БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра технологий программирования

Аннотация к дипломной работе

«Использование open source инструментария peframe для статического анализа подозрительных файлов»

Шолохов Владислав Игоревич

Научный руководитель – кандидат технических наук, доцент кафедры технологий программирования Войтешенко И. С.

Минск, 2021

РЕФЕРАТ

Дипломная работа, с.48, рис.36, 7 источников.

Ключевые слова: СТАТИЧЕСКИЙ АНАЛИЗ, PEFRAME, ВРЕДОНОСНОЕ ПО.

Объект исследований – open source инструментарий Peframe, вредоносное ПО, статический анализ.

Цель работы – изучить возможности open source инструментария Peframe, проанализировать различные образцы вредоносного.

В результате исследования изучены основные категории вредоносного ПО, изучены возможности open source инструментария Peframe и их применение для идентификации вредоносного ПО, проведен статический анализ вредоносного.

Методы исследования – статический анализ вредоносного ПО в изолированной среде.

Областью применения является обеспечение безопасности системы.

РЭФЕРАТ

Дыпломная праца, с. 48, мал. 36, 7 крыніц.

Ключавыя словы: СТАТЫЧНЫ АНАЛІЗ, PEFRAME, ШКОДНАСНАЕ ПЗ.

Аб'ект даследаванняў: open source інструментар Peframe, шкоднаснае ПЗ, статычны аналіз.

Мэта работы: вывучыць магчымасці open source інструментара Peframe, прааналізаваць розныя ўзоры шкоднаснага.

У ***выніку даследавання*** вывучаны асноўныя катэгорыі шкоднаснага ПЗ, вывучаны магчымасці open source інструментара Peframe і іх прымяненне для ідэнтыфікацыі шкоднаснага ПА, праведзены статычны аналіз шкоднаснага ПЗ.

Метады даследавання: статычны аналіз шкоднаснага ПА ў ізаляванай асяроддзі.

Вобласцю карыстання з'яўляецца забеспячэнне бяспекі сістэмы.

Abstract

Diploma project, 48p., 36 pic., 7 sources.

Keywords: STATIC ANALYSIS, PEFRAME, MALWARE.

Subject - open source Peframe toolkit, malware, static analysis.

Work goals: explore the capabilities of the open source Peframe toolkit, analyze various malware samples.

Results: The main categories of malware were examined, the capabilities of the open source Peframe toolkit and their use for malware identification were examined, and a static analysis of malware was performed.

Methods of research*:* static analysis of malware in an isolated environment.

Using sphere*:* ensuring the security of the system.