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	Information Theory, Living Systems, Communication Engineering	18.05.2024	~5050	25.09.2024
25.09.2024	2	Research and Development of Data Compression Methods Based on Neural Networks	01.01.2023	~3122	09.10.2024
09.10.2024	3	Web Scraping or Web Crawling: State of Art, Techniques, Approaches and Application	03.11.2021	~9800	23.10.2024
23.10.2024	4	MarkupLM: Pre-training of Text and Markup Language for Visually-rich Document Understanding	11.03.2022	~2900	06.11.2024
06.11.2024	5	Automated analysis of malicious Microsoft Office documents	March 2022	~9900	20.11.2024
	6				
	7				

Выполнил(а) Юксель Хамза, № группы *P3132*, оценка _____
Фамилия И.О. студента — не заполнять

Прямая полная ссылка на источник или сокращённая ссылка (bit.ly, tr.im и т.п.)
https://doi.org/10.1016/j.cose.2021.102582

Теги, ключевые слова или словосочетания (минимум три слова)
Malware, Office documents, Macro malware, Powershell, LOLBAS

Перечень фактов, упомянутых в статье (минимум четыре пункта)
1. Malicious actors frequently utilize Microsoft Office documents as droppers to spread malware by downloading and executing harmful payloads, commonly employing LOLBAS (Living Off The Land Binaries and Scripts).
2. The article examines 15,571 malicious Microsoft Office documents, encompassing 13,518 Word documents, 1,996 Excel spreadsheets, and 13 PowerPoint presentations, spanning from 2006 to 2020.
3. VirusTotal scans of the malicious documents demonstrated a high detection rate, with 14,264 files identified as malicious by at least one antivirus product, although variations in detection rates were observed among different antivirus products.
4. The article introduces an automated analysis pipeline that classifies Microsoft Office documents as either benign or malicious by employing both static and dynamic analysis techniques to extract features that are subsequently utilized by machine learning models.
5. The study highlights the significance of a two-layer approach to effectively manage the volume and speed of Microsoft Office documents, combining static analysis with endpoint security mechanisms such as EPPs and EDRs.

Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)
1. High accuracy in detecting malicious Microsoft Office documents
2. Addresses biases in existing datasets.
3. Proactive approach to threat detection.
4. Efficient handling of large volumes of documents.

Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)
1. Dependence on Up-to-Date Threat Intelligence.
2. Limited Effectiveness Against Unknown Attacks.
3. Over-Reliance on Automation.
4. Adversarial Machine Learning.

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

[1] Наличие этой графы не влияет на оценку