This translation is a joint initiative of MAAWG (www.maawg.org) and ITU (www.itu.int/ITU-D/cyb/cybersecurity).

Передовой опыт MAAWG в отношении использования "огороженного сада"

Критерии для выхода и входа, исправления и просвещения абонента

Введение

По мере роста злоупотреблений в сети исходящего абонента от поставщиков услуг интернета (ПУИ) требуется принятие более проактивных мер с целью защиты их сетей и исходящего из них трафика. "Боты" и бот-сети ("боттеры") стали все более распространенным механизмом для спаммеров и хакеров, с помощью которого они злоупотребляют сетью через распространение спама, вирусов и других вредоносных программных средств. Эти средства скрытно внедряются в персональные компьютеры абонентов без их ведома, и в результате абоненты, являющиеся конечными пользователями, в подавляющем большинстве становятся целью как невольные сообщники в этих вредоносных сетях.

Пытаясь укрепить меры, принимаемые MAAWG с целью оградить процесс передачи электронных сообщений от неправильного использования и злоупотреблений, Подкомитет MAAWG, занимающийся проблемами бот-сетей и "зомби", рекомендует воспользоваться передовым опытом в области внедрения "огороженного сада". Этот термин означает создание среды, контролирующей информацию и услуги, которыми разрешено пользоваться абоненту, а также выдачу разрешений на доступ к сети. Главная цель распространения этого передового опыта заключается в том, чтобы помочь конечным пользователям узнать о нежелательных программах или вредоносных программных средствах, внедренных в их персональные компьютеры, избавиться от них и оградить сеть от использования злоумышленниками. Если не указано иное, задача выполнения всех рекомендаций возлагается на ПУИ.

Использование и значение ключевых слов, таких как ДОЛЖЕН, СЛЕДУЕТ и МОЖЕТ, которые употребляются во всем документе, подлежат толкованию, указанному в RFC2119.

I. Критерии для выхода из "огороженного сада" и входа в него должны быть краткими

В попытке просветить пользователей в вопросах, связанных с рисками и персональными компьютерами, зараженными вредоносными программными средствами, ПУИ МОГУТ внедрить "огороженный сад" для новых отчетов или любого отчета пользователя, которые, как им представляется, являются рискованными или создающими подозрительный трафик. Критерии входа в "огороженный сад" и выхода из него должны быть четкими и точными, с тем чтобы их мог понять конечный пользователь.

Резюме рекомендаций:

a) **ДОЛЖЕН представить ясное уведомление о подозреваемой проблеме, например использование сети за пределами правил допустимого пользования (ПДП). ДОЛЖЕН также разъяснить уведомление и описать рекомендуемый процесс исправления или очистки компьютера от вредоносных средств.**

b) **МОЖЕТ перенаправить HTTP [80] на надлежащий карантинный веб-адрес или веб-сайт, соответственно.**

c) **МОЖЕТ перенаправить командно-контрольный трафик бот-сети в сеть-ловушку для анализа.**

d) **СЛЕДУЕТ организовать все внешние SMTP [25] агенту передачи сообщений (MTA) карантинной зоны или системы-ловушки.**

e) **СЛЕДУЕТ разрешить мгновенный уход на основе доверия. Доверие может быть выражено посредством действия, которое показывает чистый персональный компьютер или запрос об использовании сети "как есть" для конфигурируемого периода времени.**

f) **МОЖЕТ предоставить выход, если загружено и установлено подтвержденное ПУИ очищение или программа безопасности.**

g) **ПУИ МОЖЕТ использовать внутренние показатели репутации абонента (установленные с помощью методов обнаружения, таких как фильтры контента, глубинная инспекция пакета и особенности использования) для запуска событий входа в "огороженный сад" и выхода из него.**

h) **ПУИ МОЖЕТ использовать технологии для автоматической идентификации средств обеспечения безопасности абонента, рекламируемых установленной и проверенной программой клиента абонента.**

II. Опыт исправления должен быть удобным для конечного пользователя

Поскольку ПУИ продолжают принимать меры по защите своих сетей и абонентов от злоумышленного использования, важно, чтобы ПУИ делали это таким образом, который не создает необоснованных трудностей для конечного пользователя. В целях окупаемости инвестиций ПУИ МОЖЕТ также сделать средства исправления доступными для конечного пользователя за какую-то плату. Эти средства ДОЛЖНЫ предоставляться способами, которые соответствуют типичной среде поддержки ПУИ. Кроме того, "огороженный сад" ДОЛЖЕН обеспечивать доступ на веб-сайты, с тем чтобы конечный пользователь мог загружать важнейшие применимые обновления и корректировки программы, либо через прямой доступ, либо через косвенные механизмы соединения с модулем-посредником. (Это обеспечивает возможность того, чтобы поставщик или ASP, с которым заключен договор, предлагали исправление через единый портал, как это делает компания Microsoft в отношении своих обновлений Windows и множественными новыми загрузками на жесткий диск, которые она инициирует от вашего имени.)

Резюме рекомендаций:

a) **ДОЛЖЕН уметь предоставлять бесплатные и/или платные варианты исправления (или каналы связи с существующими онлайновыми средствами).**

b) **ДОЛЖЕН предоставлять распознаваемую информацию, которая узаконивает опыт как официальный процесс ПУИ в отношении уведомления и исправления. В качестве примера такой информации можно привести такие данные, как номер отчета или ответ на секретный вопрос.**

c) **ДОЛЖЕН предоставлять подробную информацию о том, как обратиться за помощью в отдел обслуживания клиентов.**

d) **не СЛЕДУЕТ требовать перезагрузки персонального компьютера конечного пользователя, с тем чтобы закрепился опыт исправления.**

e) **ДОЛЖЕН предоставить каналы связи URL и доменам, которые помогают разрешить нежелательную ситуацию с корректировками операционной системы и обновлениями программ безопасности (в надлежащих случаях).**

f) **СЛЕДУЕТ обеспечить "щелкнуть для взаимодействия с отделом обслуживания клиентов" или клиентское обслуживание третьим лицом от имени ПУИ.**

g) **СЛЕДУЕТ обеспечить поддержку ПУИ или контактные данные в случае злоупотребления (например, номер телефона).**

h) **СЛЕДУЕТ дать указание клиентам, направляющим вредный трафик SMTP [25], относительно реконфигурации почтовых агентов пользователей (MUA), с тем чтобы направлять выходной трафик через порт 587.**

i) **СЛЕДУЕТ представить уникальные примеры опыта исправления, в зависимости от нежелательного состояния и прежних действий пользователя, например, пользователю СЛЕДУЕТ ознакомиться с опытом, который показывает средство устранения точной проблемы или вида вредоносной программы, в отношении которой возникли подозрения.**

j) **СЛЕДУЕТ предоставить клиента безопасности, который оказывает минимальное воздействие, быстро загружается, легко устанавливается, не вступая в конфликт с другими приложениями, такими как уже сконфигурированный клиент безопасности, не требует перезагрузки, а также полного сканирования компьютера с целью обнаружения и устранения вредоносной программы.**

k) **ДОЛЖЕН допускать исключительные ситуации перенаправления, с тем чтобы пользователю было разрешено воспользоваться онлайновыми услугами экстренной помощи.**

III. Просвещение конечного пользователя должно стать одной из главных задач

Поскольку конечный пользователь обычно является слабым звеном в цепочке обеспечения безопасности, ПУИ СЛЕДУЕТ принять разумные меры с помощью документации, имеющейся на его веб-сайте, с тем чтобы конечный пользователь мог проактивно заняться самообразованием в области ослабления риска заражения вредоносными программами. Документацию в форме FAQ (часто задаваемые вопросы), вспомогательных видеоматериалов, учебных пособий и доступной для поиска базы знаний СЛЕДУЕТ сделать доступной для конечного пользователя. В случае предоставления этих материалов они ДОЛЖНЫ быть доведены до него с помощью метода, который согласуется с видом и функциями интерфейса отдела обслуживания клиентов ПУИ. Кроме того, СЛЕДУЕТ обеспечить достаточное разнообразие имеющейся документации, с тем чтобы они охватывала приложения, отражающие несколько различных видов технологий интернета и несколько различных видов компьютерных операционных систем (например, Windows, MacOS, Linux).

Резюме рекомендаций:

a) **ДОЛЖЕН представить узнаваемую информацию, которая узаконивает опыт как официальный процесс ПУИ в отношении уведомления и исправления. В качестве примера такой информации можно привести такие данные, как номер отчета или ответ на секретный вопрос.**

b) **СЛЕДУЕТ обеспечить наглядное просвещение пользователя с помощью FAQ и учебных пособий.**

c) **СЛЕДУЕТ предоставить средства центра альтернативного обучения, такие как простое видеоприветствие и центров поиска знаний.**

d) **СЛЕДУЕТ предоставить учебную информацию в отношении многих видов приложений, включая электронную почту (PO5/SMTP) и просмотр (HTTP).**