СОСТОЯНИЕ И ТРЕНДЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

Смирнов Виталий Михайлович,
старший преподаватель
кафедры информатики и математики
Московского университета МВД имени В.Я. Кикотя,
к.т.н..
Цыганкова Яна Валерьевна,
Преподаватель
кафедры информатики и математики
Московского университета МВД имени В.Я. Кикотя,
к.ю.н..
Нестеров Игорь Александрович,
Доцент
кафедры информатики и математики
Московского университета МВД имени В.Я. Кикотя,
к.т.н..

АННОТАЦИЯ

В статье говорится об использовании сетевого обеспечения и методах борьбы с вредоносного сетевой активностью.

ABSTRACT

The article deals with the use of network software and methods of combating malicious network activity.

Ключевые слова: безопасность, вредоносные программы, борьба, программное обеспечение, прокси-сервер, межсетевой экран.

Keywords: security, malware, fighting, software, proxy server, firewall.

В ходе научно-технического прогресса информационные технологии проникают во все сферы нашей жизни. Вместе с очевидными преимуществами это порождает и новые угрозы, для борьбы с которыми разрабатываются специализированные методы защиты. Динамичность данной области так велика, что применение реактивных подходов становится всё менее эффективно. Это порождает потребность в развитии проактивных технологий. В антивирусных компаниях постоянно ведутся исследования для совершенствования методов детектирования и реагирования. Сейчас наметилась тенденция к анализу паттернов поведения объекта, а не его структуры. Одним из видов активности свойственной вредоносному программному обеспечению (ПО) является сетевой обмен данными.

1.Использование сетевого соединения вредоносным программным обеспечением.

Различные типы программных зловредов имеют потребность в сетевом обмене данными по нескольким причинам. Наиболее известная — собственно проникновение и заражение системы. Известно множество сценариев этого этапа, от прямой загрузки пользователем исполняемого файла с вредоносным кодом и последующим его запуском до использования уязвимости какого-либо ПО работающего с сетью. Файловые черви могут скопировать себя на сетевой диск, с которого могут быть запущены пользователем другого устройства. Или классический пример трояна — рассылка его по электронной почте. Однако более серьёзную угрозу представляют сетевые черви называемые "бесфайловыми" или "пакетными", которые распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Распространённая проблема для атакующего заключается в невозможности повторно эксплуатировать одну и ту же уязвимость скомпрометированной системы, поскольку так работает один из механизмов предотвращения повторного заражения, которое может привести к падению системы. Поэтому система обновления является значительным преимуществом передовых разработок вредоносного ПО, позволяя удалённо менять его функциональность.

Ещё один важный, но не обязательный, компонент трояна — удалённый контроль с помощью модуля связи, позволяющего владельцу трояна, управлять его поведением, отправляя специальные сообщения.

И наконец собственно «полезная нагрузка» такой программы. Так как одна из основных целей разработки вредоносного ПО — это неправомерный доступ к конфиденциальной информации, троян может отсылать злоумышленнику собранную на скомпрометированной системе информацию через сеть или позволять использовать заражённый компьютер в качестве прокси-сервера.

Другая возможная задача трояна — создание сети заражённых систем с централизованным управлением — *ботнета* или зомби-сети. Для этого компьютеры пользователей заражают специальной программой – *ботом.* В дальнейшем «владелец» такой сети может использовать её на своё усмотрение, например, для майнинга криптовалюты за счёт чужой вычислительной мощности или с целью оказания специального воздействия на какой-либо сетевой ресурс.

Наиболее известным примером такого воздействия является организация распределённой атаки типа «отказ в обслуживании» — Distributed Denial of Service (DDoS). Вторым набирающим популярность вариантом является имитация массовой пользовательской активности на интернет портале с целью манипуляций общественным мнением.

2.Методы борьбы с вредоносной сетевой активностью.

Для борьбы с вредоносным ПО использующим возможности сетевого взаимодействия применяются прокси-сервера, межсетевые экраны (firewall) и системы обнаружения вторжений — Intrusion detection system (IDS).

Прокси – в общем случае просто посредник в сетевом взаимодействии. Он может использоваться для доступа к ресурсам недоступным напрямую. Это и применяется в основном в корпоративных локальных сетях, когда в целях безопасности все соединения с интернетом разрешены только через единую точку — прокси-сервер. На этом сервере обычно и установлена IDS и настроен firewall.

Межсетевой экран ограничивает возможности по сетевому взаимодействию между разделяемому им узлами. Его задача недопущение самого факта установки нежелательного соединения, посредством низкоуровневого контроля каналов связи и отказа как во входящем, так и в исходящем подключении к запрещённым точкам доступа.

IDS по среде функционирования подразделяют на сетевые — Network IDS, которые занимаются обработкой исходящего, входящего и локального трафика сети, и хостовые, которые являются программными агентами, контролирующими состояние системы, на которой установлены. По реакции на вторжение IDS подразделяют на пассивные, занимающиеся только уведомлением о нём и ведением логов, и активные системы предотвращения вторжений — Intrusion prevention system (IPS) — способные оказывать какое-либо активное противодействие угрозе, например, перенастраивать межсетевой экран, сбрасывать соединения, фильтровать потоки трафика. IPS обычно считаются расширением IDS, поскольку обязательно включают в себя такую подсистему. Примерами наиболее широко применяемых сейчас IPS являются Snort и Suricata. В основе работы IDS лежат два основных подхода — сигнатурное детектирование и детектирование аномалий.

Сигнатурный детектор проверяет соответствие потока данных известным шаблонам вредоносной активности. Из его принципа работы следует насколько взаимосвязанных недостатков:

не позволяет обнаруживать новые угрозы, паттерны которых ранее не были известны;

может быть обманут злоумышленником, специально модифицирующим характеристики атаки подобно полиморфным вирусам.

Детектор аномалий частично компенсирует недостатки сигнатурного анализатора, контролируя изменения динамических характеристик, таких как уровень трафика, сравнивая кратковременную статистику наблюдаемой величины с её статистикой за длительный период времени. Аномалией считает возникновение значительного их расхождения. Такой подход в свою очередь также имеет ряд сложностей:

- злоумышленник может плавно наращивать вредоносную активность, так чтобы кратковременная статистика никогда не превышала долговременную;
- естественные флуктуации или суточное изменение активности использования сервиса может приводить к ложным срабатываниям или пропуску угрозы;
- ограниченная чувствительность к предельно кратковременной активности.

Дополнительные ограничения накладываются на техники, применяемые в IDS, необходимостью работать в реальном времени с большими потоками данных, требуя при этом минимального участия человека.

Высокая динамичность характеристик сетевого трафика и постоянно растущий его объём требуют автоматизации процесса анализа данных с применением различных методов машинного обучения. Поскольку системе предстоит принимать какие-либо решения относительно непредусмотренных заранее ситуаций, особое место здесь занимает кластерные анализ, как классический пример «обучения без учителя». Кластерный анализ или кластеризация — это задача группирования множества объектов таким образом, чтобы внутри каждой группы находились объекты более похожие друг на друга, чем на объекты другой группы. Кластеризация позволяет классифицировать множество объектов, посредством сэмплирования — проанализировав лишь несколько объектов каждого кластера. Однако при таком подходе важное значение по-прежнему имеет экспертное мнение при первоначальной настройке системы (классификации), как при выборе алгоритма кластеризации, так и используемых им метрик и признаков сетевых сессий.

Библиографический список:

1- Гладских С. А. Разработка программного средства кластеризации трафика, М., МЭСИ, 2014.-126с.

2- Roberto Perdiscia, Wenke Lee, Nick Feamster. Behavioral Clustering of HTTP-Based Malware and Signature Generation Using Malicious Network Traces, Atlanta, College of Computing, Georgia Institute of Technology, 2008.-14

3- Peter Szor. The Art Of Computer Virus Research And Defense, Boston, Addison Wesley Publishing Company Incorporated, 2005.-713

4- Rick Lehtinen, Deborah Russell, G. T. Gantemi Sr. Computer Security Basics. O'Reilly, 2006.-312