«Кодекс поведения против программ-роботов для провайдеров интернет-услуг в США» с целью реагирования в порядке добровольного участия на угрозы, связанные с бот-программами и ботнетами в местных широкополосных сетях

Итоговый отчет

22 марта, 2012

1. Введение

Рост числа устройств конечных пользователей*, зараженных бот-программами*, создает значительную угрозу жизненно важным функциям и устойчивой работе Интернета и сетевой экономической деятельности. Следует заметить, что «заражение бот-программой» и «бот программа» используются в данном документе синонимически для обозначения устройства конечного пользователя, зараженного ботовым вредоносным программным обеспечением. «Ботнеты» представляют собой зараженные ботовым вредоносным программным обеспечением сетевые образования компьютерных устройств конечных пользователей, подключенных к Интернету, которые контролируются по удаленному доступу третьими сторонами в пагубных целях.

Использование бот-программ и ботнетов может привести к похищению персональных данных, атакам на открытые и закрытые сетевые системы, а также эксплуатации компьютерных мощностей и доступа в Интернет конечных пользователей. Осведомленность общества о бот-программах, их воздействии и вытекающим отсюда проблемах, связанных с безопасностью и конфиденциальностью находится на низком уровне. Данный добровольный Кодекс поведения («Кодекс») предлагает совокупность принципов и рекомендованных действий, которые провайдеры интернет-услуг могли бы принять с целью отражения угрозы, представляемой наличием бот-программ и ботнетов в местных широкополосных сетях.

Необходимо понимать, что бот-программы воздействуют на всю экосистему Интернета*, и что успешное сокращение числа бот-программ или снижение их воздействия потребует коллективного действия от всех составляющих этой экосистемы, включая конечных пользователей, разработчиков программного обеспечения, поисковых провайдеров, веб-сайтов, сайтов электронной торговли и других. Устройства конечных пользователей находятся вне контроля провайдеров интернет-услуг, поэтому все участники экосистемы Интернета должны сотрудничать в реагировании на указанную проблему. Данный Кодекс нацелен на то, чтобы положить основание для будущей координации между различными заинтересованными сторонами путем определения комплекса мер,

надлежащим образом соотнесенных с ограниченной ролью, которую могут играть провайдеры интернет-услуг при реагировании на эту важную проблему. Кодекс признаёт существенное разнообразие в объеме, ресурсах, бизнес-моделях и средах, опыте и возможностях провайдеров интернет-услуг в США. Успех деятельности провайдеров интернет-услуг зависит от сходных усилий других заинтересованных участников Интернета.

Основные требования для участия в данном Кодексе изложены в разделе 5. Другие разделы данного документа содержат справочную информацию или дополнительный пояснительный материал.

2. Определения ключевых терминов

Примечание для читателя:

Любая дискуссия о бот-программах неизбежно сопровождается использованием специального технического словаря. Осознавая, что многие читатели могут не быть знакомы с некоторыми из таких специальных терминов, составители Кодекса включили в него глоссарий, в качестве Приложения 2. Всякий термин, имеющийся в глоссарии, будет помечен звездочкой «*» в тексте самого Кодекса при первом появлении, в качестве способа предупреждения читателя о том, что определение можно найти в глоссарии.

3. Задачи и принципы

a. Задачи данного Кодекса:

1. Определить исходные рамки, в которых провайдеры интернет-услуг могут достичь большего понимания проблемы бот-программ и способствовать реагированию на нее; и

2. Призвать провайдеров интернет-услуг

- Информировать конечных пользователей об угрозе, которую представляют бот-программы, и обучать их способу действия, способствующего предотвращению заражению бот-программами
- Обнаруживать активность бот-программ или получать информацию, в т. ч. от заслуживающих доверия третьих сторон, о заражении бот-программами в базе их конечных пользователей
- Уведомлять конечных пользователей о подозрении на зараженность бот-программами или содействовать конечным пользователям в диагностике того, что они могут подвергнуться заражению бот-программой; а также

- Обеспечивать, непосредственно или путем ссылки на другие ресурсы, конечных пользователей информацией и ресурсами для содействия им в устранении заражения бот-программой.

б. Внедрение Кодекса будет проводиться по следующим принципам:

1. Добровольность – участие в Кодексе носит добровольный характер и, несмотря на то, что данный Кодекс не требует никаких конкретных действий, поощряет определенный образ действий, которые могли бы предпринимать провайдеры интернет-услуг.

2. Технологическая неангажированность – данный Кодекс не предписывает никаких конкретных технических средств и методологий

3. Неангажированность подхода – данный Кодекс не предписывает никаких конкретных подходов для внедрения любой части Кодекса.

4. Внимание к вопросам конфиденциальности – провайдеры интернет-услуг должны затрагивать вопросы, связанные с конфиденциальностью, надлежащим образом, согласующимся с применимым законодательством.

5. Соответствие законодательству – деятельность должна соответствовать применимому законодательству.

6. Общая ответственность – провайдеры интернет-услуг, действующие поодиночке, не могут в полной мере отреагировать на угрозу, которую представляет бот-программа. Другие участники экосистемы Интернета также должны исполнить свою роль.

7. Экономическая дееспособность – провайдеры интернет-услуг должны стремиться к тому, чтобы их деятельность была рентабельной и устойчивой в рамках их бизнес-моделей

8. Обмен информацией – провайдеры интернет-услуг должны указывать, каким образом они собираются участвовать в Кодексе, и делиться полученными при своей работе знаниями и опытом с другими надлежаще заинтересованными сторонами. Весь обмен информацией между провайдерами интернет-услуг и

другими вовлеченными сторонами должен происходить в соответствии с применимым законодательством, включая, но не ограничиваясь, антимонопольными законами и нормами, защищающими конфиденциальность.

9. Эффективность – необходимо побуждать провайдеров интернет-услуг принимать участие в деятельности, доказавшей соответствие своей цели и эффективность.

10. Эффективная коммуникация – в общении с клиентами * необходимо принимать во внимание разные аспекты, такие как язык, и добиваться того, чтобы информация предоставлялась тем способом, каким она может быть понята и принята получателем в своем достоверном виде.

4. Круг вопросов и роли

Данный Кодекс был составлен с учетом особенностей провайдеров интернет-услуг и прочих услуг, предоставляющих услугу доступа к широкополосному Интернету для местных конечных пользователей. Деятельность согласно данному Кодексу можно адаптировать для других интернет-провайдеров и участников.

Проект данного Кодекса не предусматривает того, что он станет всеобъемлющим подходом к онлайн-безопасности. Он должен встать в один ряд с другими текущими и будущими усилиями в этом направлении. Он предусматривает значимую роль для других участников экосистемы Интернета, включая, но не ограничиваясь:

- Поставщиков программного обеспечения для безопасности
- Разработчиков операционных систем
- Организации, ориентированные на конечных пользователей
- Провайдеров интернет-контента, приложений и услуг

Онлайн-безопасность должна содержать в себе многогранный, эластичный подход с использованием рекомендаций и инструментов от различных источников, обладающих хорошей репутацией.

a. Определение успешности

Первоначальный успех данного Кодекса должен быть оценен при участии сообщества провайдеров интернет-услуг. Широкая поддержка экосистемы Интернета, тем не менее, представляется высшим проявлением успеха в борьбе против бот-программ.

б. Преимущества участия в Кодексе

Полномасштабное участие в данном Кодексе может дать следующие высшие преимущества:

- Возросший уровень безопасности для информации и устройств конечных пользователей, а также для инфраструктуры США;
- Возросший уровень осведомленности об угрозе, связанной с бот-программами, а также о том, как ей противостоять, для конечных пользователей, провайдеров интернет-услуг и иных участников отраслей, связанных с использованием Интернета;
- Уведомление* о деятельности бот-программ на зараженных бот-программами устройствах конечных пользователей и устранение* ее;
- Создание среды в местных широкополосных сетях США, которая была бы особенно неблагоприятна к установке и использованию бот-программ; а также
- Разработка и широкое использование эффективной архитектуры и инструментов уведомления и устранения среди конечных пользователей и провайдеров интернет-услуг.

Некоторые провайдеры интернет-услуг, участвующие в разработке Кодекса, которые прежде внедрили ряд положений Кодекса, получили благоприятные результаты в таких аспектах, как снижение числа обращений в службы технической поддержки со стороны клиентов с зараженными компьютерами, уменьшение потребления пропускной способности исходящего канала DDoS атаками и спамом*, возросший уровень клиентского доверия и снижение оттока клиентов, а также уменьшение числа жалоб, связанных со спамом, от других провайдеров интернет-услуг. Несмотря на то, что отдельные результаты могут варьироваться, провайдеры интернет-услуг призываются к тому, чтобы искать те особенные способы, с применением которых участие в Кодексе может способствовать их общему уровня бизнеса в области широкополосного Интернета, а также к тому, чтобы делиться этим опытом с другими провайдерами. Более того, участие провайдеров интернет-услуг в данном Кодексе может позволить им выработать реальные параметры в отношении воздействия специфической деятельности на общий уровень бизнес-операций в области широкополосного Интернета. Это, в свою очередь, может ускорить разработку или реализацию наиболее действенных мер для противостояния бот-программам.

5. Параметры участия

Участие в данном Кодексе носит добровольный характер.

Требования, необходимые для участия в добровольном Колексе Поведения

Чтобы участвовать в данном Кодексе, провайдер интернет-услуг должен применить хотя бы одну меру (т. е. предпринять существенное действие) в каждой из следующих общих областей:

- Обучение – деятельность, направленная на содействие росту уровня навыков и осведомленности конечного пользователя в отношении проблем, связанных с ботнетами, а также на содействие в предотвращении заражения бот-программами;
- Обнаружение – деятельность, направленная на регистрирование функционирования ботнета в сети, подведомственной провайдеру интернет-услуг, или на предоставление конечным пользователям возможности самостоятельно обнаружить заражение бот-программой на своих устройствах;
- Уведомление – информирование клиентов о предполагаемом заражении бот-программой, или предоставление клиентам возможности определить, заражено ли их устройство бот-программой;
- Устранение – предоставление конечным пользователям информации о том, как им устранить заражение бот-программой, или содействие конечным пользователям в устранении заражения бот-программой.
- Сотрудничество – передача другим провайдерам сведений об обратной связи и опыте, полученных в результате деятельности провайдера интернет-услуг, участвующего в Кодексе.

Концепция проведения «хотя бы одной меры» в каждой из данных общих областей имеет своей целью призвать к достижению определенного уровня деятельности в каждой из пяти вышеуказанных областей. Это составляет часть общенационального процесса создания в местных сетях широкополосного Интернета США среды, которая была бы наиболее неблагоприятна для установки и использования бот-программ. Она предназначена для оказания поддержки и поощрения широкого спектра удобоприменимых усилий для экспериментирования и инноваций в отношении различных методов обучения, обнаружения*, уведомления и устранения. Соответственно тому, требование делиться с другими провайдерами данными обратной связи не направлено на принуждение к определенным средствам и методам осуществления такого обмена информацией об обратной связи.

6. Обучение конечных пользователей

a. Краткий обзор

Конечные пользователи несут основную ответственность за защиту своих устройств и за исправление их в случае заражения. Провайдеры интернет-услуг, подобно многим другим участникам Интернета и правительственным работникам, могут содействовать обучению конечных пользователей на предмет угроз, которые представляют бот-программы, и шагов, которые могут предпринять конечные пользователи для сохранности своих устройств и устранения их заражения.

б. Рекомендуемые действия:

1. Обучение предотвращению* заражения бот-программой:

Провайдеры интернет-услуг должны дать доступ к информации о предотвращении заражения бот-программой и сопряженных с этим вопросах. Как минимум, эта информация должна включать в себя:

- Как и почему конечные пользователи должны поддерживать для своего программного обеспечения необходимый уровень обновлений, установленный для компьютеров и устройств с программным обеспечением, легко доступным для обновления.
- Важность использования эффективного и своевременного программного обеспечения по безопасности от поставщика с хорошей репутацией.
- Основные действия конечного пользователя, направленные на сведение к минимуму открытости для заражения бот-программой при пользовании Интернетом.

Ожидается, что многие провайдеры интернет-услуг смогут достичь этой цели через предоставление такой информации непосредственно своим абонентам или предоставлением ссылок на существующие ресурсы открытого доступа, содержащие эту информацию.

2. Поддержка усилий конечных пользователей, направленных на устранение заражения бот-программой:

Наряду с информацией о предотвращении, провайдеры интернет-услуг должны дать доступ (например, через собственные публикации, публикации третьих лиц или веб-ссылки) к информации о том, как конечные пользователи могут принципиально устранить заражение бот-программой. В этой области, как ожидается, провайдеры интернет-услуг смогут достичь этой цели путем предоставления ссылок на существующие общедоступные ресурсы, содержащие такую

информацию, или путем создания новых ресурсов с такой информацией, как в индивидуальном порядке, так и соединенными силами.

При уведомлении своих конечных пользователей, провайдерам интернет-услуг надлежит включить в такие уведомления или предоставить иным образом информацию о том, куда может пользователь обратиться за дополнительными сведениями и помощью. Такая информация может включать ссылки на общедоступную онлайн-информацию, средства защиты информации или предложения обратиться за помощью к профессионалу в компьютерной области. Дополнительные темы и ссылки, которые провайдеры интернет-услуг могли бы приобщить:

- Риски для конечных пользователей и интернет-сообщества от употребления устройства, предположительно зараженного бот-программой,
- Способы идентификации и удаления распространенных разновидностей заражения бот-программой,
- Общедоступные инструменты и сервисы (бесплатные или платные), которые способствуют обнаружению и удалению заражения бот-программой, а также
- Руководство по нахождению дополнительных (бесплатных или платных) вспомогательных средств.

3. Руководящие указания:

При рассмотрении вышеуказанных требований, провайдер интернет-услуг должен принимать во внимание следующие руководящие указания:

- Непосредственно или через ссылки на услуги третьей стороны предлагать обучающую информацию и ресурсы.
- Оформлять обучающий контент доступным для понимания образом и сосредотачивать его на наиболее важных предметах, которые необходимо знать пользователям.
- Обеспечивать возможность следования инструкциям для аудитории пользователей, не имеющих технического образования.
- Использовать мультимедийные средства, например, изображения, видео, текст, субтитры и т. д., а также, где целесообразно, многоязычную поддержку, с целью

максимального понимания и доступности для клиентов.

- Содействие конечным пользователям в определении того, подверглись ли их устройства заражению бот-программой, путем предоставления информации или указания на ресурсы, где содержится описание аномального поведения устройств, зараженных бот-программой, а также доступность и способы использования программных инструментов и сервисов для обнаружения бот-программ.

7. Обнаружение бот-программ

а. Краткий обзор

По мере развития бот-программ должны совершенствоваться и инструменты и технические методы, применимые для их обнаружения. Проблема обнаружения состоит в том, что ботовый траффик приспособляется к тому, чтобы обходить отдельные технические решения, используемые в механизмах обнаружения, например, простое сопоставление с шаблоном. Обнаружение может осложнить то, что некоторые интернет-приложения, такие как распределенные централизованные сети доставки кэшированного контента, приложения для сетевых игр и иные сервисы такого рода могут вести себя сходно с вредоносными бот-программами и использовать те же технологии. Провайдеры интернет-услуг должны действовать с осторожностью при идентификации участников, которых эта проблема затронула, для оповещения и устранения проблемы.

б. Рекомендуемые действия:

Провайдеры могут распознать вредоносную активность и устройства конечных пользователей, скомпрометированных наличием бот-программ разнообразными способами:

1. Получение уведомлений от внешних организаций, особенно таких, которые созданы с целью содействовать установлению общей картины и распространения в реальном времени данных, связанных с бот-программами. Перечень ресурсов доступен в Приложении 2.

2. Внедрение мощностей внутри своих сетей, способствующих установлению возможного заражения бот-программой.

3. Направление клиентов к инструментам, веб-порталу или другим ресурсам, которые позволили бы им самостоятельно определить возможное заражение бот-программой.

8. Уведомление конечных пользователей о возможном заражении бот-программой

а. Краткий обзор:

Многие конечные пользователи не знают, что их устройства заражены и действуют как бот-программа. В результате эти пользователи и их данные подвержены риску, тогда как бот-программы могут оставаться в активированном состоянии неограниченное время. Провайдерам интернет-услуг следует действенно использовать способы, описанные в разделе 7, для того, чтобы ставить клиентов в известность об активированном заражении.

Уведомления следует составлять так, чтобы они помогали уменьшить воздействие бот-программ и вред, который они причиняют. Уведомления могут включать в себя информацию о том, что такое бот-программа, о средствах заражения, о том, что бот-программы могут действовать без видимых признаков и о том, что означает уведомление. Они также могут содержать в себе или определять иные ресурсы – инструменты, руководства и сервисы, облегчающие предотвращение заражения, проверку его наличия и снижение* его последствий. Также они могут предоставлять информацию о любой обнаруженной разновидности бот-программ.

Уведомление конечных пользователей может принимать разные формы. Его может осуществлять непосредственно провайдер интернет-услуг или третья сторона от лица провайдера. Провайдеры интернет-услуг могут непосредственно предупреждать конечных пользователей об опасности или предоставлять механизмы, позволяющие конечным пользователям делать запрос и получать сведения о состоянии зараженности своих устройств. Сходным образом провайдеры интернет-услуг могут заключать соглашения о допуске уведомлений конечным пользователям со стороны других участников экосистемы Интернета, с которыми конечный пользователь поддерживает отношения, например, со стороны провайдера интернет-приложений или сервиса.

Провайдер интернет-услуг должен продумывать механизмы, обеспечивающие для клиента возможность легко опознавать подлинность уведомления, а также препятствующие подделке таких уведомлений.

При наличии возможности, провайдер интернет-услуг может по желанию отслеживать получение уведомлений. Это может помочь провайдеру лучше изучить эффективность разных механизмов уведомления.

Каждому провайдеру интернет-услуг вменяется в обязанность проводить оценку разных способов уведомления для того, чтобы найти тот из них, который наиболее подходит конкретному провайдеру в отношении конкретной угрозы бот-программы. Возможно, выбранную методику уведомления потребуется интегрировать в наличный бизнес-процесс и сетевую инфраструктуру. Может быть востребованным исследование и анализ с целью разработки и эксплуатации подходящих систем и политик уведомления.

б. Рекомендуемые действия:

Обеспечить информированность клиента о предположительном заражении бот-программой или способствовать тому, чтобы клиенты могли самостоятельно определить возможное заражение своих устройств бот-программами. Многие методики уведомления описаны в ссылках в Приложении 2; тем не менее, можно использовать и другие методы.

9. Устранение бот-программ

а. Краткий обзор

Снижение и устранение воздействия бот-программ составляет конечную цель любой программы уведомления. Основную ответственность за это несет конечный пользователь. Самих по себе уведомлений может быть достаточно для технически подготовленных пользователей, но для большинства пользователей требуется содействие в удалении вредоносного ботового программного обеспечения с их зараженных устройств. Несмотря на это, устранение может быть сопряжено с трудностями и может потребовать привлечения других сложных функциональных действий, таких как изолирование источника заражения среди множества устройств, объединенных одним соединением с Интернетом; предварительное резервное копирование всех данных и системного программного обеспечения способом, дающим возможность конечным пользователям их восстановить (но наряду с этим не производя резервного копирования зараженных файлов или программ); и

удостоверения наличия у конечного пользователя резервных дисков или других носителей, с которых можно восстановить образ их жесткого диска, если это требуется при устранении.

Необходимо считаться с тем, что некоторые провайдеры интернет-услуг не располагают ресурсами, которые позволили бы обеспечить данный уровень обслуживания и не в состоянии поддерживать такую деятельность бесплатно или даже за плату. Во многих случаях конечным пользователям могут потребоваться ссылки на провайдеров или профессиональные службы компьютерной поддержки для того, чтобы полностью восстановить свои устройства. Уведомления от провайдера интернет-услуг могут по желанию предвосхищать данное обстоятельство и предполагать, что клиенты ищут поддержки третьей стороны для того, чтобы не разочаровывать конечных пользователей ограниченным уровнем обслуживания со стороны службы поддержки и не поддерживать линии, которые неспособны или недостаточно оснащены для оказания полноценной помощи в вопросах устранения заражения бот-программой.

б. Рекомендуемые действия:

1. Бот-программы задуманы таким образом, чтобы действовать скрытно и быть трудноудалимыми. Как описано выше, провайдеры интернет-услуг должны, в качестве частичной функции уведомления, предлагать руководство, которое может включать в себя ссылки на разного рода публично доступные онлайн и принадлежащие третьим сторонам ресурсы информации, программного обеспечения и инструментов. Оно также может включать в себя ссылки на профессиональное обслуживание. Такие ссылки должен предоставлять не обязательно сам провайдер интернет-услуг, но их могут предлагать третьи стороны.

2. Провайдер интернет-услуг может предоставлять конечному пользователю инструменты для устранения заражения, как во время, так и после процесса уведомления. Однако провайдер не должен ставить обязательным условием, чтобы конечный пользователь запускал инструменты устранения. Если провайдер предоставляет инструменты конечному пользователю, то тот должен иметь возможность прервать свое участие в процессе без запуска любого из предлагаемых инструментов или процедур.

3. В качестве частичной функции уведомления провайдер интернет-услуг может по желанию включать наставление (в зависимости от природы рассматриваемой бот-программы) о том, что настройки на собственном клиентском сетевом оборудовании, например, домашние шлюзы и маршрутизаторы, могут претерпеть изменение и должны быть восстановлены до безопасного состояния, в зависимости от природы заражения бот-программой.

в. Руководящие указания:

1. Инструменты и сервисы для удаления бот-программ должны соблюдать конфиденциальность пользователя.

2. Возможные методы устранения заражения описаны в документах CSRIC II WG 8 best practices и в IETF RFC по устранению бот-программ, ссылки на которые даны в Приложении 2.

10. Сотрудничество между провайдерами интернет-услуг

а. Краткий обзор

Снижение воздействия бот-программ и управление процессами, связанными с ними, относятся к деятельности, в которой провайдеры интернет-услуг, поисковые провайдеры, конечные пользователи, IT-подразделения, хостинговые компании, провайдеры блог-платформ, поставщики услуг по безопасности, исследователи, правительство, компании финансовых услуг, провайдеры облачных сервисов и другие участники играют свою роль. При многостороннем вкладе и сотрудничестве результаты превзойдут те, что могут быть получены при изолированных действиях. Участие провайдеров интернет-услуг, наряду с дополняющими и содействующими подходами других сегментов экосистемы Интернета, как ожидается, может стимулировать существенное уменьшение угрозы, исходящей от ботнетов.

б. Рекомендуемые действия:

Участие в Кодексе требует сотрудничества внутри организации провайдера интернет-услуг, в рамках отрасли или более широкого сообщества посредством совместной деятельности, примеры которой таковы:

1. Обмен информацией о методах обнаружения, уведомления или смягчения угрозы бот-программ, которые стоят в планах на внедрение или уже внедрены в сетях провайдеров интернет-услуг, и, где практически доступно, оценка их эффективности.

2. Обмен информацией превентивного характера или данные об уже запущенных атаках, которые могли бы послужить для предотвращения, защиты или устранения последствий.

3. Определение ключевых данных или технических ресурсов, требуемых от систем или лиц вне сети провайдера интернет-услуг.

4. Участие в определении, разработке или функционировании интегрированных защитных стратегий или систем, которые простираются за пределы сети провайдера интернет-услуг.

5. Иные совместные действия, связанные с передачей информации сторонам вне сети провайдера интернет-услуг или передачей данных вовне сети провайдера интернет-услуг.

Весь обмен информацией между провайдерами и другими заинтересованными сторонами должен осуществляться в соответствии с применимым законодательством включая, но не ограничиваясь, антимонопольными законами и нормами о защите конфиденциальности.

11. Дальнейшая разработка данного Кодекса

Вследствие природной динамики угрозы, связанной с применением бот-программ а также по мере накопления опыта и оценивания провайдеров интернет-услуг, данный Кодекс будет со временем развиваться.

12. Дополнительная информация и источники

Приложение 1 – глоссарий

Приложение 2 - ссылки

Приложение 1 – Глоссарий:

1. Бот-программа

Нижеследующее определение в значительной степени перенесено из «Рекомендаций для устранения бот-программ в сетях провайдера интернет-услуг» (ссылка присутствует в Приложении 2):

Термин «вредоносная (или потенциально вредоносная) программа-робот (далее «бот-программа»)» относится к программе, установленной в системе с целью принудить эту систему автоматически (или полуавтоматически) исполнять определенное задание, или набор заданий, обычно по команде и под контролем администратора удаленного доступа (часто называемого «бот-мастером» или «бот-пастырем»).

Компьютерные системы и прочие устройства конечных пользователей, которые подверглись воздействию бот-программ также известны как «зомби».

Вредоносные бот-программы обычно установливаются исподволь, без согласия пользователя или полного понимания со стороны пользователя относительно того, что будет данная бот-программа делать после установки.

Бот-программы часто используют для рассылки нежелательной электронной почты («спама»), для шпионажа или атаки на другие системы, для прослушивания сетевого траффика или для приема нелегального контента, такого как пиратское программное обеспечение, материалы, связанные с эксплуатацией детей и т. д.

Многие правовые институты рассматривают недобровольное заражение хостов конечных пользователей как образец противозаконного компьютерного вторжения.

2. Ботнет

«Ботнеты» представляют собой зараженные ботовым вредоносным программным обеспечением сетевые образования компьютерных устройств конечных пользователей, подключенных к Интернету, которые контролируются по удаленному доступу третьими сторонами в пагубных целях.

Ботнетом управляет определенный «бот-пастырь» или «бот-мастер». Ботнет может состоять как из небольшого числа так и из миллионов зараженных бот-программами хостов,.

3. Клиент (или «Непосредственный клиент»)

Сторона, находящаяся в контакте с провайдером интернет-услуг для обслуживания. Следует отличать «клиента» от «авторизованного пользователя»: к примеру, кофейный магазин может приобрести интернет-услуги у провайдера интернет-услуг. Тогда кофейный магазин станет его клиентом. Кофейный магазин, в свою очередь, может решить предложить свободное пользование своим соединением (если это дозволяется Политикой использования доступа у данного провайдера) тем, кто в нем покупает кофе. В таком случае покупатели кофе будут авторизованными пользователями соединения, приобретенного кофейным магазином, но не непосредственными клиентами провайдера.

4. Обнаружение

Обнаружение представляет собой процесс, посредством которого провайдер услуг или конечный пользователь узнают о том, что отдельная система или устройство подверглись заражению вредоносным программным обеспечением. Провайдер услуг может обнаружить, что система заражена, многими различными способами, включая, в конечном счете, жалобы на спам от третьих сторон, сетевое сканирование или атаки, исходящие от этой системы. Конечные пользователи могут обнаружить заражение системы посредством программных средств или иными средствами.

5. Экосистема

Данный термин часто используется для описания взаимоотношений между разными участниками Интернета – производителями аппаратного обеспечения, разработчиками программного обеспечения, провайдерами интернет-услуг и провайдерами различного интернет-контента, приложений и услуг, которые обеспечивают работу Интернета и полезны для конечных пользователей.

Экосистема Интернета включает в себя поставщиков операционных систем, организации, работающих непосредственно с конечными пользователями, провайдеров интернет-контента, приложений и сервисов, провайдеров интернет-услуг, поисковых провайдеров, конечных пользователей, IT-подразделения, хостинговые компании, провайдеров блог-платформ, поставщиков услуг по безопасности, исследователей, правительство, компании финансовых услуг, провайдеров облачных сервисов и других участников.

Так называемая «теневая экономика» также часто определяется как «экосистема», с множеством участников, исполняющих разные специализированные роли. К примеру, некоторые участники могут специализироваться в написании вредоносного программного обеспечения, в то время как другие могут «пожинать» адреса электронной почты с веб-страниц и списков адресатов, иные – специализироваться на распределении вредных программ по полученным адресам почты. Экосистема вредоносного программного обеспечения также обычно включает в себя представителей целевой аудитории злонамеренных акций и правоохранительные службы, противостоящие киберпреступности.

6. Конечный пользователь

В контексте компьютерной техники и сетевой деятельности, конечный пользователь – лицо, которое авторизованно использует продукт или услугу в конечном счете.

Конечный пользователь часто может не быть тем же, кто приобрел продукт или услугу. К примеру, владелец кофейного магазина может приобрести интернет-подключение для себя и своих клиентов; при таком сценарии, клиенты кофейного магазина, а не его владелец, представляют действительных «конечных пользователей», при том даже, что они не заключали непосредственно контракт с провайдером интернет-услуг на соединение, которое используют.

Лицо, такое как хакер или взломщик, которое использует продукт или услугу без авторизации в качестве приобретателя, нормативно рассматривается как кибервзломщик, а не «конечный пользователь» в собственном смысле слова.

7. Провайдер интернет-услуг

Провайдер интернет-услуг – компания, которая предоставляет розничный доступ к интернету для членов общественных, коммерческих и иных организаций. Эти соединения могут быть осуществлены через кабель, цифровую абонентскую линию (DSL), спутник, беспроводные коммуникации, телефонную линию или иные технологии. Провайдеров интернет-услуг иногда называют «провайдерами доступа».

Предприятие, предоставляющее доступ в Интернет исключительно для своих сотрудников, обычно не относится к провайдерам интернет-услуг. Также и сетевой оператор, который предоставляет лишь оптовый доступ к Интернету для других провайдеров интернет-услуг, обычно чаще рассматривается как провайдер сетевых услуг, но не провайдер интернет-услуг.

8. Вредоносное программное обеспечение (англ. сокращение malware)

Вредоносные бот-программы составляют одну из разновидностей вредоносного программного обеспечения. Другие виды включают в себя категории программного обеспечения, известные как вирусы, трояны, черви, руткиты, хакерские программы, перехватчики ввода с клавиатуры, набиратели телефонных номеров, шпионские и рекламные программы и т. д. Факторы, отличающие эти разные типы вредных программ, имеют меньшее значение, нежели понимание того, почему вредоносное программное обеспечение можно рассматривать как «злоумышленное».

Вредоносные программы часто нарушают нижеследующие основные принципы, один или больше:

(а) Согласие: Вредоносные программы могут быть установлены даже в том случае, если пользователь не делает осознанного запроса на это.

(б) Честность: Вредоносные программы могут обозначать один род деятельности, при этом производя совершенно другие действия.

(в) Уважение к конфиденциальности: Вредоносные программы могут нарушать конфиденциальность пользователя, в частности, считывая пользовательские пароли или информацию с кредитных карт.

(г) Ненавязчивость: Вредоносные программы могут досаждать пользователям, постоянно открывая всплывающие окна с рекламой, меняя домашнюю страницу браузера, замедляя работу системы или делая ее нестабильной и предрасположенной к взлому, или вмешиваясь в работу ранее установленных программ безопасности.

(д) Безвредность: Вредоносные программы могут наносить пользователям вред (как программное обеспечение, разрушающее систему, рассылающее спам по электронной почте или деактивирующее программы безопасности).

(e) Приоритет пользовательского управления: Если пользователь пытается удалить программу, она повторно устанавливается в системе или иным образом игнорирует выбор пользователя.

Все это прибавляется к тому, что это «программное обеспечение, которое пользователи просто не желают иметь».

Пользователи могут по неведению установить вредоносное программное обеспечение посредством открытия подозрительного приложения, полученного по электронной почте, или посещения веб-страницы, содержащей вредоносный контент. Системы также могут быть непосредственно заражены субъектом, производящим атаку по удаленному доступу, в результате нацеливания на разведанную уязвимость, которая может подвергнуться эксплуатации с удаленного доступа, или самим пользователем, установившим зараженный CD, DVD или USB флэш-накопитель.

9. Снижение последствий

Снижение последствий – процесс управления или контроля над последствиями, связанными с деятельностью бот-программы. Например, если система заражена спам-ботом и извергает нежелательные рекламные электронные письма, то снижение последствий может заключаться в фильтрации спама, исходящего с этого устройства.

Следует заметить, что снижение последствий обычно не затрагивает исправление основной причины (такое действие уже считается «устранением»); снижение последствий лишь делает управляемой ситуацию с симптомами, связанными с этой причиной.

10. Уведомление

Уведомление – действие, посредством которого провайдеры интернет-услуг сообщают своим конечным пользователям о возможном заражении устройства конечного пользователя бот-программой или о том, как абонент может предотвратить или определить такое заражение. Уведомление может также направить конечных пользователей к инструментам, которые позволят им самостоятельно обнаруживать зараженность бот-программой. Уведомления могут посылаться в разных формах, включая прямое сообщение конечному пользователю от провайдера интернет-услуг, или косвенное информирование через доступные инструменты самостоятельного тестирования, или через третью сторону. Уведомления могут производиться по многим возможным каналам связи, включая (но не ограничиваясь) электронную почту, обычную почту, телефонный звонок, внутрибраузерные уведомления, инструменты самостоятельного тестирования, расположенные в вебе, или SMS-сообщения.

11. Предотвращение

Предотвращение представляет собой действие, направленное на укрепление системы или сервиса с целью уменьшить его уязвимость к компрометации и эксплуатации. К примеру, на многих системах предотвращение может состоять:

- постановка заплат на операционной системе и всех приложениях, на которых доступна доработка программ безопасности

- установление или допуск межсетевого экранирования

- использование антивирусного программного обеспечения

- обеспечение регулярного резервного копирования данных системы

- использование надежных паролей

- отключение всех ненужных сетевых услуг

- приглашение пользователей к безопасному использованию интернет-услуг (напр., электронной почты, веб-браузеров и т. д.)

12. Устранение

Устранение – действие, которое необходимо совершить конечному пользователю для очистки пораженного бот-программой компьютера так, чтобы он перестал быть зараженным. В легких случаях это может потребовать установки и использования антивирусного продукта. В более сложных случаях устранение может потребовать более существенного вмешательства, вплоть до того, чтобы «убить жесткий диск и вымостить заново» систему – форматировать ее и установить заново с нуля, или, по крайней мере, с последней достоверно чистой резервной копии. После того как систему очищают или переустанавливают, ее следует укрепить с целью защиты от повторного заражения.

13. Спам

Нежелательное и невостребованное электронное письмо, часто рекламное по своей природе, обычно посылаемое обширному числу получателей в идентичной по существу форме. Спам часто рассылают «партнеры», которым лицо, запускающее партнерскую программу, выплачивает вознаграждение каждый раз, когда получатели приобретают продукт, рекламируемый в спаме.

Приложение 2 – Ссылки

1. Рекомендации о том, как привести последствия заражения компьютеров вредоносными бот-программами: «Рекомендации к устранению бот-программ в сетях провайдеров интернет-услуг»

http://tools.ietf.org/rfc/rfc6561.txt

2. Рабочая группа № 8 CSRIC II – *Лучшие практические способы обеспечения защиты сетей провайдеров интернет-услуг*

http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf

3. icode – Кодекс практических действий в отношении кибербезопасности для интернет-индустрии (Австралия)

http://iia.net.au/images/resources/pdf/icode-v1.pdf

4. Центр очистки киберпространства (Япония) – Проект противодействия ботнетам

https://www.ccc.go.jp/en_index.html

5. Консультационный центр по противодействию ботнетам – Проект противодействия ботнетам

https://www.botfrei.de/en/

6. Группа реагирования на инциденты компьютерной безопасности (CERT, Япония)

http://www.jpcert.or.jp/english/

7. US CERT – Распознавание скрытых угроз: руткиты и ботнеты

http://www.us-cert.gov/cas/tips/ST06-001.html

8. Альянс по решениям в области телекоммуникаций (ATIS)

http://www.atis.org/

9. Министерство национальной безопасности

http://www.dhs.gov/files/programs/gc_1158611596104.shtm

10. Министерство национальной безопасности - Группа реагирования на инциденты компьютерной безопасности США (US-CERT)

http://www.us-cert.gov/

11. Инструментарий для снижения последствий ботнетов – Международный телекоммуникационный союз

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

12. Национальный институт стандартов и технологий (NIST) Министерства торговли США

http://www.nist.gov/index.html

13. Министерство торговли/ Министерство национальной безопасности – Служба безопасности информационных запросов – Модели для внедрения добровольных корпоративных уведомлений потребителей относительно незаконного использования компьютерного оборудования в ботнетах и смежном программном обеспечении

http://www.gpo.gov/fdsys/pkg/FR-2011-09-21/pdf/2011-24180.pdf

14. Комментарии, полученные в ответ на: Министерство торговли/ Министерство национальной безопасности – Служба безопасности информационных запросов – Модели для внедрения добровольных корпоративных уведомлений потребителей относительно незаконного использования компьютерного оборудования в ботнетах и смежном программном обеспечении

http://www.nist.gov/itl/botnetcomments.cfm

15. Рабочая группа по противодействию злоупотреблениям при обмене сообщениями (MAAVG.org) – Кодекс поведения

http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf

16. Собрание лучших практических решений для провайдеров интернет-услуг и сетевых операторов M3AAVG

http://www.maawg.org/published-documents

17. Национальная база данных уязвимостей - Национальный институт стандартов и технологий

http://nvd.nist.gov/

18. Internet Storm Center

http://isc.sans.edu/index.html

19. Shadowserver Foundation

http://shadowserver.org

20. Spamhaus Policy Block List

http://www.spamhaus.org/pbl/

21. Composite Blocking List

http://cbl.abuseat.org

22. OnGuard Online

http://www.onguardonline.gov/default.aspx

23. IETF BCP38 Network Ingress Filtering

http://tools.ietf.org/html/bcp38