УДК 004.056.2 **10.52167/1609-1817-2024-135-6-170-177**

Е. Майлыбаев[1], А. Козьякова[2], В. Прошин[2], Е.Таштай[2]
[1]Международный транспортно-гуманитарный университет, Алматы, Казахстан
[2]Satbayev University, Алматы, Казахстан
E-mail: ersind@mail.ru

ИССЛЕДОВАНИЕ МЕТОДОВ ДИНАМИЧЕСКОГО ОБНАРУЖЕНИЯ И АНАЛИЗА ЗЛОНАМЕРЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В РЕАЛЬНОМ ВРЕМЕНИ

Аннотация. В данной научной статье рассматриваются методы динамического обнаружения и анализа злонамеренного программного обеспечения (ЗПО) в реальном времени. Проблема обнаружения и анализа ЗПО становится все более актуальной в современном информационном обществе, где угрозы кибербезопасности постоянно эволюционируют. В статье анализируются существующие подходы к динамическому обнаружению ЗПО и выявляются их преимущества и недостатки. Также предлагается новый метод, основанный на комбинации техник машинного обучения и анализа поведения программ, который способен эффективно выявлять и анализировать ЗПО в реальном времени.

Ключевые слова. Злонамеренное программное обеспечение, кибератаки, вредоносные программы, динамический анализ кода, мониторинг.

Введение.

В современных реалиях угрозы киберпреступности становятся все более серьезными и непредсказуемыми. Различные типы вредоносных программ представляют собой серьезные проблемы для конфиденциальности, безопасности и целостности информационных систем как в государственном, так и в частном секторах.

В данной статья проведем исследование методов динамического обнаружения и анализа злонамеренного программного обеспечения в реальном времени. Рассмотрим инструменты для обнаружения вредоносного ПО.

Материалы и методы.

В наше время угрозы киберпреступности становятся все более серьезными и непредсказуемыми. Разнообразные вредоносные программы представляют значительные риски для конфиденциальности, безопасности и стабильности информационных систем как в государственном, так и в частном секторах.

Первым этапом анализа вредоносных программ в кибербезопасности является получение образцов таких программ. Процедура получения образца осуществляется различными способами, включая:

- предоставление файла;
- загрузку вредоносного ПО из интернета по URL-адресу;
- извлечение из электронной почты;
- извлечение из хранилища мобильных устройств.

Дополнительная информация о происхождении, методе атаки и возможных целях атаки предоставляется для понимания контекста действий киберпреступников.

В процессе исследования применяются передовые методы статического, динамического и гибридного анализов для частичного раскрытия принципов работы вредоносной программы.

Статический анализ подразумевает изучение исходного кода или структуры двоичного файла с целью выявления уникальных особенностей, скрытых функций и использованных уязвимостей без необходимости запуска самой программы. Используя инструменты декомпиляции и дизассемблирования, раскрываются функциональные возможности вредоносных программ, выявляются манипуляции на уровне файловой системы и реестра.

Динамический анализ является еще одним ключевым методом расследования, используемым при реверс-инжиниринге. Он заключается в выполнении образца вредоносного ПО в контролируемой лабораторной среде с последующим наблюдением за его поведением. Исследователи отслеживают интерактивность образца с операционной системой и фиксируют возможные изменения системных регистров [1].

Гибридный подход к анализу — это дополнительное решение для изучения поведения вредоносных программ. Он объединяет функциональные возможности нескольких из вышеупомянутых методов анализа. Следует отметить, что комбинирование различных методов анализа вредоносного ПО позволяет получить более полную информацию о вирусах, что улучшает их обнаружение. После того как функции были созданы с использованием любого из упомянутых выше методов анализа вредоносных программ, следующим этапом является разработка и обучение сложной модели для обнаружения с использованием соответствующих функций и методов машинного или глубокого обучения. Методы машинного и глубокого обучения показали многообещающие результаты в обнаружении вредоносных программ.

Это помогает получить детальную информацию о функциях, целях атак и действиях, предпринимаемых вредоносным программным обеспечением.

Важной частью анализа вредоносных программ является изучение сетевого трафика. Специалисты по кибербезопасности проводят подробные исследования связей между вредоносными программами и серверами командного управления, выявляя IP-адреса, порты, протоколы и содержимое, передаваемое вредоносным программам.

Полученные знания позволяют определить примерное местоположение противников и другие характеристики, необходимые для выявления известных групп APT.

Хакеры постоянно создают новые подходы и методы, направленные на скрытие вредоносного программного обеспечения от антивирусных систем. Одним из самых сложных способов маскировки вредоносного ПО является запутывания кода. Этот процесс включает использование различных методов для усложнения дизассемблирования и декомпиляции. Путем изменения структуры кода, скрытия функций и манипулирования данными запутанного кода затрудняет определение и понимание работы вредоносного ПО. Также возможно скрытие структуры кода для усложнения его анализа. Примерами таких методов являются: размывание инструкций, создание ложных путей выполнения программы, а также добавление избыточных функций и процедур для осложнения интерпретации ключевых частей кода.

Результатом анализа образца вредоносного программного обеспечения является отчет с подробным описанием проведенных исследований, информацией о вредоносном ПО и рекомендациями. Этот документ содержит информацию о выявленных угрозах, используемых методиках атаки, информацию о системных уязвимостях и рекомендации для представителей военной и государственной сфер управления. Данный отчет представляет собой ценный ресурс информации, необходимый для повышения уровня безопасности системы и разработки эффективной стратегии защиты от киберпреступников.

Особое внимание нужно уделить алгоритмам, используемым зловредным программным обеспечением, таким как DGA (Domain Generation Algorithm), для создания

доменных имен. Схему механизма генерации доменов-DGA можно увидеть на рисунке 1. В последние годы доменные имена стали уязвимыми точками для ботнетов; блокировка этих доменов (например, операциями CERT Polska) приводила к прекращению их активности. Некоторые вредоносные программы автоматически генерируют большое количество доменных имен за короткое время для поиска зарегистрированных операторами и получения от них настроек. Когда один из таких доменов закрывается, процесс повторяется. Злоумышленники могут заранее приобретать домены, зная алгоритм их генерации, чтобы использовать их в будущем [2].

Например, домены, создаваемые с помощью DGA, могут меняться в зависимости от текущего времени (как это было с Conficker):

fupwo.cd
rcilgcgk.co.uk
wwwlmy.com.hn
zxszv.com.ar
zfmflv.tc
jttbrq.co.id
lfjxj.co.kr

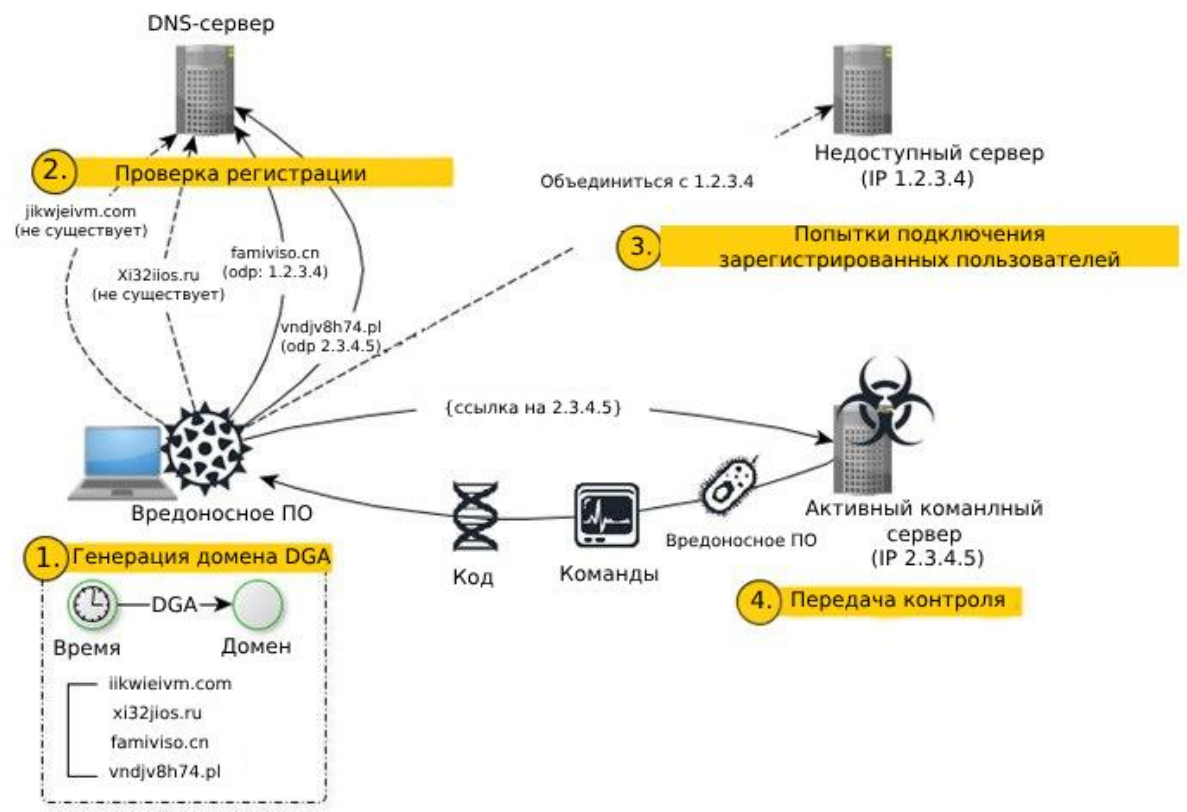

Рисунок 1 – Схема механизма генерации доменов-DGA

Самые стойкие и ценные для защиты являются МОКи (механизмы обнаружения компрометации), описывающие всю оперативную работу. Иногда разработчики вредоносного ПО ошибаются при попытке получить доступ к несуществующей учетной записи или при использовании определенной техники или инструментов атаки. Эти особенности помогают выявлять последующие поколения угроз с высокой вероятностью обнаружить тех самых злоумышленников.

Анализ разновидностей технологий по защите и мониторингу злонамеренных ПО.

QualysGuard — это инновационная технология сканирования, основанная на логических выводах нового поколения. Этот веб-сервис, который управляется пользователями, но размещается и управляется удаленно, автоматизирует проверку безопасности и управление уязвимостями в сетях. Это позволяет администраторам безопасности работать более эффективно и продуктивно. Цикл управления уязвимостями с помощью QualysGuard можно увидеть на рисунке 2. QualysGuard преследует точку зрения хакера - “извне внутрь” - и анализирует сеть как изнутри, так и снаружи брандмауэра. Этот сервис предоставляется по подписке, что дает клиентам возможность выполнять неограниченное количество сканирований по запросу или по расписанию из любого веб-браузера. Стоимость подписки зависит от количества сканируемых IP-адресов, что позволяет сетевым администраторам проводить столько сканирований, сколько им необходимо для выявления уязвимостей и проверки успешного исправления. Подключившись к сервису QualysGuard, компании получают преимущество объективной оценки от независимой третьей стороны. Это помогает им автоматически обнаруживать уязвимости, которые могли бы остаться незамеченными при самостоятельной проверке, а также соответствовать стандартам отраслевой безопасности и корпоративного управления [3].

Рисунок 2 – Цикл управления уязвимостями с помощью QualysGuard

Zabbix - это эффективная система мониторинга и управления различными IT-ресурсами, включая сети, серверы, приложения и другие компоненты. Она предлагает централизованное решение для отслеживания и анализа различных параметров и состояний системы в реальном времени. Работу инструмента Zabbix можно посмотреть на рисунке 3.

Описание работы с Zabbix:

1) Начните с установки и настройки. Первый шаг - установить сервер Zabbix и агентов на отслеживаемые узлы. Затем следует провести настройку, включая параметры подключения, сетевые настройки и другие детали.

2) Определите хосты и элементы мониторинга. В Zabbix определяются хосты (системы, которые будут отслеживаться) и элементы мониторинга (например, процессор, память, дисковое пространство и другие параметры для мониторинга). Для каждого элемента задается пороговые значения и условия тревоги.

3) Создайте триггеры и условия тревоги. В Zabbix создаются триггеры для определения условий возникновения тревоги. Это может быть превышение пороговых значений или другие неполадки в системе.

4) Настройте уведомления. При возникновении тревоги можно настроить отправку уведомлений администраторам или ответственным лицам через электронную почту, SMS или другие доступные каналы связи.

5) Мониторинг и анализ. Zabbix автоматически собирает данные от агентов и проводит мониторинг параметров системы. Он отображает информацию в виде графиков, диаграмм и отчетов, что помогает администраторам следить за состоянием системы, оценивать производительность и выявлять проблемы

Оптимизация и настройка. При использовании Zabbix возможно провести оптимизацию мониторинга для улучшения производительности системы и ее адаптации под конкретные потребности. Zabbix предлагает широкий спектр возможностей и функций для мониторинга и управления IT-инфраструктурой. Он является гибким и масштабируемым решением, позволяющим эффективно отслеживать состояние системы и оперативно реагировать на возникающие проблемы [4].

Рисунок 3 – Работа инструмента Zabbix

Монитор процесса (ProcMon).

ProcMon — это мощный инструмент от Microsoft, который отслеживает активность файловой системы в реальном времени, например, создание процессов и изменения в реестре. Работу инструмента ProcMon можно посмотреть на рисунке 4. Это удобно совмещать с Process Hacker: можно создать новый процесс и быстро завершить его. Затем этот процесс можно просмотреть в журнале ProcMon. Аналитики могут быстро определить, какие процессы были созданы, откуда запущен файл и какие у него родительские и дочерние зависимости, используя готовые фильтры или дерево процессов. При анализе вредоносных документов особенно полезен ProcMon. Злоумышленники, стоящие за Emotet, часто используют вредоносные документы Word как вектор атаки. Макросы из файла Word при активации подключаются к инфраструктуре C2 злоумышленников и загружают полезную нагрузку Emotet без видимых для пользователя следов на зараженном устройстве. С помощью ProcMon можно отследить открытие

документа Word, обнаружить скрытый запущенный процесс PowerShell и выполнение команды base64 encoding. Одной из проблем с ProcMon является его способность быстро записывать более 100 000 событий за короткое время. Хотя фильтры в ProcMon эффективны, всегда есть возможность пропустить нужное событие. Тем не менее данные можно экспортировать в формат CSV для последующей обработки другим инструментом из моего списка [5].

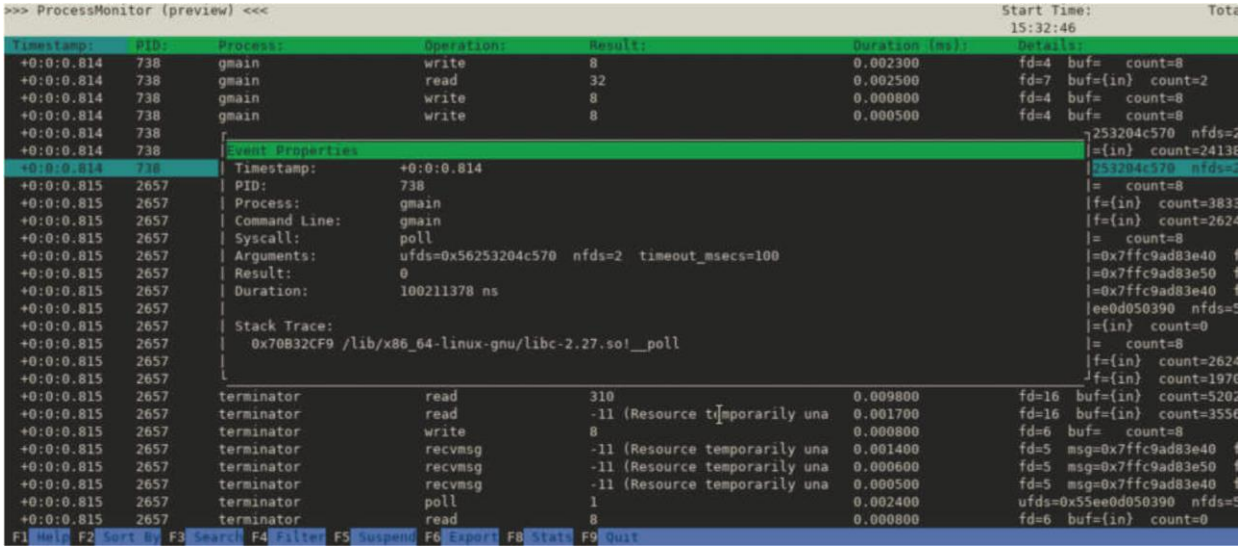

Рисунок 4 – Работа с инструментом ProcMon

Результаты.

В ходе анализа методов динамического обнаружения и анализа злонамеренного программного обеспечения в реальном времени на каждом уровне исследования были выявлены определенные уязвимости систем, которые подвержены злонамеренному программному обеспечению и методы защиты, такие как технологии сканирования, монитор процесса, управления сетями, программы для анализа вредоносных ПО, инструменты для автоматизированного тестирования и анализа качества кода приложения.

Обсуждение.

Анализ вредоносных программ может быть выполнен в основном с помощью статического анализа, анализа кода, динамического анализа, анализа памяти и гибридных методов анализа. Статический анализ предполагает анализ исполняемого двоичного файла без его запуска. Метаданные, связанные с подозрительным двоичным файлом, могут быть извлечены и проанализированы с помощью статического анализа. Динамический анализ кода связан с отладкой подозрительной программы в реальной или виртуальной среде.

Важно отметить, что важно понять какая уязвимость перед нами, поэтому и существуют столько методов. После анализа злонамеренных ПО будет понимание, где брешь и знание как создать надежную систему информационной безопасности в рамках современных организаций.

Выводы.

В данной статье мы рассмотрели такую важную тему, как исследование методов динамического обнаружения и анализа злонамеренного программного обеспечения в реальном времени, рассмотрели методы мониторинга и управления IT-ресурсами.

Понимание и применения методов предотвращения и защиты позволяет эффективно защищать информацию в рамках современных реалиях.

ЛИТЕРАТУРА

[1] Украинский Д.Д., Статистический и динамический анализ как методы исследования вредоносных компьютерных программ в рамках судебной компьютерно-программной экспертизы, журнал «Научный аспект» №11-2023, Самара, 2023. –с. 57.

[2] Галиахметов Д.Г., Сравнение алгоритмов классификации применительно к задаче обнаружения вредоносных доменных имен, Математические методы в технике и технологиях – ММТТ, Т. 12-1, 2019. –с. 190.

[3] Himanshu K., CVE-2021-3156: Heap-Based Buffer Overflow in Sudo (Baron Samedit), Qualys Community, 2022, [Электронный ресурс]. – URL: https://blog.qualys.com/vulnerabilities-threat-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit

[4] Смушкина В.А., Zabbix для мониторинга в IT-инфраструктуре, журнал «Форум молодых ученых» №4(32), Красноярск, 2019. –с. 958.

[5] Alex M., Getting started with Procmon: The Beginner’s Guide to Monitoring Windows Systems, The MSIx Experts Crib, 2022, [Электронный ресурс]. – URL: https://www.advancedinstaller.com/process-monitor-beginner-guide.html

REFERENCES*

[1] Ukrainskij D.D., Statisticheskij i dinamicheskij analiz kak metody issledovanija vredonosnyh komp'juternyh programm v ramkah sudebnoj komp'juterno-programmnoj jekspertizy, zhurnal «Nauchnyj aspekt» №11-2023, Samara, 2023. –s. 57.

[2] Galiahmetov D.G., Sravnenie algoritmov klassifikacii primenitel'no k zadache obnaruzhenija vredonosnyh domennyh imen, Matematicheskie metody v tehnike i tehnologijah – MMTT, T. 12-1, 2019. –s. 190.

[3] Himanshu K., CVE-2021-3156: Heap-Based Buffer Overflow in Sudo (Baron Samedit), Qualys Community, 2022, [Jelektronnyj resurs]. – URL: https://blog.qualys.com/vulnerabilities-threat-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit

[4] Smushkina V.A., Zabbix dlja monitoringa v IT-infrastrukture, zhurnal «Forum molodyh uchenyh» №4(32), Krasnojarsk, 2019. –s. 958.

[5] Alex M., Getting started with Procmon: The Beginner’s Guide to Monitoring Windows Systems, The MSIx Experts Crib, 2022, [Jelektronnyj resurs]. – URL: https://www.advancedinstaller.com/process-monitor-beginner-guide.html

Ерсайын Майлыбаев, PhD, Халықаралық көліктік-гуманитарлық университеті, Алматы, Қазақстан, ersind@mail.ru

Анна Козьякова, студент, Satbayev University, Алматы, Қазақстан, st_un@mail.ru

Владислав Прошин, студент, Satbayev University, Алматы, Қазақстан, vp2020@mail.ru

Ерлан Таштай, т.ғ.к., доцент, Satbayev University, Алматы, Қазақстан, y.tashtay@satbayev.university

НАҚТЫ УАҚЫТТАҒЫ ЗИЯНДЫ БАҒДАРЛАМАЛЫҚ ЖАСАҚТАМАНЫ ДИНАМИКАЛЫҚ АНЫҚТАУ ЖӘНЕ ТАЛДАУ ӘДІСТЕРІН ЗЕРТТЕУ

Аңдатпа. Бұл ғылыми мақалада нақты уақыттағы зиянды бағдарламалық жасақтаманы динамикалық анықтау және талдау әдістері қарастырылған. Зиянды бағдарламалық жасақтаманы анықтау және талдау мәселесі киберқауіпсіздік қаупі үнемі дамып келе жатқан қазіргі ақпараттық қоғамда өзекті бола түсуде. Мақалада зиянды бағдарламалық жасақтаманы динамикалық түрде анықтаудың қолданыстағы тәсілдері талданды және олардың артықшылықтары мен кемшіліктері анықталды. Сондай-ақ, нақты уақыт режимінде зиянды бағдарламалық жасақтаманы тиімді анықтауға және талдауға қабілетті машиналық оқыту әдістері мен бағдарламалардың мінез-құлқын талдауға негізделген жаңа әдіс ұсынылды.

Түйінді сөздер. Зиянды бағдарламалық жасақтама, кибершабуылдар, зиянды бағдарламалар, динамикалық кодты талдау, бақылау.

Yersaiyn Mailybayev, PhD, International University of Transport and Humanities, Almaty, Kazakhstan, ersind@mail.ru
Anna Kozyakova, student, Satbayev University, Almaty, Kazakhstan, st_un@mail.ru
Vladislav Proshin, student, Satbayev University, Almaty, Kazakhstan, vp2020@mail.ru
Erlan Tashtai, candidate of technical sciences, docent, Satbayev University, Almaty, Kazakhstan, y.tashtay@satbayev.university

RESEARCH OF METHODS OF DYNAMIC DETECTION AND ANALYSIS OF MALICIOUS SOFTWARE IN REAL TIME

Abstract. This scientific article discusses methods of dynamic detection and analysis of malicious software in real time. The problem of detecting and analyzing malicious software is becoming increasingly relevant in the modern information society, where cybersecurity threats are constantly evolving. The article analyzes the existing approaches to the dynamic detection of malicious software and identifies their advantages and disadvantages. A new method based on a combination of machine learning techniques and program behavior analysis is also proposed, which is able to effectively identify and analyze malicious software in real time.

Keywords. Malicious software, cyber-attacks, malware, dynamic code analysis, monitoring.

****

Редакцияға түсті / Поступила в редакцию / Received 13.05.2024
Жариялауға қабылданды / Принята к публикации / Accepted 29.09.2024