УДК:004.49

ВЫЧИСЛЕНИЕ УРОВНЯ УГРОЗЫ ВРЕДОНОСНОЙ ПРОГРАММЫ НА ОСНОВЕ АНАЛИТИЧЕСКИХ ДАННЫХ СИСТЕМЫ tLab

Ахметов Мурат Куанышович
muratahmetov_1998@mail.ru
Студент 4-го курса специальности «5В070400 - Вычислительная техника и ПО»
ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
стажер ТОО «T&T Security»
Научный руководитель – Д.Ж. Сатыбалдина

Ежедневно институт AV-TEST [1] регистрирует более 350 000 новых вредоносных программ (вредоносных программ) и потенциально нежелательных приложений (PUA). Они проверяются и классифицируются в соответствии с их характеристиками и сохраняются. Затем программы визуализации преобразуют результаты в диаграммы, которые можно обновлять, и генерируют текущую статистику вредоносных программ (см. рисунок 1). В связи с этим специалисты по безопасности и разработчики антивирусов вынуждены постоянно совершенствовать инструменты и методы автоматического анализа вредоносных программ.

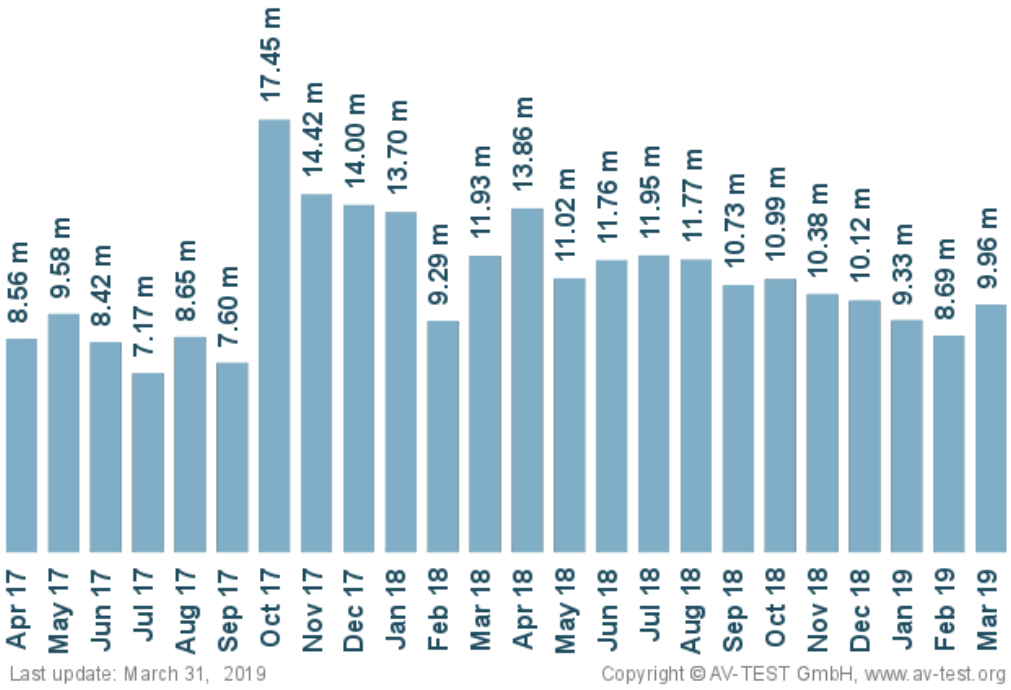

Рисунок 1. Общее количество нового вредоносного ПО за последние два года [1].

Методы анализа программ с целью обнаружения вредоносного функционала можно разделить на три группы: сигнатурные, эвристические и на основе спецификации [2]. Эти методы идентифицируют и обнаруживают вредоносные программы и принимают контрмеры для обеспечения безопасности компьютерных систем от возможной потери данных и ресурсов. Метод обнаружения на основе сигнатур используется большинством антивирусных программ. Антивирусная программа разбирает код зараженного файла и ищет шаблон, принадлежащий семейству вредоносных программ. Сигнатуры вредоносных программ хранятся в базе данных, а затем используется для сравнения в процессе сканирования. Данный метод является неэффективных для новых угроз и требует просмотра больших массивов данных. Эвристическое детектирование обнаруживает или различает нормальное и ненормальное поведение системы, так что в конечном итоге известные и неизвестные вредоносные атаки могут быть идентифицированы. Хотя эвристическое обнаружение является эффективным методом, но есть ограничения, связанные с необходимостью больших ресурсов и высоким уровнем ложных срабатываний. В методике обнаружения на основе спецификаций приложения отслеживаются в соответствии с их спецификацией и проверяется нормальное и ненормальное поведение. Каждая из вышеперечисленных технологий обнаружения вредоносных программ может быть статической, динамической или гибридной.

В работе [3] был представлен новый подход к кластеризации вредоносных программ в области их поведения. Для этого была разработана системам tLab, которая предлагает анализ и обнаружение современных сложных вредоносных программ, в том числе ориентированных на пользователя и целевых атак. Благодаря используемым технологиям tLab идентифицирует и описывает поведение вредоносных программ на различных уровнях семантики, что делает

его очень полезным для кластерного анализа [4]. Технически, система использует защищенные контейнеры, позволяющие пользователю выполнять зависимую среду выполнения при анализе вредоносных действий. Чтобы обеспечить эффективное обнаружение вредоносных программ, в tLab имеется технология для глубокого динамического контроля поведения всей системы, которая позволяет проводить структурный анализ и создавать так называемые деревья действий, определенные в области функциональных возможностей системы. Модифицированные иерархические цветные сети Петри используются для распознавания функциональных возможностей вредоносной программы, включая обфускацию и распределенность [3].

В настоящей работе представлены результаты проектирования и программной реализации на языке программирования Python модуля расчета уровня вредоносности, анализируемого ПО на основе аналитических данных с системы tLab. Для разработки программного модуля использованы возможности интегрированной среды разработки PyCharm Community Edition 2017.

Система tLab представляет собой корпоративный локальный сервис для удаленного и безопасного анализа подозрительных объектов, является примером казахстанской инновационной разработки песочницы, т.е. изолированной среды, имитирующей операционные среды конечных пользователей [5]. Система tLab производит автономный динамический анализ поведения программ и идентификацию вредоносных функциональностей в локальном облаке. Система позволяет автоматизировать процедуру анализа поведения любых программ и выявлять в них признаки вредоносных функций.

Динамическим анализом называется анализ поведения программы во время ее выполнения. Программа запускается в защищенной среде с определенным временем для мониторинга поведения. Процесс мониторинга занимает много времени и должен гарантировать, что исполняющее вредоносное ПО не сможет заразить платформу. Помимо этого, защищенная среда может отличается от реальной среды выполнения, и вредоносное ПО может вести себя по-разному в двух средах, вызывая неточный журнал поведения вредоносного ПО. Кроме того, некоторые действия вредоносного ПО активируются или запускаются при определенных условиях (системная дата и время или некоторый конкретный ввод данных пользователем) может не обнаруживаться защищенной виртуальной средой.

В качестве данных на выходе динамического анализа, могут включать доменные имена, IP-адреса, пути к файлам, ключи реестра, дополнительные файлы, расположенные в системе или сети. Помимо этого, можно также получить информацию о связи с внешним сервером, контролируемым злоумышленником, для командных и контрольных целей или в попытке загрузить дополнительные файлы вредоносных программ.

Процесс анализа потенциально вредоносного файла начинается с его отправки в систему tLab (смю рисунок 2).

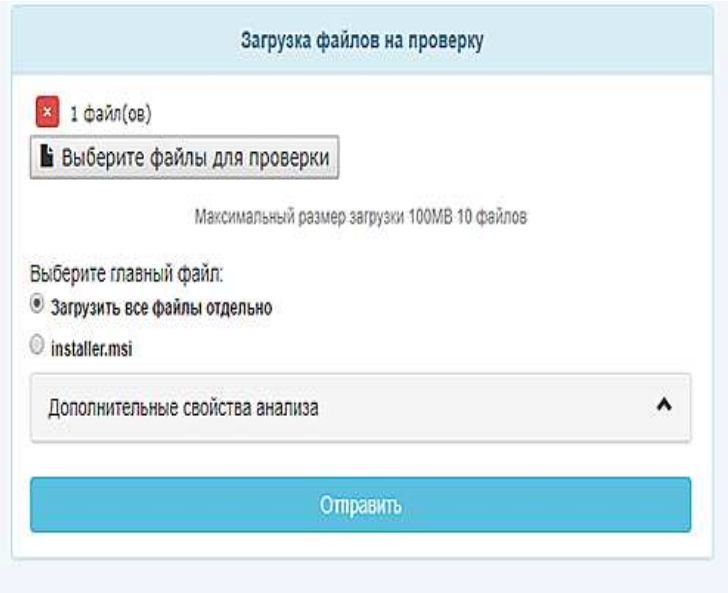

Рисунок 2. Процесс отправки файла на проверку в систему tLab

Каждый файл, проверяемый в системе, дает выходную информацию, необходимую для вычисления уровня вредоносности. Загрузив файл и подождав определенное количество времени, получим результаты проверки файла: какие события были обнаружены, как они взаимодействуют и какой вред несут.

Каждое событие разбирается по отдельности и представляет собой отдельную угрозу. Если же событие не представляет никакой угрозы для системы, то соответственно ее уровень равен 0. Может произойти и такое, что выделенного количества времени на анализ было недостаточно, поэтому данные могут быть различными. Из одного процесса могут вызываться другие (см.рисунок 3), а если этот процесс не исполнится за определённый промежуток времени, то и вытекающие из его события не произойдут.

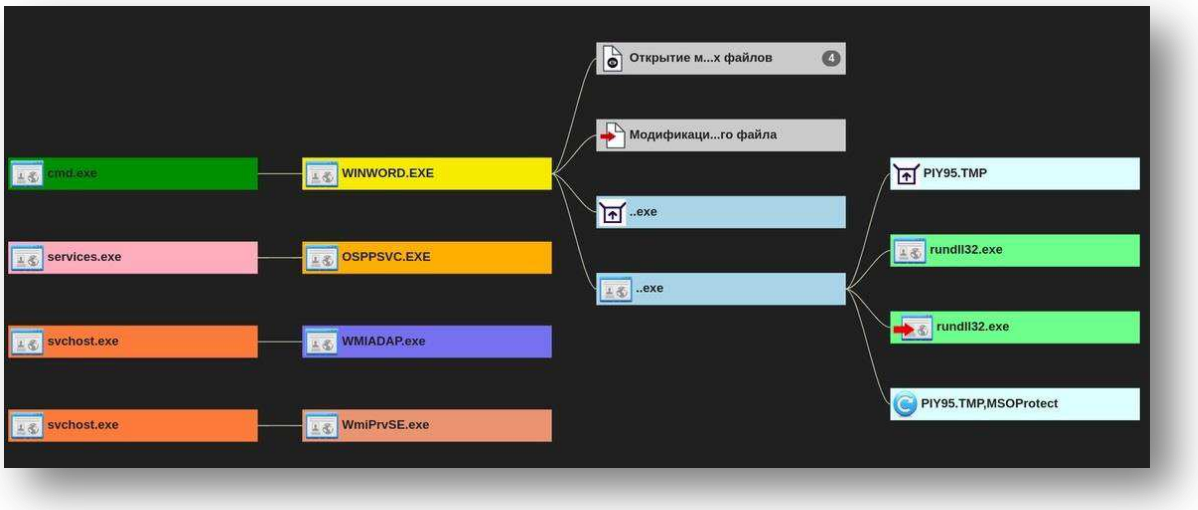

Рисунок 3. Данные системы tLab, представляющие цепочку взаимосвязанных событий

Исходя из полученных данных и подставив в формулу для вычисления уровня угрозы, получаем результат для каждого проверяемого файла (см. рисунок 4).

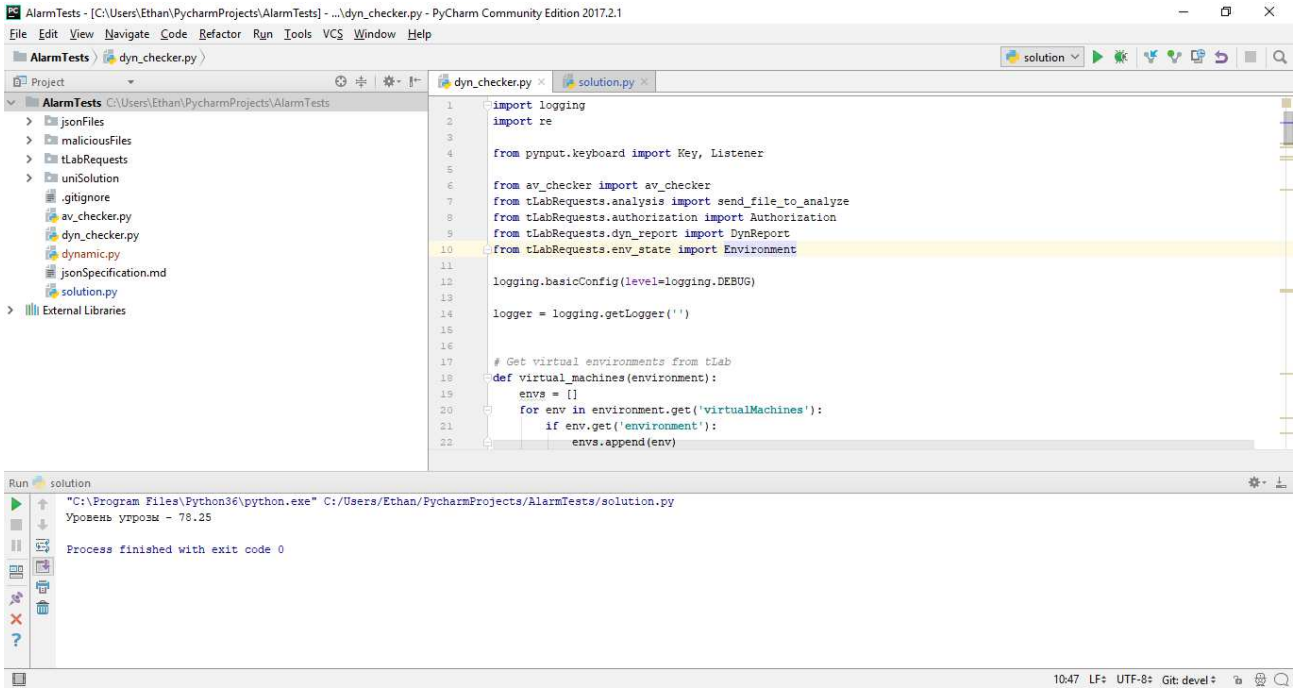

Рисунок 4. Полученный уровень угрозы для проверяемого файла.

Получив уровень опасности для файла, можно сделать вывод о том, насколько целесообразен его запуск и вообще наличие этого файла в системе пользователя, если же этот показатель превышает 40, то файл может нести потенциальную угрозу пользователю и не стоит открывать его.

Научно-исследовательская работа выполнена в рамках дипломного проектирования по теме «Разработка модуля для вычисления уровня угрозы вредоносного ПО на основе аналитических данных системы tLab». Данное направление исследований было инициировано компанией-работодателем – ТОО «**T&T security**» (генеральный директор, PhD, А. Тохтабаев).

Список использованных источников

1. https://www.av-test.org/en/statistics/malware/
2. Rabia Tahir, A Study on Malware and Malware Detection Techniques //I.J. Education and Management Engineering. – 2018.- № 2. – Pp. 20-30. DOI: 10.5815/ijeme.2018.02.03
3. Tokhtabayev A., Kopeikin A., Tashatov N., Satybaldina D. Malware Analysis and Detection via Activity Trees in User-Dependent Environment. In: Rak J., Bay J., Kotenko I., Popyack L., Skormin V., Szczypiorski K. (eds) Computer Network Security. MMM-ACNS 2017. Lecture Notes in Computer Science, Springer, Cham. - 2017.- vol. 10446. – pp. 211-222. DOI:10.1007/978-3-319-65127-9_17
4. Kopeikin A., Tokhtabayev A., Tashatov N., Satybaldina D. tLab: A System Enabling Malware Clustering Based on Suspicious Activity Trees. In: Rak J., Bay J., Kotenko I., Popyack L., Skormin V., Szczypiorski K. (eds) Computer Network Security. MMM-ACNS 2017. Lecture Notes in Computer Science, Springer, Cham. - 2017.- vol. 10446. – pp. 195-210. DOI:10.1007/978-3-319-65127-9_16
5. https://tntsecure.kz/ru/tlab.html