ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Коновалова С.В., Миронов А.Н.

[1]*Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технологический университет» (МИРЭА), 119454, Россия, г. Москва, проспект Вернадского, 78, ksv98@inbox.ru, amironov1993@yandex.ru*

Интернет Вещей, Internet of Things (далее IoT) синоптически представляет собой глобальную инфраструктуру информационного общества, включающую в себя прогрессирующие сервисы физического и виртуального взаимодействия устройств (или «вещей»). Данная инфраструктура целиком и полностью основана на существующих и разрабатываемых информационных и телекоммуникационных технологиях. При этом под термином «вещи» соответственно подразумеваются как объекты физического мира (физические вещи/устройства), так и объекты информационного мира (виртуальные вещи/устройства), которые могут быть идентифицированы и интегрированы в коммуникационные сети.

Ключевые слова: Интернет Вещей, информационная безопасность, IOT-ботнеты.

QUESTIONS OF THE INFORMATION SECURITY OF THE INTERNET OF THINGS

[1]Konovalova S.V., [1]Mironov A.N.

[1]*Federal State Educational Institution of Higher Education "Moscow Technological University" (MIREA), 119454, Russia, Moscow, Vernadscogo avenue, 78,* ksv98@inbox.ru, amironov1993@yandex.ru

Internet of Things synoptically represents a global infrastructure for the informational society, including the advanced services of physical and virtual interconnecting of things. This infrastructure is fully based on existing and evolving interoperable information and communication technologies. Wherein under the term "things" are implied objects of the physical world (physical things) that go with the objects of the virtual world (virtual world). Those things are yet to be identified and integrated into the communication networks.

Key words: Internet of Things, information security, IOT-botnets

В современном мире телекоммуникационные, запоминающие, идентификационные и другие устройства занимают в жизни общества главенствующее положение, в связи с наступлением так называемого «Века Информационных Технологий». Если ранее человеку было необходимо непосредственно взаимодействовать с устройством, то теперь научно-технический прогресс открывает новые возможности. В создаваемых системах предусматривается возможность взаимодействия по новой схеме «устройство-устройство», а не только «человек-устройство». Набор современных информационных и телекоммуникационных технологий, способных обеспечить данный вариант взаимодействия, получил название «Интернет Вещей».

Минимально необходимый набор устройств, который должен включать в себя Интернет Вещей весьма ограничен, так как единственным условием его общности должна быть возможность поддержки коммуникации внутри сети этих самых устройств. Таким образом можно выделить несколько категорий «вещей»:

- **Устройства переноса данных (data-carrying devices)**, которые отвечают за подключение к сети передачи данных.
- **Устройства хранения данных (data-capturing devices)** это запоминающие устройства, которые относятся к типу «считывающих/записывающих» устройств, с возможностью взаимодействия с физическими вещами.
- **Контрольно-измерительная аппаратура (sensing and actuating devices)** это устройства, отвечающие за получение информации, отражающей состояние окружающей среды. Информация кодируется в цифровой сигнал, который позже обрабатывается другими устройствами IoT.
- **Устройства общего назначений (general devices)** могут взаимодействовать с телекоммуникационными системами посредством проводного или беспроводного подключения. Включают

в себя устройства для различных областей Интернета Вещей, таких как промышленное оборудование, домашняя бытовая техника и смартфоны.

Таким образом можно сказать что имеется большое количество устройств, которые соединены между собой, следовательно, к ним должны быть предъявлены уникальные требования по безопасности. Конфиденциальность личной информации, геолокации, также достоверность цифровых подписей и сертификатов устройств Интернета Вещей - все это лишь малая часть того, что должно быть подвергнуто стандартизации.

В современном мире информационная безопасность становится не менее важным аспектом, чем личная физическая безопасность индивида, поскольку с появлением Интернета Вещей виртуальная и физическая среда обитания получают непосредственную связь. Это является одной из причин возникновения потребности в обеспечении высокой безопасности средств взаимодействия с человеком, к примеру, в области медицины (Da Vinci).

Обращаясь к недавним событиям, легко можно проследить серию DDos-атак, самыми интересными и техничными из которых были атаки IoT - ботнетов на базе вирусов типа Trojan.

21 октября мощнейшей DDos-атаке (до 1 Тб/с) , состоящей из двух волн, подверглась инфраструктура DNS-провайдера Dyn. В последствии миллионам пользователей было отказано в доступе к социальным сетям, стриминговым, новостным сайтам и так далее. Виной всему IoT - ботнет Mirai (усовершенствованный Bashlight), который объединил более 100 000 инфицированных IoT - устройств для целенаправленной атаки. Атака осуществлялась с помощью пакетов TCP и UPD, через 53 порт.

Аналогично в начале ноября этого года Либерия подверглась атаке “Ботнет 14” на базе Mirai. Поскольку в Либерии проходит всего лишь один оптоволоконный кабель ACE с общей пропускной способностью 5,1 Тб/с, страна представляет собой своеобразную “песочницу” для тестирования IOT-ботнетов.

Не так давно были опубликованы исходные коды IoT - ботнета Mirai, что позволило провести тщательный анализ. Mirai использует простой, но действенный метод взлома. Он заключается в использовании одинакового, неизменного, установленного производителем по умолчанию пароля для доступа к учетной записи администратора на устройствах типа “интернет вещей”. Используется всего 61 комбинация логин-пароль для доступа к учетной записи методом перебора. Программное обеспечение непрерывно сканирует определенный диапазон IP-адресов для поиска устройств с “вшитыми” учетными данными, после заражения устройство оправляет сообщение в “командный центр”, откуда координируется DDos- атака.

Для примера приведены пароли, которые входят в список “проверяемых” Mirai:

root xc3511
root vizxv
root admin
admin admin
root 888888
root xmhdipc
root default
root juantech
root 123456

Семантический анализ показывает, что пароли хоть и не все являются “слабыми”, но однако же имеются в открытом доступе или выложены в сеть Интернет. В данном случае, элементарного метода перебора из известных комбинаций вполне достаточно, чтобы инфицировать тысячи устройств в считанные дни. Для сравнения, использование слепого метода “brutforce” потребовало бы глобальных вычислительных мощностей и гораздо большего количества времени на “подготовку” атаки.

Обращаясь к анализу последних атак, можно заключить, что одним из основных требований, которые можно предъявить к аспектам информационной безопасности Интернета Вещей является строгая конфиденциальность данных учетной записи администратора IoT - устройства. Таким образом, как вариант реализации требования, имеет смысл включить в стандарты, чтобы данные типа “login-password” генерировались случайно и автоматически, поставлялись в индивидуальном комплекте с устройством и требовали изменения на “пользовательские” при первом подключении устройства. При этом сложность пароля должна быть оценена в терминах информационной энтропии, как достаточная, чтобы метод “brut-force” соответственно также перестал иметь смысл.

Такой алгоритм позволит также защититься от более мощного, чем Mirai, ботнета Aidra, которые впервые был создан, как достаточно этически противоречивое исследование компании Guerilla, чтобы проверить уровень безопасности всего интернета и выявить уязвимости. В процессе тестирования было инфицировано более 400 000 Linux-устройств, что является более чем внушающим результатом. Вредоносное программное обеспечение на базе Aidra получило название Linux/IRCTelnet и действовало аналогично Mirai, но с заметным “улучшением”. Когда устройство было уже заражено, его IP-адрес заносился в базу и оператор ботнета мог свободно заражать его снова и снова до тех пор, пока не потеряет связь с каналом контроля и управления.

Рассматривая Aidra, как следующую ступень эволюции Mirai и Bashlight, можно заключить, что устройства должны быть оборудованы механизмом резервного копирования данных и принудительного разрыва связи, а также обязательной возможностью смены данных учетной записи.

Стоит также обратить внимание на подготовку атаки с помощью LuaBot типа Trojan, ориентированного на заражение Linux-систем и IOT-устройств, работающих на Linux, который также объединяет устройства в ботнет. Распространение происходит в основном на ARM-платформы устройств типа «Интернет Вещей». Ревер-инжиниринг показал, что сервера управления находятся в Нидерландах, но данной информации недостаточно, чтобы найти «автора» данного malware.

Сотрудники передовых лабораторий по обеспечению кибербезопасности заключили, что на данный момент необходимо произвести пять шагов для того, чтобы обезопасить свои устройства / устройства своей организации от кибератак.

- Предотвращение: Компания должна иметь четко выверенный алгоритм действий в чрезвычайной ситуации, а также узнать свои слабые места.
- Введение защитных мер: множество интегрированных механизмов защиты должны гарантировать, что угрозы не смогут проникнуть в информационную сеть.
- Обнаружение: Следует не пренебрегать контекстной информацией о возможных угрозах заражения и своевременно проверять работоспособность устройств.
- Реагирование: При поражении сети вредоносные программы необходимо удалить полностью без каких-либо остаточных следов, а также установить, когда и каким образом было заражено устройство.
- Восстановление: Имеется необходимость проводить периодические сессии резервного копирования данных для последующего восстановления системы или устройства после заражения.

Однако же следует отметить, что данные шаги не являются достаточным условием для обеспечения безопасности устройств типа «Интернет Вещей». Необходима строгая ее стандартизация и расширение аспектов противодействия в первую очередь тем факторам, благодаря которым стали возможны недавние DDos-атаки. Сейчас этим вплотную занимаются в крупных компаниях, например, Kaspersky Lab, Comparex, CROC INC, Эшелон и т.д.

Заключение

В общем, необходимо отметить, что появление устройств класса «интернет вещей» может послужить толчком к новому этапу бурного развития информационных технологий. Однако, надежность и безопасность таких систем должна продумываться еще задолго до их массового внедрения, а основные принципы – закрепляться в национальных и международных стандартах и прочих нормативно-правовых актах.

Список литературы

1. Unleashing the potential of the Internet of Things - / USA - ITU 2016. – 1054 c.
2. Нефедова М. IOT-ботнет на базе трояна Mirai // Xakep – 2016 - №213
3. Кочеткова Е. Кибератака на DNS-провайдера Dyn// Kaspersky Lab Daily [Электронный ресурс] - 2016 URL: https://blog.kaspersky.ru/attack-on-dyn-explained/13471/
4. Литвин П. Информационная безопасность: пять способов защиты от кибератак // Comparex Blog [Электронный ресурс] - 2016 URL:https://habrahabr.ru/company/comparex/blog/314450/
5. Приказ ФСТЭК России от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

References

1. Unleashing the potential of the Internet of Things - / USA - ITU 2016. – 1054 c.
2. Nefedova M. IOT-botnet based on Mirai Trojan // Xakep – 2016 - №213
3. Kochetkova E. Cyberattack on the Dyn DNS-provider // Kaspersky Lab Daily [Electronic resource] - 2016 URL: https://blog.kaspersky.ru/attack-on-dyn-explained/13471/
4. Litvin P. Information Security: five steps to defend yourself from cyberattacks // Comparex Blog [Electronic resource] - 2016 URL:https://habrahabr.ru/company/comparex/blog/314450/
5. Prikaz FSTEK Rossii ot 14 marta 2014 g. N 31 «Ob utverzhdenii trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"ektakh, potentsial'no opasnykh ob"ektakh, a takzhe ob"ektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudey i dlya okruzhayushchey prirodnoy sredy»