УДК 004.056.5

L.U. Molkova, E.D.Pasechnic

PROBLEMS OF NEGATIVE IMPACT AND ECONOMIC HARM CAUSED BY BOTNETS

Currently, malicious bots pose a serious threat in the field of information security due to the fact that they are used for such crimes on the Internet as fraud, extortion, blocking the Internet resources of enterprises, which leads to a deterioration in the reputation of enterprises and the inability to fully implement business processes. Thus, at the present stage of development of information systems and information protection, detection and elimination of malicious bots is one of the most pressing tasks. This article discusses the architecture of malicious bots and possible ways to destroy them.

Keywords: malware; botnets; botnet; botmaster; DDoS attack, Internet traffic tags.

Л.Ю. Молькова[1], Е.Д. Пасечник[2]

ПРОБЛЕМЫ НЕГАТИВНОГО ВОЗДЕЙСТВИЯ И ЭКОНОМИЧЕСКОГО ВРЕДА, НАНОСИМОГО БОТНЕТАМИ

В настоящее время серьёзную угрозу в области информационной безопасности представляют вредоносные боты, в связи с тем, что они используются для таких преступлений в интернете как мошенничество, вымогательство, блокирование интернет-ресурсов предприятий, что приводит к ухудшению репутации предприятий и невозможности полноценной реализации бизнес-процессов. Таким образом, на современном этапе развития информационных систем и защиты информации обнаружение и ликвидация вредоносных ботов является одной из наиболее актуальных задач. В данной статье рассмотрена архитектура вредоносных ботов и возможные способы уничтожения их.

Ключевые слова: вредоносные программы; бот-сети; ботнет; ботмастер; DDoS-атака, метки интернет трафика.

DOI: 10.36807/2411-7269-2024-2-37-200-203

В настоящее время проблемы обеспечения информационной безопасности становятся всё более актуальными. Постоянно увеличивающиеся потоки информации, применение передачи огромного объёма информации через сети интернет несут в себе определённые риски информационной безопасности, которые постоянно возрастают. В связи с постоянно возрастающими рисками информационной безопасности необходимо ставить новые задачи по защите передаваемой информации. Эффективная и надёжная доставка данных и информации является одной из приоритетных задач обеспечения целостности информации и безопасности информационных систем. Один из методов обеспечения безопасной передачи данных в сети интернет – это маркирование пакетов данных, передаваемых по сети. Маркирование сетевых потоков обеспечивает эффективное функционирование IT-инфраструктуры. Маркирование пакетов данных в сети даёт возможность проводить идентификацию трафика исходя из таких параметров как источник, назначение, протокол, тип сервиса и приложение. Действия по маркированию сети дают возможность оптимизировать сетевую нагрузку и обеспечивают применение политик безопасности [1].

За последние несколько лет произошло существенное развитие искусственного интеллекта в сфере информационных технологий. Одним из направлений в развитии технологий искусственного интеллекта является создание различных ботов – программ, которые способны в автоматическом режиме самостоятельно выполнять определённый перечень задач, которому они заранее обучены. Зачастую такие программы способны моделировать поведение пользователя. В современных условиях боты нашли широкое применение в обеспечении различных бизнес-процессов и решении бизнес-задач. Однако, технологи искусственного интеллекта, боты применяют не только добропорядочные компании для оптимизации и ускорения бизнес-процессов. Подобные техноло-

[1] Молькова Л.Ю., преподаватель ИСПО, ФГАОУ ВО "Санкт-Петербургский политехнический университет Петра Великого", г. Санкт-Петербург

Molkova L.U., lecturer of ISVE, D. Eng.; Federal State Autonomic Educational Institution of Higher Education "Peter the Great St.Petersburg Polytechnic University (SPbPU)", Saint-Petersburg

E-mail: lolita-molkova@mail.ru

[2] Пасечник Е.Д., ассистент кафедры бизнес-информатики; ФГБОУ ВО "Санкт-Петербургский государственный технологический институт (технический университет)", г. Санкт-Петербург

Pasechnic E.D., Assistant of the Department of Business Informatics; Federal State Budgetary Educational Institution of Higher Education "Saint-Petersburg Federal State Institute of Technology (Technical University)", Saint-Petersburg

E-mail: kate.pasechnik@yandex.ru

гии также используют различного рода злоумышленники. Существуют различные типы вредоносных ботов, которые используют злоумышленники. Вредоносные и интернет-боты приносят существенный вред и угрожают защищённости учётных записей пользователей на различных интернет-платформах и сервисах, способны искать персональные данные людей в интернете с целью несанкционированного использования, а также рассылать спам от лица пользователей. Можно перечислить основные типы вредоносных ботов: спам-боты, вредоносные чат-боты, боты для обмена файлами и др. [1].

Бот-сети на настоящий момент представляют собой одну из самых больших угроз информационной безопасности в сети интернет, бот-сети используются злоумышленниками для подавляющего количества преступлений в сети интернет. Теневые преступные организации используют бот-сети для проведения DDoS-атак, рассылки спама, запуска шпионских программ, мошенничества с кликами и других атак. Рост числа кибератак и киберпреступлений, несанкционированного автоматического сбора и распространения цифровой информации становится всё более распространённым среди киберпреступников. Они могут использовать собранную информацию для финансовых мошенничеств, кражи личных данных, шпионажа и других преступных действий. В связи с этим, разработка методов и моделей противодействия такому сбору и распространению становится необходимой.

Для защиты от вредоносных программ в современных условиях необходимо применять комплексы информационных систем. Например, высокой эффективностью защиты данных при передаче данных обладает система, помогающая классифицировать данные по различным критериям с использованием специальных меток. Использование меток при передаче пакетов данных способствует отражению кибератак на информационные системы, а также повышает уровень надёжности информационной системы, в которой хранятся и передаются данные [2].

Сети ботнет

Для того чтобы разработать информационную систему защиты от воздействия вредоносных ботов, необходимо в первую очередь понять принцип их вредоносного воздействия. Компьютерная сеть, в которой действуют боты, называется ботнет.

Компьютерная вредоносная сеть ботнет состоит из таких компонентов как бот, ботмастер и каналы управления и контроля.

Ботнет – компьютерная сеть, скоординированная группа взломанного хоста, которая связывает бот и ботмастер. Ботнет координируется ботмастером и используется им как платформа для осуществления вредоносных действий и атак.

Бот – это компьютер, который может быть заражён вредоносным программным компонентом, которым можно удалённо управлять с целью нападения, реализации несанкционированных действий. Боты применяются в тех случаях, когда необходима высокая скорость ответа, которую не могут обеспечить действия человека, но может обеспечить компьютер. Бот во вредоносных сетях представляет собой компьютер, заражённый вредоносной программой, которая по "указанию" ботмастера "руками" компьютера-бота осуществляет вредоносные действия. Бот в данной схеме является лишь средством исполнения вредоносных действий, координатором вредоносных действий является ботмастер.

Ботмастер – компьютер или сервер, который заражает компьютеры, находящиеся в сети, вредоносной бот-программой, после чего заражённые компьютеры становятся инфицированными ботами и начинают выполнять вредоносные действия в сети на основе команд от ботмастера.

Любой компьютер подключённый к сети интернет может быть заражён вредоносным ботом и начать выполнять вредоносные действия, продиктованные ботмастером. Таким образом, ботмастер "прикрывается" IP-адресом компьютера-бота, при обнаружении атаки обнаруживается в первую очередь компьютер-бот, который всего лишь является исполнителем атак и в случае обнаружения и устранения бота, ботмастер создаст нового бота. Такая схема позволяет ботмастеру долго быть необнаруженным. В настоящее время системы обнаружения угроз направлены на обнаружение вредоносных ботов, но при этом данный способ не является полностью эффективным. Таким образом, перспективным и актуальным направлением исследований и разработок является создание способов борьбы не с ботами, а именно с ботмастерами в сети.

По топологии командной сети ботнеты можно разделить на ботнеты с тремя типами сетевой архитектуры:

а) централизованная;

б) децентрализованная;

в) гибридная.

На Рис. 1 показаны топологии сетей ботнет, где Botmaster – ботмастер, Bot – бот, C&C (command-and-control) communication channel – канал связи управления и контроля, C&C servers – C&C сервер, Proxy bots – прокси бот, Working bots – бот-исполнитель.

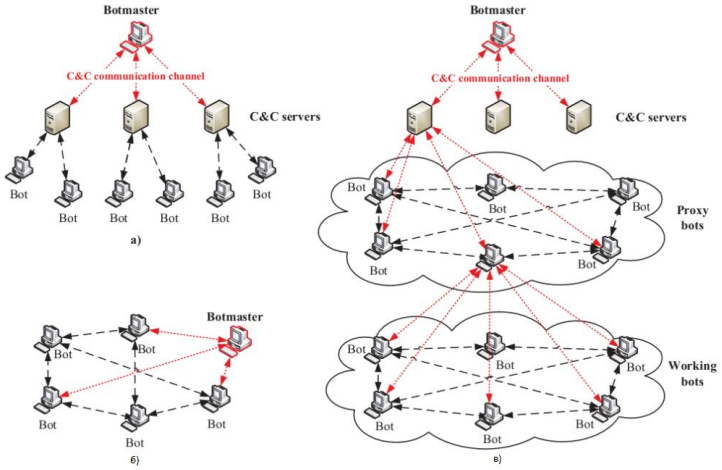

Рисунок 1 – Топологии сетей ботнет

Канал управления и контроля (C&C Channel) является основным средством связи и обеспечения в работе вредоносной сети ботов и он представляет собой канал связи, установленный между бот-мастером и скомпрометированными хостами (компьютерами-исполнителями вредоносной программы). Этот канал используется злоумышленником для выдачи команд ботам и получения информации от скомпрометированных компьютеров. C&C канал обеспечивает удалённую координацию большого количества ботов и обеспечивает уровень гибкости в операциях ботнетов, создавая возможность изменять и обновлять код вредоносного ботнета.

Наиболее распространённый способ реализации управления (C&C Channel – использование протокола Internet Relay Chat (IRC). В рамках реализации ботнетов посредством протокола IRC ботмастер использует данный протокол для передачи команд ботам, ответ от ботов направляется по данному протоколу обратно ботмастеру как широковещательные или как личные сообщения.

Методы обнаружения и защиты от создания бот-сетей до сих пор остаются сложными и ресурсозатратными, в связи с чем остаётся проблема в обнаружении бот-сетей, которые используют в качестве платформы домашние компьютеры пользователей и компьютеры компаний с простой IT-инфраструктурой, так как данная группа пользователей зачастую не имеет возможностей противостоять подобным атакам.

В последние несколько лет наблюдается существенное увеличение количества компьютерных атак, проведённых с помощью бот-сетей. Как правило, проводятся DDoS-атаки, которые чаще всего затрагивают такие сферы, как электронная коммерция, игровые сервисы, образовательные платформы [11]. Например, в 2020 г. данные сегменты в мире значительно пострадали от вредоносного воздействия DDoS-атак. Оценить ущерб от подобных атак можно в объёме не менее 600 000 руб. в сутки.

Рассматривая наиболее крупные мировые DDoS-атаки на известные информационные ресурсы, стоит отметить, что в 2020 г. на информационную систему компании Amazon была направлена одна из крупнейших DDoS-атак объёмом 2.3 Тб/с.

Другая крупнейшая за последние несколько лет DDoS-атака объёмом 809 MPPS (миллионов пакетов в секунду) была исполнена в июне 2020 г. в отношении мировых финансовых организаций. Важной особенностью этой атаки с технической стороны было то, что она была реализована более чем на 90% с помощью тех компьютеров, IP адреса которых ранее не были замечены в участии в подобных атаках, что говорит о том, что на базе "ничего не подозревающих" компьютеров была основана сеть ботнет, которая осуществляла данную атаку.

IT-аналитики по всему миру сходятся во мнении, что с 2020 г. существенно возросло количество DDoS-атак и в масштабах всего мира увеличилось до 20-30% от числа всех вредоносных атак, которые существуют в сетях Интернет.

Наибольшую угрозу вредоносные боты и произведённые ими DDoS-атак стали представлять именно в 2020-м пандемийном году, когда большая часть экономической деятельности перешла в сферу онлайн, для того чтобы продолжить деятельность и не потерять прибыль в условиях ковидных ограничений. От вредоносных атак в 2020 г. особенно пострадали те предприятия, деятельность которых стала максимально зависеть от Интернет-ресурсов. Наиболее пострадали от воздействия вредоносных ботов такие сферы экономической деятельности как торговля, развлекательная сфера, IT-сфера, также существенно пострадали образовательные ресурсы, информационные системы медицины. Основной целью проведения DDoS-атак является вымогательство [3], [4].

Разработка систем защиты от вредоносных ботов – является сложной задачей для специалистов в сфере информационной безопасности, но при этом экономически обоснованной и необходимой [9], [10].

В настоящее время производятся различные разработки в области защиты от вредоносных ботов. Одним из методов защиты является использование коллаборативного сетевого водяного знака. Данный метод позволяет обнаруживать бот-сети, основанные на протоколе IRC.

Водяной знак – это уникальная метка, встраиваемая в интернет-трафик, которую не видят пользователи и злоумышленники. Метод водяных знаков используется в системе BotMosaic, использующей принцип коллаборации множества хостов (узлов) для создания сетевого водяного знака. Водяной знак из BotMosaic позволяет обнаруживать и идентифицировать в трафике сети наличие ботнетов благодаря внедрению водяных знаков в обычный трафик сети ботов, далее происходит сбор информации о водяных знаках с помощью сети хостов-наблюдателей, и наконец, анализ для обнаружения ботнета. Существенным преимуществом метода BotMosaic является возможность обнаружения ботнетов, даже если в них злоумышленниками изменены протоколы и структура. Использование водяных знаков в трафике сети даёт возможность обнаружения истинных IRC-каналов ботнетов, которые могут быть скрыты. Таким образом, можно утверждать, что метод внедрения в сетевой трафик водяных знаков BotMosaic является эффективным инструментом для выявления сетей ботнет и противодействия им [8].

Список использованных источников

1. Коломеец М.В., Чечулин А.А. Метрики вредоносных социальных ботов. Труды учебных заведений связи, 2023. – 9(1). – С. 94-104. https://doi.org/10.31854/1813-324X-2023-9-1-94-104.
2. Vitkova L. Kolomeec M., Chechulin A. Taxonomy and Bot Threats in Social Networks // Proceedings of the International Russian Automation Conference (RusAutoCon, Sochi, Russia, 04-10 September 2022). IEEE, 2022. PP. 814-819. DOI: 10.1109/RusAutoCon54946.2022.9896268.
3. Мустафаев А.Г. Система обнаружения вредоносных ботнет на основе интеллектуального анализа данных и машинного обучения // ПРОМЫШЛЕННЫЕ АСУ И КОНТРОЛЛЕРЫ. – Издательство "Научтехлитиздат". – ISSN: 1561-1531. – 2018. – С. 20-26.
4. Felix Leder. Proactive botnet countermeasures: an offensive approach / Felix Leder, Tillmann Werner, Peter Martini // Institute of Computer Science IV. University of Bonn. Germany. 2009.
5. Галиахметов Д.Г. Сравнение алгоритмов классификации применительно к задаче обнаружения вредоносных доменных имен // Математические методы в технике и технологиях – ММТТ. – М.: Саратовский государственный технический университет имени Гагарина Ю.А. – 2019. – С. 190-194.
6. Коломеец М.В., Чечулин А.А. Компонент обнаружения метрик ботов в социальной сети. Свидетельство о регистрации программы для ЭВМ RU 2022681600, 15.11.2022.
7. Замолоцких В.С., Сидоренко В.Г. Киберугрозы в социальных сетях // Информатизация образования и науки. – М.: Федеральный институт цифровой трансформации в сфере образования, 2020. – С. 66-75.
8. Amir Houmansadra, Nikita Borisovb. BbotMosaic: Collaborative network watermark for the detection of IRC-based otnets // The Journal of Systems and Software. – Elsevier. The Netherlands – 2013.
9. Massi J., Panda S., Rajappa G., Selvaraj S., Revankar S. Botnet Detection and Mitigation. Proceedings of Student-Faculty Research Day. Available at: http://csis.pace.edu/ctappert/srd2010/c4.pdf (accessed 04.11.2014).
10. Котенко И.В., Коновалов А.М., Шоров А.В. Исследовательское моделирование бот-сетей и механизмов защиты от них // Новые технологии. – 2012. – № 1. – Приложение к журналу Информационные технологии, 32 с.
11. Гончаров Н.О. Современные угрозы бот-сетей / Молодёжный научно-технический вестник // Академия инженерных наук им. А.М. Прохорова. – 2014. – С. 34.