

УДК 004.056.57

Разработка специализированного модуля системы нахождения и противодействия компьютерным вирусам в программном обеспечении на производстве

Чекалкин Владимир Дмитриевич

Князева Светлана Вадимовна (научный руководитель)

МГТУ им. Н.Э. Баумана, Москва, Россия

Рассмотрена возможность противодействия уязвимости программного обеспечения в производственных системах. Воздействие вредоносного программного обеспечения, особенно криптомайнеров, вызывает сбои и простои производства. Предложен экспериментальный модуль обнаружения, учитывающий специфику промышленных сред. Анализ количества потоков по определенному принципу и их жизненному циклу помогает выявить угрозы, обеспечивая бесперебойность и стабильность выполнения производственных процессов.

Ключевые слова: программное обеспечение в производстве, вирусы, вредоносное программное обеспечение, потоки в операционной системе, процессы в операционной системе

Введение. Современные производственные процессы в значительной степени зависят от специализированного программного обеспечения (ПО), обеспечивающего автоматизацию и оптимизацию технологических операций. Однако наличие вредоносного ПО, включая криптомайнеры, которые потребляют значительные вычислительные ресурсы, может привести не только к сбоям в работе оборудования, но и к простоям производства. В связи с этим актуальной задачей является разработка специализированного модуля для детектирования вредоносных программ, в том числе ресурсоемких майнеров, способных дестабилизировать работу промышленных систем. Разработка такого модуля требует не только учета специфики промышленных сред, включая требования к минимальной нагрузке на оборудование и высокую отказоустойчивость, но также требует криминалистического подхода к выявлению противоправного ПО. Внедрение предложенного решения обеспечит устойчивость и бесперебойность производственных процессов, а также повысит ее экономичность.

Архитектура разработанного программного комплекса. Архитектура разработанного программного комплекса под ОС Windows представлена на рисунке и построена по модульному принципу. Такой принцип обеспечивает в дальнейшем гибкость и масштабируемость решения.

Центральным компонентом системы является модуль сбора данных о процессах (ProcessMonitor), который реализует функции инвентаризации запущенных процессов через парсинг файлов снимков системы (snapshots) и использование Windows API для получения точных временных характеристик потоков.

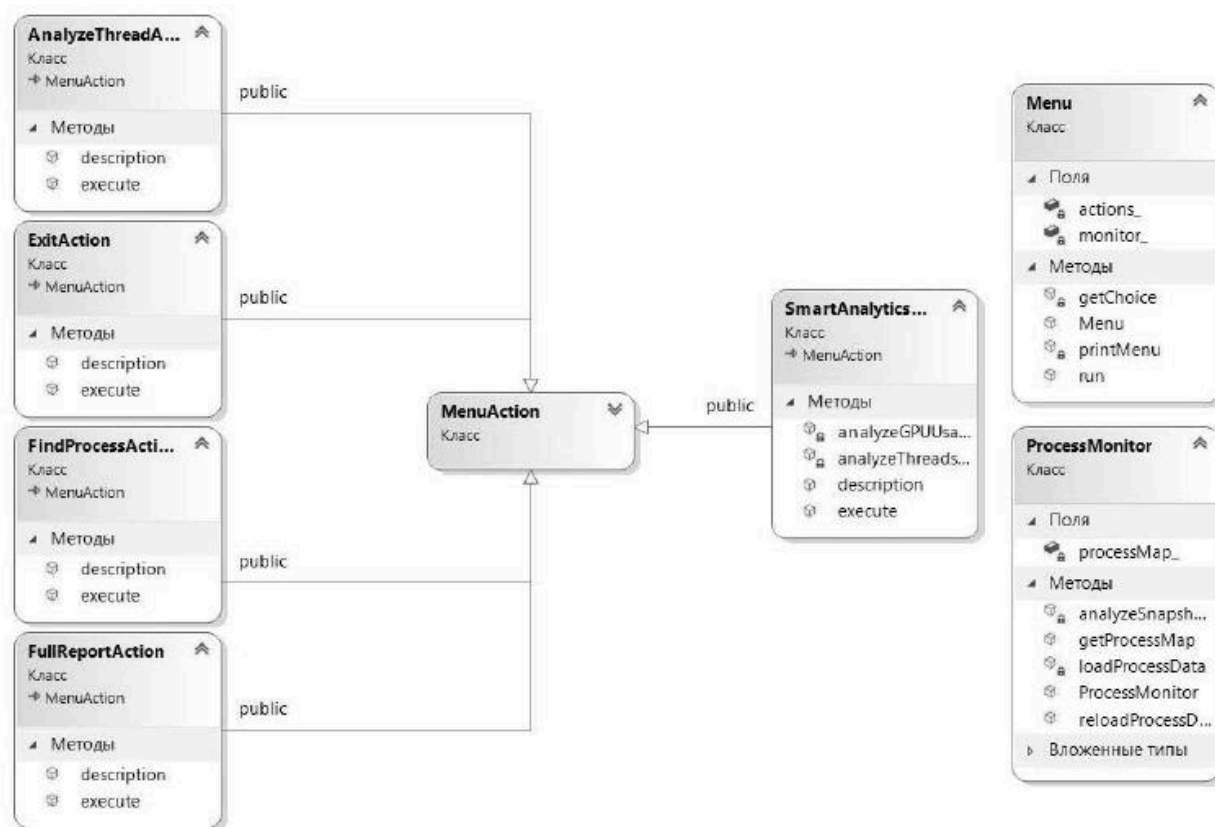


Диаграмма классов

Важнейшим аналитическим модулем выступает SmartAnalyticsAction, реализующий алгоритмы выявления аномалий в поведении процессов [1].

Одним из аспектов анализа является вычисление загрузки CPU на уровне отдельных потоков. Для этого используется формула

$$CPU_{usage} = \frac{[(KernelTime_2 + UserTime_2) - (KernelTime_1 + UserTime_1)]}{(MeasurementInterval) \times 100\%},$$

где KernelTime и UserTime — время выполнения потока в режиме ядра и пользовательском режиме соответственно; MeasurementInterval — интервал измерения; CPU_{usage} — загрузка CPU на уровне отдельных потоков.

Динамика создания/уничтожения потоков анализируется через мониторинг их жизненного цикла с вычислением показателя частоты регенерации потоков

$$Thread_Regeneration_Rate = \frac{(N_{new_threads} + N_{terminated_threads})}{(Observation_Period \times Total_Threads)},$$

где Total_Threads — общее число потоков; Observation_Period — интервал снятия данных; $N_{new_threads}$ — число созданных потоков; $N_{terminated_threads}$ — число уничтоженных потоков; Thread_Regeneration_Rate — частота регенерации потоков.

Значения CPU выше 0,2 считаются потенциально опасными согласно исследованиям Payload Security.

В основе работы модуля, который анализирует центральный процессор (CPU), лежат низкоуровневые функции API операционной системы Windows Thread. Эти функции позволяют с точностью до наносекунды измерять временные характеристики потоков.

Методология анализа сочетает несколько инновационных подходов, интегрируя методы поведенческого анализа с принципами цифровой криминалистики [2]. Анализ количества потоков основан на эмпирически установленном факте, что легитимные приложения редко используют более 10 потоков, тогда как вредоносное ПО часто создает их избыточное количество для брутфорс-алгоритмов или, в нашем случае, для уменьшения производительности системы за счет вычислений хеша криптовалют. Динамический анализ жизненного цикла потоков позволяет выявлять инжекторы кода по характерным паттернам постоянного создания/уничтожения потоков.

С криминалистической точки зрения, разработчики современных вредоносных программ (особенно криптомайнеров) сталкиваются с парадоксальной задачей, а именно, их ПО должно одновременно:

- использовать максимально доступное количество вычислительных мощностей;
- оставаться незаметным для пользователя и систем мониторинга [3].

Сравнительный анализ демонстрирует существенные преимущества предлагаемого решения перед традиционными антивирусами. Ресурсная эффективность обеспечивается ограниченным временем работы (10 секунд для полного анализа) против постоянного фонового мониторинга антивирусов. Способность обнаруживать неизвестные угрозы через поведенческий анализ превосходит сигнатурные методы. Глубокая аналитика на уровне потоков обеспечивает детализацию, недоступную большинству антивирусных решений [4, 5].

Научная новизна подхода заключается в комбинации временных характеристик потоков (через FILETIME структуры) с количественным анализом их поведения. Многоуровневая система оценки угрозы учитывает как абсолютные значения (количество потоков), так и относительные показатели (нагрузка CPU, частота регенерации).

Заключение. Следует отметить, что представленный вариант программного комплекса демонстрирует эффективный подход к выявлению вредоносного ПО через инновационную методику анализа процессов и потоков. Сочетание научно обоснованных алгоритмов с практической реализацией делает данное решение перспективной альтернативой традиционным антивирусным системам, особенно в условиях резкого роста угроз информационной безопасности.

Литература

- [1] Egele M., Scholte T., Kirda E., Kruegel C. A Survey on Automated Dynamic Malware-Analysis Techniques and Tools. ACM-Transaction, 2012, vol. 44, no. 2.
<http://doi.acm.org/10.1145/2089125.2089126>

- [2] Эриксон Д. *Хакинг: искусство эксплойта*. Санкт-Петербург, Питер, 2018, 496 с.
- [3] Сикорски М., Хониг Э. *Вскрытие покажет! Практический анализ вредоносного ПО*. Санкт-Петербург, Питер, 2018, 768 с.
- [4] Русинович М., Соломон Д., Ионеску А., Йосифович П. *Внутреннее устройство Windows*. Санкт-Петербург, Питер, 2018, 944 с.
- [5] Макконнелл С. *Совершенный код. Мастер-класс*. Москва, Русская редакция, 2010, 896 с.

Specialized Module Development for Detecting and Countering Computer Viruses in Production Software

Chekalkin Vladimir Dmitrievich

Knyazeva Svetlana Vladimirovna (*scientific advisor*)

BMSTU, Moscow, Russia

The article discusses the possibility of countering software vulnerabilities in production systems. Exposure to malicious software, especially cryptominers, causes disruptions and production downtime. An experimental detection module is proposed that takes into account the specifics of industrial environments. Analyzing the number of threads based on a certain principle and their life cycle helps identify threats, ensuring uninterrupted and stable performance of production processes.

Keywords: production software, viruses, threads and processes, Windows environment
t