УГРОЗА БОТНЕТОВ ДЛЯ IOT-УСТРОЙСТВ

Чаган Н. Ф., Белоусова Е. С.
Кафедра защиты информации,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: chagan_nf@pac.by, belousova@bsuir.by

В материалах доклада рассматривается развитие интернета вещей с представлением подробной статистики по количеству IoT-устройств и прогнозом их увеличения в ближайшие несколько лет. Особо уделяется внимание проблеме кибербезопасности интернета вещей, а именно механизму формирования ботнетов, таких как AISURU, в сетях с IoT-устройствами. На основе оценки последствий кибератак, реализованных посредством ботнета AISURU, описывается проблема необходимости создания подходов и средств по обеспечению безопасности интернета вещей.

Введение

В настоящее время создание моделей будущего, где общество сформировало общественный строй, члены которого живут комфортной жизнью с максимальной автоматизацией и интеграцией информационных систем, уже не представляется чем-то нереальным. В условиях стремительного развития искусственного интеллекта, интернета вещей IoT (Internet of Things) и автоматизированных систем уже представляется возможным построение модели, основанной на объединении физических и виртуальных объектов в единую инфраструктуру – киберфизическую систему, обеспечивающую оптимизацию ресурсов и повышение качества жизни.

Основная часть

Интернет вещей уже активно проникает в различные сферы жизнедеятельности человека. На текущий момент наблюдается экспоненциальный рост умных устройств интернета вещей. По данным сервиса Statista [1], в настоящее время в мире насчитывается порядка 19,8 млрд. подключенных IoT-устройств. Таким образом, количество устройств, которые подключены к сети Интернет, уже превышает более чем вдвое население Земли. С течением времени эта разница будет только увеличиваться в геометрической прогрессии. По прогнозу (рис. 1) к 2030 году таких устройств будет насчитываться более 31,2 млрд [1], что обусловлено стремлением производителей к совершенствованию производимых ими IoT-устройств с целью получения конкурентного преимущества.

Однако вместе с перспективами и возможностями развития IoT неизбежно возникают новые социальные, этические и экономические проблемы. Также развивается зависимость человека от интеллектуальных систем, которая ставит под угрозу конфиденциальность и безопасность персональных данных.

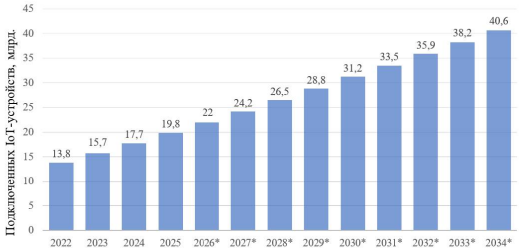

Рис. 1 – Количество устройств, подключений к Интернету вещей по всему миру в период с 2022 по 2024 гг. с прогнозами на период с 2025 по 2034 гг.

Каждый год нарушители получают доступ к миллионам устройств по всему миру, превращая их в ботнеты, или так называемые «зомби-сети». Таким образом нарушители осуществляют свои противоправные действия в отношении организаций, осуществляют кражу персональных данных, нарушают работу важных информационных систем либо манипулируют процессами. Любое устройство, подключенное к сети Интернет, может стать элементом ботнета без ведома пользователя. Происходит это скрытно, в процессе функционирования взломанного устройства, которое при этом выполняет указания киберпреступников.

Создание ботнета является лишь шагом к достижению конечной цели нарушителя. Сформировав мощную инфраструктуру, появляются способы не только проводить различные кибератаки, такие как DDoS, спам, кража данных и т.д., но и заниматься процессом масштабирования ботнета с целью последующей продажи или аренды другим нарушителям.

Примером зафиксированной DDoS-атаки является ботнет AISURU. По оценкам исследователей QiAnXin XLab [2], в данном ботнете оказались порядка 300 тыс. маршрутизаторов по всему миру. В основном использовались уязвимости N-day в IP-камерах и маршрутизаторах D-Link, Linksys, Zyxel, SDK Realtek, а именно уязвимости CVE-2017-5259 [3] в устройствах Cambium, CVE-2023-28771 [4] в оборудовании Zyxel, CVE-2023-50381 [5] в SDK Realtek Jungle. К ботне-

ту AISURU оказались подключенными видеорегистраторы nvms9000, ранее относившиеся к другому ботнету RapperBot. Для повышения пропускной способности трафика операторы задействовали GRE-туннели, которые были установлены на четырёх командных узлах.

Стоит учитывать, что весной 2025 года ботнет AISURU проводил волну кибератак [2] мощностью 5,8 Тбит/с, в сентябре мощность увеличилась почти вдвое и достигала 11,5 Тбит/с, в октябре произошло очередное более чем двукратное увеличение мощности атаки – 29,69 Тбит/с, что на данный момент является новым рекордом.

Потенциальные жертвы для формирования ботнетов выбираются случайным образом. В настоящее время отсутствуют свидетельства того, что целью нарушителя является какая-либо конкретная отрасль или страна. География кибератак затрагивает организации таких стран, как Китай, США, Великобритания, Германия. Несмотря на это, можно смело сказать, что защита крупнейших игровых и облачных платформ в настоящее время находится под угрозой кибератак данного или аналогичного ботнета, так как атака, проведенная 6 октября 2025 года, которая затронула игровые сервисы Steam (рис. 2), Xbox (рис. 3), Riot Games, PlayStation Network и другие популярные онлайн-сервисы согласно информации онлайн системы мониторинга сбоев онлайн-сервисов Downdetector [6].

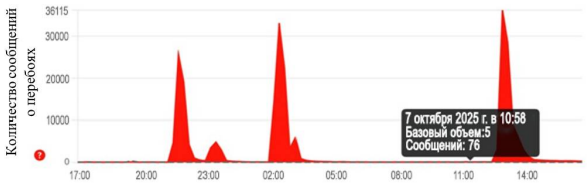

Рис. 2 – Количество сообщений о перебоях в работе сервиса Steam в сравнении с базовым объемом

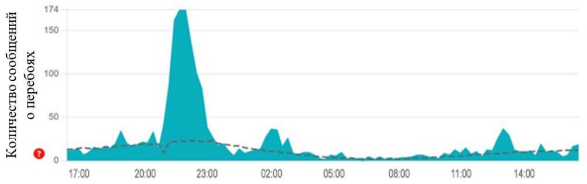

Рис. 3 – Количество сообщений о перебоях в работе сервиса Xbox в сравнении с базовым объемом

В результате кибератаки по всему миру пользователи испытывали трудности с входом в их игровые аккаунты, подключением к игровым магазинам и серверам. Геймеры жаловались на невозможность подключения к таким платформам, как Counter-Strike, Dota 2, Valorant, League of Legends и др.

Интересным является подход к маскировке ботнета. Вредоносное программное обеспечение проверяет наличие анализаторских инструментов или виртуальных сред и прекращает свое функционирование при их обнаружении. Также используются TCP Carpet Bomb-атаки [7], имитирующие легитимный трафик. С марта 2025 года нарушители внедрили два крупных обновления, направленных на усиление шифрования и изменение сетевого протокола. Одной из характерных черт AISURU является использование модифицированного алгоритма RC4 со статическим ключом PJbiNbbeasddDfsc.

Несмотря на то, что AISURU является наглядным примером злонамеренного использования IoT-устройств, он далеко не единственный в своем роде. В даркнете продолжают формироваться и другие ботнеты. Эти сети действуют незаметно, накапливая ресурсы и охватывая все больше уязвимых устройств. Неизвестно, когда именно, при каких условиях и с какой целью они будут активированы, что делает угрозу еще более тревожной и непредсказуемой.

Заключение

Ботнеты не являются принципиально новой угрозой, но в то же время выходят за рамки обычного инструмента для целенаправленных атак на IoT-устройства и представляют собой многофункциональную платформу. Для эффективного противодействия данной нарастающей угрозе требуются конкретные оперативные действия в сфере кибербезопасности по созданию подходов и средств, позволяющих обеспечить защиту информации, в том числе совместные действия международного сообщества и правоохранительных органов.

1. Компания Statista [Электронный ресурс]. – Режим доступа: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. – Дата доступа: 15.10.2025
2. Компания XLab [Электронный ресурс]. – Режим доступа: https://blog.xlab.qianxin.com/super-large-scale-botnet-aisuru-en/. – Дата доступа: 15.10.2025
3. The National Institute of Standards and Technology (NIST). – [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE-2017-5259. – Дата доступа: 15.10.2025
4. The National Institute of Standards and Technology (NIST). – [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE-2023-28771. – Дата доступа: 15.10.2025
5. The National Institute of Standards and Technology (NIST). – [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/CVE-2023-50381. – Дата доступа: 15.10.2025
6. Компания Downdetector [Электронный ресурс]. – Режим доступа: https://downdetector.com. – Дата доступа: 15.10.2025
7. Российский портал SecurityLab.ru [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/glossary/carpet_bombing/. – Дата доступа: 15.10.2025