Университет ИТМО, факультет программной инженерии и компьютерной техники
Двухнедельная отчётная работа по «Информатике»: аннотация к статье

Дата прошедшей лекции	Номер прошедшей лекции	Название статьи/главы книги/видеолекции	Дата публикации (не старше 2021 года)	Размер статьи (от 400 слов)	Дата сдачи
11.09.2024	1	Энтропия. Как хаос помогает искать вирусы	29.01.2021	~1300	25.09.2024
25.09.2024	2				
	3				
	4				
	5				
	6				
	7				

Выполнил(а) Галак Е. А., № группы *P3115*, оценка _____
Фамилия И.О. студента — не заполнять

Прямая полная ссылка на источник или сокращённая ссылка (bit.ly, tr.im и т.п.)
https://xakep.ru/2021/01/29/viruses-entropy/

Теги, ключевые слова или словосочетания (минимум три слова)
Энтропия, вирусный анализ, вирус, метод скользящего окна, обфускация

Перечень фактов, упомянутых в статье (минимум четыре пункта)

1. Энтропия – это мера хаоса в расположении данных внутри файла (чем хаотичнее данные, тем выше энтропия).
2. Энтропия рассчитывается методом «скользящего окна», учитывая частоты появления различных значений байтов.
3. Высокая энтропия может свидетельствовать о наличии вирусов, т.к. вредоносный код может создаваться с помощью случайных элементов для затруднения обнаружения антивирусами.
4. Высокая энтропия может указывать на неравномерное распределение кода и наличие обфускации или шифрования.

Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)

1. Анализируя энтропию подозрительных файлов, можно определить, были ли они зашифрованы, подвержены обфускации или сжаты.
2. Использование энтропии в антивирусных программах помогает им лучше распознавать угрозы и снижает количество ложных тревог, что делает антивирусы более точными.
3. Анализ энтропии позволяет быстрее обнаруживать неизвестные ранее типы вирусов, особенно те, которые маскируются под случайные данные.

Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)

1. Высокая энтропия не всегда указывает на наличие вирусов, что может привести к ложным срабатываниям антивирусных программ.
2. Злоумышленники могут использовать знания об энтропии, чтобы создавать вирусы, которые сложнее обнаружить с её помощью, что может затруднить борьбу со злоумышленниками.
3. Энтропия не гарантирует обнаружение всех типов вирусов (вирусы, которые используют сложные методы шифрования или обфускации, могут легко обмануть анализ энтропии).

Ваши замечания, пожелания преподавателю *или* анекдот о программистах[1]