РЕФЕРАТ

В связи с развитием с атак и угроз возникает проблема: их становится сложнее обнаруживать и сложнее выяснять является ли трафик легитимным или вредоносным. Существующие системы обнаружения вторжений требуют постоянного обновления набора правил, которые должны соответствовать актуальным угрозам. Но даже периодического обновления набора правил может быть недостаточно для того, чтобы система всегда оставалась в актуальном состоянии.

В настоящее время разработано достаточно различных защитных методик для обнаружения вредоносного трафика и защиты от DDoS-атак.

Elastic Cloud Security System ECS2 [1] предоставляет сложную защитную систему от вредоносного трафика. ECS2 имеет антибот-таблицы и антивирусные решения, встроенные в систему защиты. Также в системе установлены межсетевые экраны, работающие в режиме реального времени. Минусом использования подобного подхода является время обновления репутационных таблиц и сигнатур вирусов. Несвоевременное обновление таблиц может привести к пропуску вредоносного трафика, генерируемого с непомеченных IP-адресов. Поэтому мой подход не основан на сигнатурах, списков вредоносных IP-адресов и других методов, данные для которых необходимо постоянно обновлять.

В статье [2] описан защитный метод, использующий ресурсы для обнаружения вредоносного трафика виртуальных машин. Метод был протестирован на 108 сервисах, запущенных на различных виртуальных машинах. Приведенные в статье методы основаны на технологии интеллектуального анализа данных и запускаются как приложения на виртуальных машинах. Минусом данного решения является расположение процессов защиты на стороне клиента. Многие клиенты не хотят видеть на своих виртуальных машинах фоновые сторонние процессы. Это не соответствует политикам безопасности многих компаний.

В статье [3] рассматривается новый метод обнаружения аномалий в трафике, использующий анализ потоков, основанный на K-mean алгоритме. Обучение данных, содержащих неподписанные записи потоков, делится на кластеры легитимного и вредоносного трафиков. Соответствующие центроиды кластеров используются как паттерны для эффективного обнаружения аномалий в анализируемом потоке трафика. Авторы указывают, что применение алгоритма раздельно для разных сервисов (использующих разные протоколы и номера портов) увеличивает точность обнаружения.

Авторы [4] описывают алгоритм для обнаружения DDoS-атак, который использует SSL/TLS протокол. Алгоритм основан на фильтрации шума в данных и кластеризации для обнаружения вредоносного трафика. Модели были обучены на данных, полученных с реалистичной компьютерной среды. Авторы заключают, что предложенная модель позволяет обнаруживать все вредоносные потоки с очень малым количеством ложных срабатываний.

Использование методов детектирования DDoS-атак на основе машинного обучения является достаточно популярной задачей среди исследователей. Один из методов детектирования, предложенный в работе [5] Keisuke Kato, с использованием алгоритма машинного обучения support vector Keisuke Kato machine with the radial basis function machine with the radial basis function (Gaussian) kernel на dataset from UCLA. Однако в работе не рассматривается возможность динамического изменения трафика.

В работе Wafa Slaibi Alsharafat [6] представлен метод детектирования на основе генерации классификаторов с использованием генетического алгоритма с набором данных KDD’99.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. About SecuCloud. URL: https://secucloud.com/en/company/about-us (дата обращения: 03.12.2018).
2. Delimitrou C.; Kozyrakis C. Security Implications of Data Mining in Cloud Scheduling // IEEE Computer Architecture Letters. 2015. №PP. pp. 64-68.
3. Munz, G., Li, S., Carle, G.: Traffic Anomaly Detection Using K-Means Clustering // Proceedings of GI/ITG Workshop MMBnet. 2007. pp. 106-110.
4. Zolotukhin, M., Hamalainen, T., Kokkonen, T., et al.: Data Mining Approach for Detection of DDoS Attacks Utilizing SSL/TLS Protocol. Proceedings of 15th International Conference, NEW2AN 2015, pp. 274-285. St. Petersburg, Russia, (2015)
5. Kato K., Klyuev V. Large-scale network packet analysis for intelligent DDoS attack detection development // Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for. – IEEE, 2014. – С. 360-365.
6. AlSharafat M. S. et al. Adaptive steady state genetic algorithm for scheduling university exams // Networking and Information Technology (ICNIT), 2010 International Conference on. – IEEE, 2010. – С. 70-74.