УДК 004.056.53

СИСТЕМА КОМПЛЕКСНОГО АНАЛИЗА ОПЕРАТИВНОЙ ПАМЯТИ.

Рябенков М.Ю. (Государственный университет морского и речного флота имени адмирала С.О. Макарова)

Научный руководитель – Шипунов И.С.

(Государственный университет морского и речного флота имени адмирала С.О. Макарова)

Аннотация: Расследование преступлений является одной из важнейших областей информационной безопасности. Система комплексного анализа оперативной памяти направленна на облегчения процесса расследования инцидентов.

Введение. Тема информационной безопасности особенно актуальна в наше время. Количество киберпреступлений увеличивается из года в год. На данный момент преступность в информационной сфере достигла небывалых масштабах в связи с пандемией и переходом на дистанционный режим работы.

Компанией TrendMicro было заблокировано 48 млрд. атак в 2018 году. Positive Technologies отмечают, что количество атак во 2-ом квартале 2020 года увеличилось на 59% по сравнению со 2-м кварталом 2019 года. Процент направленных атак продолжает расти и, как следствие, ущерб компаний, подвергшихся нападению, увеличивается.

Методы киберпреступников постоянно совершенствуются и единственная возможность остановить рост количества преступлений – это позволить системам защиты развиваться в ногу со временем.

В данной ситуации, важную роль играет процесс расследования компьютерных инцидентов, который, в свою очередь, оказывает влияние на развитие систем безопасности.

Основная часть. Каждый из нас встречался с угрозами информационной безопасности в повседневной жизни будь то безобидный вирус или троян. Безусловно, каждый инцидент необходимо классифицировать и определить степень его угрозы, но не стоит забывать, что безответственное отношение к «мелким» инцидентам может послужить причиной существенных потерь в будущем.

Рационально исследуя причины нарушения, можно или повлиять на них с целью предотвращения преступления, или модифицировать требования к системе защиты от данного вида инцидентов.

Реагирование на инцидент является одним из важнейших критериев оценки эффективности информационной безопасности в целом. Исходя из этого, к самому процессу расследования должны быть применены специальные меры. К ним относится специальное программное обеспечение, которое должно быть предварительно установлено, сетевые и системные настройки, а также должна быть реализована возможность доступа к сети и системе, подвергшейся атаке, для специалистов, которые будут проводить расследование. Расследование инцидента должно проводится в соответствии со специально разработанным и четко определенным задокументированным планом. Вся информация, полученная в ходе расследования, также подлежит документации.

Расследование нарушений должно быть основано на следующей стратегии:

- Обнаружении инцидента;
- Сдерживание;
- Сбор доказательств;
- Устранение последствий;
- Предложения по совершенствованию системы.

Сбор доказательств включает в себя:

- Анализ журналов;
- Анализ сетевого трафика;
- Анализ оперативной памяти;

- Анализ жестких дисков;
- Анализ вредоносного ПО.

Система комплексного анализа оперативной памяти была реализована с использованием The Volatility Framework, проекта с открытым исходным кодом, написанного на языке программирования Python. Данный фреймворк является наиболее распространённой платформой для криминалистического анализа оперативной памяти.

Он обладает широкими аналитическими возможностями:

- Анализ процессов;
- Обнаружение API хуков в процессах и памяти ядра;
- Выгрузка процессов для обратного инжиниринга;
- Создание временных шкал из артефактов в памяти;
- Поиск скрытого и встроенного кода;
- Поддержка YARA.

Выводы. Данная система позволит ускорить процесс анализа дампов оперативной памяти. Кроме того, в состав включена YARA, система, предназначенная для облегчения работы исследователей. Она позволяет профессионалам писать собственные правила идентификации образов вредоносного ПО в системе (или любых других шаблонов, которые могут быть описаны в текстовом или бинарном формате). YARA используется в продуктах "Лаборатории Касперского", ESET, Radare2, McAfee и так далее.

Используя Volatility и базу правил YARA, система анализа оперативной памяти может производить тщательный поиск вредоносного ПО в оперативной памяти, а также отслеживать путь, пройденный вирусом в систему.

Данная система так же поддерживает плагины, написанные для фреймворка Volatility, тем самым предоставляя широкий спектр возможностей для улучшения и модификации системы анализа и позволяют развивать ее модульно, без больших затрат на разработку и обновление программного обеспечения. Достаточно разработать плагин и разместить его рядом с системой расследования инцидентов.

Рябенков М.Ю. (автор) Подпись

Шипунов И.С. (научный руководитель) Подпись