УДК 004.056

Особенности разработки и оценки системы раннего обнаружения программ-шифровальщиков в информационно-управляющей системе орбитальной группировкой космических аппаратов

Долгов Евгений Валентинович(*) dogobvk@gmail.com

НИУ «МИЭТ», Москва, Россия

Аннотация. *Представляется один из методов раннего обнаружения программ-шифровальщиков, опирающийся на агрегированную телеметрию подсистем хранения и оперативной памяти. Комбинация первичного аномалистического детектора и последующей проверки классификатором позволяет поймать раннюю фазу шифрования при контролируемом уровне ложных срабатываний. Сбор телеметрии выполняется легким гипервизором вне гостевой ОС, что повышает устойчивость к компрометации контролируемой системы и упрощает интеграцию с существующими контурами мониторинга.*

Ключевые слова: *информационно-управляющая система, орбитальная группировка, враждебная неисправность, детектор, программы-шифровальщики*

Введение. Орбитальные группировки являются неотъемлемой частью современной жизни, выполняя широкий спектр целевых задач в разных областях: геология, метеорология, связь, навигация и многое другие. Надежность, длительные сроки активного существования, гарантоспособность [1] определяют качество выполнения целевых задач. Неисправности управляющей системы орбитальных группировок могут привести к серьезным проблемам от финансовых потерь до техногенных катастроф. Особенно это относится к неисправностям, носящим враждебный («византийский») характер [2].

В [3] показано, что одной из причин появления враждебных неисправностей могут оказаться компьютерные вирусы, представляющие большую опасность для управляющих систем орбитальными группировками. Поэтому цель данной работы — повышение устойчивости таких систем к вирусным атакам, в частности, к проблемам, создаваемым программами-шифровальщиками.

В данной работе ставится задача заложить основу метода, который позволяет как можно раньше замечать начало шифрования, опираясь на ограниченный набор доступных данных [4] и одновременно соблюдая требования к надежности и устойчивости к сбоям управляющих систем орбитальной группировки.

Методы и материалы; результаты. Исходные данные — журналы низкоуровневых обращений к диску и памяти. Для анализа формировались перекрывающиеся окна, по каждому окну вычислялись устойчивые агрегаты: скорости чтения и записи, квантильные и вариативные показатели размеров

блоков, доля высокоэнтропийных записей, а также межоконные изменения и тренды. Isolation Forest обучается на доброкачественных данных и выдает оценку аномальности каждого окна, которая затем используется как дополнительный признак во входе модели CatBoost., после чего CatBoost классифицировал отмеченные окна, обучаясь на примерах шифровальщиков и «шумных» легитимных задач, что уменьшало число ложных тревог. Качество оценивалось по точности, полноте, F-мере (среднее гармоническое точности и полноты) и показало раннюю фиксацию начала шифрования при сохранении низкой доли ложных срабатываний.

Заключение. Полученные результаты соответствуют ожиданиям: комбинация выявления аномалий и последующей классификации снижает ложные тревоги при сохранении высокой полноты. Данный сенсор можно использовать как основу второго эшелона защиты в обороне космических аппаратов и для проектирования автоматических реакций в них, например, изоляции подозрительных модулей, временной блокировки записи на хранилище.

Список источников

[1] Авиженис А., Лапри Ж.-К. Гарантоспособные вычисления: от идей до реализации. *ТИИЭР*, 1986, т. 74, № 5, с. 8–21.

[2] Lamport L., Shostak R., Pease M. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 1982, vol. 4, no. 3, pp. 382–401.

[3] Ашарина И.В. Компьютерный вирус как разновидность враждебной неисправности в системе управления орбитальной группировкой космических аппаратов. *L Академические чтения по космонавтике, посвященные памяти академика С.П. Королёва и других выдающихся отечественных ученых — пионеров освоения космического пространства: сб. тез.* Москва, Изд-во МГТУ им. Н.Э. Баумана, 2026.

anabu Hirano, Ryotaro Kobayashi. RanSMAP: Open dataset of Ransomware Storage and Memory Access Patterns for creating deep learning based ransomware detectors. *Computers & Security*, 2025, vol. 150, art. no. 104202. https://doi.org/10.1016/j.cose.2024.104202