РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

RU2023619553

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2023619553
Дата регистрации: **12.05.2023**
Номер и дата поступления заявки:
2023618737 03.05.2023
Дата публикации и номер бюллетеня:
12.05.2023 Бюл. № 5

Контактные реквизиты:
115409, Москва, Каширское шоссе, 31, НИЯУ МИФИ, ОУИС, info@mephi.ru

Автор(ы):
Басыня Евгений Александрович (RU),
Антропов Даниил Сергеевич (RU),
Сапегин Владислав Юрьевич (RU),
Когос Константин Григорьевич (RU)

Правообладатель(и):
федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ) (RU)

Название программы для ЭВМ:
«Автоматизированная система выявления вредоносного программного обеспечения типа Ransomware в операционных системах семейства Linux»

Реферат:
Назначение программы: выявление вредоносной активности программ-вымогателей на ЭВМ, функционирующих на базе операционных систем семейства Linux. Выявление вредоносного программного обеспечения базируется на анализе событий, регистрируемых в подсистеме eBPF. В основе ее ключевых метрик лежит анализ потребления системных ресурсов и пакетов, передаваемых по корпоративной вычислительной сети. Область применения: системы для предотвращения утечек конфиденциальных данных в корпоративной вычислительной сети. Функциональные возможности программы: мониторинг и анализ вредоносной активности программ-вымогателей при использовании подсистемы eBPF в классах систем EDR/XDR/DLP. Способ использования: интеграция частей системы на ЭВМ, выполняющих роль клиента и/или сервера. Тип ЭВМ: IBM PC-совмест. ПК. ОС: Ubuntu 20.04 LTS и выше.

Язык программирования: Python

Объем программы для ЭВМ: 11 МБ