Секция «Компьютерное право и информационная безопасность»

Анализ вредоносных программ с использованием облачных песочниц

Научный руководитель – Фролов Андрей Евгеньевич

Фоминых Владислав Вячеславович
Студент (бакалавр)
Алтайский государственный университет, Физико-технический факультет, Кафедра прикладной физики, электроники и информационной безопасности, Барнаул, Россия
E-mail: fominykhvladislav567@gmail.com

Развитие глобальных информационных сетей сделало распространение вредоносных программ более объемным. Вредоносные программы находят самые разные каналы проникновения и распространения, причем к старым способам постоянно добавляются новые. Злоумышленники постоянно развивают вредоносное ПО так, чтобы его не обнаруживали классические средства защиты: антивирусные средства, межсетевые экраны, IDS/IPS,почтовые и веб-шлюзы.

Чтобы создать, эффективную систему зашиты компьютерной системы и корпоративных сетей, а также справиться с постоянно растущим объемом образцов вредоносных программ, неизбежны методы автоматического анализа программ. В частности, песочницы стали стандартом де-факто для извлечения информации о поведении программы.

Цель работы заключается в анализе точек входа, которые могут быть использованы вредоносными программами, анализе онлайн сред для автоматического безопасного исполнения компьютерных программ.

Для достижения поставленной цели были сформулированы следующие задачи:

- определить каналы проникновения;
- определить основные индикаторы ВПО;
- сформулировать понятие песочница и рассмотреть примеры;
- выполнить анализ вредоносного ПО в онлайн-песочницах;
- провести сравнительный анализ онлайн-песочниц.

Источники и литература

1) Сикорски М. Вскрытие покажет! Практический анализ вредоносного ПО: пер. с англ. / М.Сикорски, Э.Хониг. - СПб. и др.: Питер, 2018. - 768 с. - (Для профессионалов).
2) https://bugs.chromium.org/p/project-zero/issues/detail?id=820 (Symantec/Norton Antivirus ASPack Remote Heap/Pool memory corruption Vulnerability CVE-2016-2208)
3) https://www.sans.org/blog/security-intelligence-attacking-the-cyber-kill-chain/ (Security Intelligence: Attacking the Cyber Kill Chain)
4) https://encyclopedia.kaspersky.ru/knowledge/how-malware-penetrates-systems/ (Способы проникновения вредоносных программ в систему)
5) https://tipi-hack.github.io/2020/03/29/VolgaCTF-Quals-20-NetCorp.html (Writeup VolgaCTF Qualifier 2020 – NetCorp)