intelligent Data Acquisition and Adv. Comp. Systems: Techn. and App. (IDAACS), Warsaw. – 2015. – Pp. 322-327.

6. Evsutin O., Kokurina A., Meshcheryakov R., Shumskaya O. An adaptive algorithm for the steganographic embedding information into the discrete fourier transform phase spectrum // Advances in Intelligent Systems and Computing. – 2016.

7. Iskhakov S., Shelupanov A., Meshcheryakov R. Simulation modelling as a tool to diagnose the complex networks of security systems // J. of Phys.: Conf. Series. – 2017. – Vol. 803. – Pp. 12-57.

8. Abomhara M., Kien G.M. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks // Journal of Cyber Security. – 2015. – Vol. 4. – Pp. 65–88.

9. LoRa Alliance [Electronic resource]. URL: https://www.lora-alliance.org/.(access date: 01.10.2017).

10. Sicari S., Rizzardi A., Grieco L., Coen-Porisini A. Security, Privacy & Trust in Internet of Things: the road ahead // Computer Networks (Elsevier). – 2015. – Vol. 76. – Pp. 146–164.

АНАЛИЗ УЯЗВИМОСТЕЙ ВСТРОЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ IOT-УСТРОЙСТВ ПОСРЕДСТВОМ ВНЕДРЕНИЯ СЕТИ HONEYPOT

А.О. Исхакова, А.Ю. Исхаков, Р.В. Мещеряков
Томск (Томский государственный университет систем управления и радиоэлектроники)
shumskaya.ao@gmail.com

ANALYSIS OF THE VULNERABILITIES OF THE EMBEDDED INFORMATION SYSTEMS OF IOT-DEVICES THROUGH THE HONEYPOT NETWORK IMPLEMENTATION

A.O. Iskhakova, A.Yu. Iskhakov, R.V. Meshcheryakov
Tomsk (Tomsk State University of Control Systems and Radioelectronics)

Abstract. The Internet of Things is now an essential tool in many areas of human life. Researches related to the security of IoT-devices and IoT-networks are extremely relevant over the past ten years. The violation of the confidentiality, integrity of the transmitted data and the availability of smart objects and control devices can lead to major risks and various negative consequences. The article details the conduct of the research experiment on the introduction of a honeypot trap into a smart house IoT-network. The results allow to make a conclusion about the ways of attacks on smart objects, the protocols and services use, the influence of the devices placement in the network on their security level.

Keywords: Internet of Things; IoT-device; smart device; information security; honeypot, IoT-network; attack; trap; unauthorized access

Введение. Переход к Интернету вещей, согласно исследованию Cisco [1], произошел примерно в 2008-2009 годах. С этих пор количество устройств, подключенных к глобальной сети Интернет, превысило численность населения Земли. Число инноваций в этой области непрерывно растет, что говорит об активном развитии Интернета вещей.

Интернет-вещи могут образовывать локальные сети, объединенные какой-либо одной зоной обслуживания или функцией. По данным [2] на май 2017 года в коллекции «Лаборато-

рии Касперского» находилось более 7000 различных образцов вредоносного ПО для «умных» устройств, причем около половины из них были добавлены в 2017 году. Чтобы обеспечить надлежащий уровень безопасности для инфраструктуры IoT, необходима стратегия всесторонней защиты [3]. В рамках нее обеспечивается защита данных в облаке, защита целостности данных при передаче в Интернет, а также безопасное производство устройств. Актуальность направления обеспечения безопасности IoT-устройств обуславливает необходимость разработки новых методов и средств борьбы со злоумышленниками, атакующими подобные системы [4].

Целью данного исследования является расширение знаний об источниках атак и способах несанкционированного получения доступа к IoT-устройствам. Для достижения данной цели была поставлена задача размещения нескольких smart-устройств в качестве honeypot [5, 6] объектов.

Использование honeypot в информационной безопасности. На сегодняшний день человек доверил smart-устройствам важные сферы своей жизни. Тренд развития IoT-систем и сетей в целом состоит в том, что рост количества smart-устройств, используемых конечными потребителями, приводит к росту числа новых угроз и видов атак [7].

Для обеспечения безопасности smart-объектов и настройки параметров защиты применяются различные методы и средства компьютерной безопасности [8], в том числе использование ловушки honeypot. Задача honeypot-ловушки – заинтересовать злоумышленника для осуществления им попыток получения несанкционированного доступа. Тем самым, организуя honeypot в сети, можно получить информацию о начале, процессе, результате атаки и взлома. Существует множество вариаций [9] применения данного инструмента для выведывания тактики злоумышленника.

Подобный инструмент дает возможности исследователю получить необходимую информацию, собрать статистику по нарушениям безопасности в контролируемой сети. Несмотря на это, создавая honeypot, необходимо помнить, что это «окно» для злоумышленника в вашу систему. В связи с этим следует учитывать основы обеспечения компьютерной безопасности, а также проявлять профессиональную бдительность при проведении экспериментов с применением данной технологии [10].

Постановка и ход проведения эксперимента. Задача для каждого из внедряемых объектов honeypot — подвергнуться атаке или несанкционированному исследованию и поиску уязвимостей. Это впоследствии позволит изучить стратегию злоумышленника и определить перечень средств, с помощью которых проводятся атаки на ресурсы. Для реализации honeypot-ловушки было использовано 9 устройств, применяемых в системе «Умного дома»: видеорегистратор (DVR), IP-видеокамеры, IP-домофон, TV-приставка, а также такие smart-устройства с возможностью доступа в Интернет как система управления кондиционированием, чайник, холодильник и лампа освещения. Перед началом эксперимента на все устройства были установлены последние версии программного обеспечения.

В ходе подготовки эксперимента было принято решение реализовать два различных варианта размещения ловушек, которые помогут предоставить полные сведения о тактике злоумышленника. Таким образом, 4 устройства (далее объединим их в класс 1) были размещены в демилитаризованной зоне (DMZ) [11]. Для имитации наиболее реалистичной картины размещения и усложнения доступа злоумышленнику оставшиеся 5 устройств были установлены внутри локальной сети (класс 2). Доступ к данным устройствам из Интернет возможен по нескольким открытым портам посредством технологии Port Forwarding, настроенной на пограничном маршрутизаторе. При этом для усложнения путей эксплуатации уязвимостей стандартные значения «пробрасываемых портов», отвечающих за те или иные сервисы, были изменены.

На используемом DVR и двух ip-камерах были сохранены значения имени пользователя и пароля, установленные производителем по умолчанию: «root»/«pass» (устройство класса 1), «ubnt»/«ubnt» (устройство класса 2), «admin»/«4321» (устройство класса 1). В

остальных устройствах были установлены пароли, удовлетворяющие следующему критерию сложности: не менее 7 символов, использование разных регистров, минимум 1 спецсимвол, наличие не менее 1 цифры. Схема построенной сети–ловушки представлена на рис. 1.

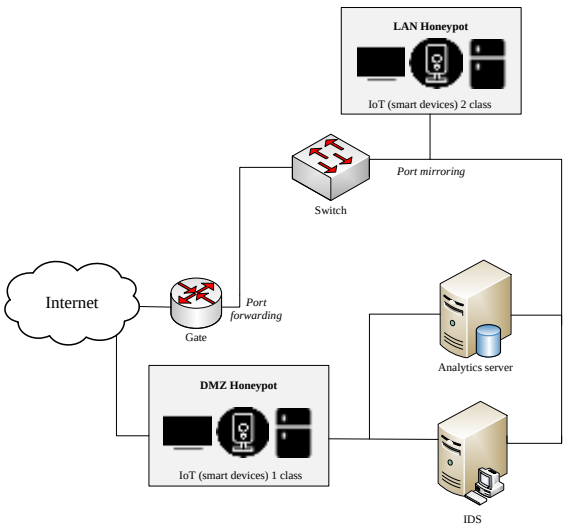

Рис. 1. Технология построенной сети-ловушки из IoT устройств

Весь трафик, поступаемый на smart-устройства, посредством технологии Port-mirroring дублируется на сервер аналитики и систему обнаружения вторжений. В качестве основного средства автоматизации выявления потенциальных атак был выбран программно-аппаратный комплекс ViPNet IDS [12]. Работа данного комплекса строится на основе динамического анализа сетевого трафика, начиная с канального уровня и заканчивая прикладным уровнем модели взаимодействия открытых систем (OSI) [13]. Вторым инструментом для проведения эксперимента был выбран анализатор протоколов Wireshark [14], выполняющий захват трафика по заранее настроенным фильтрам, и позволяющий провести «ручной» разбор множества потенциально опасных запросов. Первые попытки подключения к открытым SSH и Telnet-портам были зафиксированы уже в течение нескольких минут после запуска устройств. За сутки же было зарегистрировано более двух тысяч обращений с нескольких сотен уникальных IP-адресов.

Результаты проведения эксперимента. Период мониторинга составил 3 месяца. Общее количество попыток авторизации на 9 устройствах составляет 520 479, из них неудачных попыток 515 057, а успешных 5 422. При этом, все зафиксированные факты несанкционированной успешной авторизации относятся ко всем элементам 1 класса: 2 устройства, содержащие стандартные пары логин/пароль от производителя и 2 устройства с измененным паролем. Анализ поступивших за данный период запросов позволяет говорить о том, что порядка 80% подключений осуществляется по стандартным портам следующих сервисов: SSH, Telnet, HTTP, FTP, SMB. Несмотря на многочисленные попытки авторизации, системами аналитики не было зафиксировано ни одного успешного факта несанкционированного доступа к устройствам класса 2.

Большинство IP-адресов, с которых на smart-ловушках были зафиксированы попытки подключения, успешно отвечали на icmp-запросы. Идентификация категорий атакующих устройств проводилась следующими методами: анализом заголовков сетевых пакетов атакующих устройств, а также проверкой результатов ответа на HTTP-запросы. Зачастую в ответ на «встречный» запрос открывалась панель управления устройством (видеорегистратором, IP-камерой или маршрутизатором). Очевидно, что при составлении статистики нельзя однозначно полагать, что на HTTP-запрос всегда отвечает именно то устройство, которое проводило атаку на honeypot. Во многих случаях можно говорить об использовании технологии

NAT [15] при которой за одним «внешним» IP-адресом находятся несколько атакующих устройств.

На рис. 2 приводится консолидированный график несанкционированных обращений к smart-устройствам.

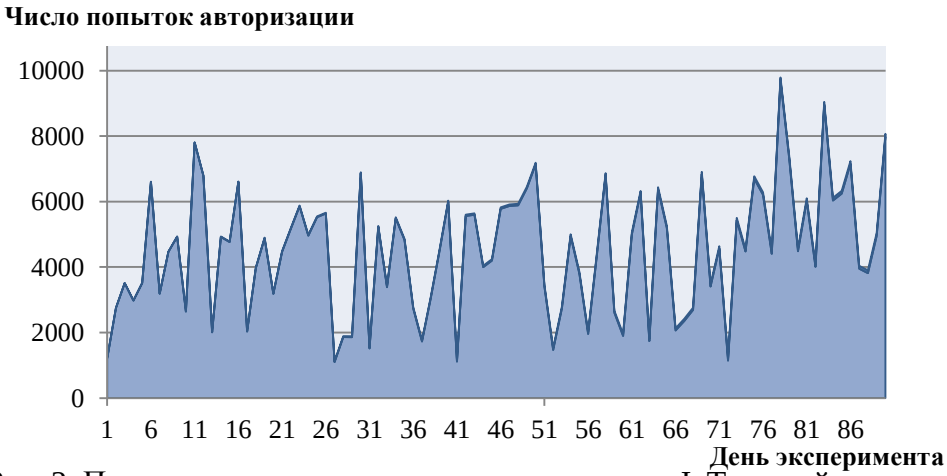

Рис. 2. Попытки несанкционированного доступа к IoT-устройствам.

Более 45% уникальных IP-адресов источников можно определить, как DVR-сервисы или IP-камеры. Более 20% устройств относятся к классу маршрутизаторов и другого сетевого оборудования. Еще около 15% – серверы (в том числе домашние медиа-центры и ТВ-приставки) и рабочие станции пользователей. Категорию оставшихся 20% однозначно идентифицировать не удалось.

Примечательно, что большинство устройств, проводивших атаки на созданную в ходе эксперимента honeypot-ловушку из IoT-устройств, представляют собой бот-сети, объединяющие в себя представителей инфраструктуры Интернета вещей. За три месяца исследований не было зафиксировано ни одной попытки получения RTSP URI [16] потока с камер. Причем, идентификация модели камеры в предоставленной ловушке и процесс получения RTSP-ссылки на сайте производителя не представляли собой трудоемкой задачи. Это еще раз подтверждает отсутствие деятельности человека в выявленных попытках несанкционированного получения доступа. Этому есть объективные объяснения. Высокая эффективность существующих систем и средств противодействия DDoS-атакам подталкивает злоумышленников к поиску новых ресурсов, которые помогли бы им устраивать все более мощные атаки.

Заключение. Количество smart-устройств, составляющих инфраструктуру Интернета вещей, уже сегодня исчисляется миллиардами. К 2020 году аналитики различных компаний прогнозируют их рост в пределах от 20 до 50 миллиардов. Проведенный авторами практический эксперимент позволяет убедиться в том, что на текущий момент огромное количество представителей IoT-инфраструктуры может управляться неизвестными злоумышленниками посредством пула командных серверов. Большинство людей, приобретая IoT-устройства и подключая их в глобальную сеть без включения базовых механизмов обеспечения безопасности, не задумываются о вполне вероятных негативных последствиях.

Безопасность IoT-устройств часто находится на довольно низком уровне. Данное исследование показало, что минимальные действия по размещению smart-устройств за границей межсетевого экрана, смена стандартных паролей и сетевых портов доступа позволяет защититься от воздействий бот-сетей. Экспериментальные атаки на умные лампочки и IP-видеокамеры могут казаться невинными, пока мы не осознаем, что вокруг нас активно развиваются «умные» города. Уже через несколько лет крупные населенные пункты по всему миру могут быть полностью подключенными к сети. Если устройства и системы Интернета вещей не получат должной защиты, злоумышленники смогут получить над ними контроль и

вызвать полный хаос в городах, управляя системами освещения, транспортными потоками и другими информационными системами ключевой инфраструктуры.

Данная работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках проектной части государственного задания ТУСУР на 2017–2019 гг. (проект № 2.3583.2017/4.6).

ЛИТЕРАТУРА

1. Evans D. The Internet of Things. How the Next Evolution of the Internet is Changing Everything" [Electronic resource]. URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (access date: 28.09.2017).

2. Кусков В., Кузин М., Макрушин Д., Шмелев Я., Грачев И. Ловушки «интернета вещей». Анализ данных, собранных на IoT-ловушках «Лаборатории Касперского» [Электронный ресурс]. URL: https://securelist.ru/ honeypots-and-the-internet-of-things/30874/ (дата обращения: 14.10.2017).

3. Zhao K., Ge L. A Survey on the Internet of Things Security // 2013 Ninth International Conference on Computational Intelligence and Security. – 2013. – Pp. 663 – 667.

4. Gupta K., Shukla S. Internet of Things: Security challenges for next generation networks // 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH). – 2016. – Pp. 315 - 318.

5. Anirudh M., Thileeban S A., Nallathambi D. Use of honeypots for mitigating DoS attacks targeted on IoT networks // 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP). – 2017. – Pp. 1 – 4.

6. Тарасенко А. Технология Honeypot, Часть 1: Назначение Honeypot [Электронный ресурс]. URL: http://www.securitylab.ru/ analytics/275420.php (дата обращения: 10.10.2017).

7. Prokofiev A., Smirnova Y., Silnov D. Examination of cybercriminal behaviour while interacting with the RTSP-Server // 2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). – 2017. – Pp. 1 - 4.

8. Iskhakov S., Shelupanov A., Meshcheryakov R. Assessment of security systems complex networks security // Dynamics of Systems, Mechanisms and Machines (Dynamics): Proceeding of the International Scientific and Technical Conference. – 2014. – Pp. 1–4.

9. La Q., Quek T., Lee J. A game theoretic model for enabling honeypots in IoT networks // 2016 IEEE International Conference on Communications (ICC). – 2016. – Pp. 1 - 6.

10. Dowling S., Schukat M., Melvin H. Data-centric framework for adaptive smart city honeynets // 2017 Smart City Symposium Prague (SCSP) . – 2017. – Pp. 1 – 7.

11. Rouse M. DMZ (demilitarized zone) [Electronic resource]. URL: http://searchsecurity.techtarget.com/definition/DMZ (access date: 10.10.2017).

12. Infotecs, ViPNet IDS [Электронный ресурс]. URL: https://infotecs.ru/product/setevye-komponenty/vipnet-ids/ (дата обращения: 10.10.2017).

13. Maini A. K., Agrawal V. Networking Concepts. – 2014. – P. 848.

14. Das R., Tuna G., Packet tracing and analysis of network cameras with Wireshark. – 2017 5th International Symposium on Digital Forensic and Security (ISDFS). – 2017. – Pp. 1 - 6.

15. Ganguly S., Bhatnagar S., Network Address Translation (NAT) and Firewall, VoIP:Wireless, P2P and New Enterprise Voice over IP. – 2008. – P. 276.

16. Schulzrinne H., Rao A., Lanphier R. Real Time Streaming Protocol (RTSP) [Electronic resource]. URL: https://www.ietf.org/rfc/rfc2326.txt (access date: 19.10.2017).