



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2023619552

Дата регистрации: 12.05.2023

Номер и дата поступления заявки:
2023618739 03.05.2023

Дата публикации и номер бюллетеня:
12.05.2023 Бюл. № 5

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

Автор(ы):

Басыня Евгений Александрович (RU),
Сапегин Владислав Юрьевич (RU),
Антропов Даниил Сергеевич (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 вредоносных программ типа Ransomware на основе анализа взаимодействия с файловой и сетевой системами»

Реферат:

Назначение программы: выявление вредоносной активности программ-вымогателей (англ. Ransomware) на ЭВМ, функционирующих на базе операционных систем семейства Windows. Выявление вредоносной программной активности базируется на анализе событий, регистрируемых в подсистеме Event tracing for Windows. В основе ее ключевых метрик лежит анализ пакетов и потребления системных ресурсов. Область применения программы: корпоративные вычислительные сети, функционирующие на основе стека протоколов TCP/IPv4. Функциональные возможности программы: мониторинг сетевой и файловой активности в корпоративных вычислительных сетях с целью предотвращения угроз вредоносных последствий действия программ-вымогателей. Способ использования: интеграция частей системы на ЭВМ, выполняющих роль клиента и/или сервера. Тип ЭВМ: IBM PC-совмест. ПК. ОС: Windows 10 и выше.

Язык программирования: Python

Объем программы для ЭВМ: 15,300 МБ