Борлакова М.А., Гебенова А.А., Халкечева А.А.

Применение инструментов форензики на пути к расследованию инцидентов

*Северо-Кавказская государственная академия
(Россия, Черкесск)*

doi: 10.18411/lj-01-2021-04

idsp: ljjournal-01-2021-04

Аннотация

В данной работе рассматривается применение инструментов форензики специализированные с целью фиксации утечек конфиденциальной данных, их сравнение и возможности, а также функционалы современных систем контроля информационных потоков.

Ключевые слова: DLP, инциденты, форензика, инфосистемы, Big Data, COPM.

Abstract

This paper discusses the use of specialized forensics tools for fixing confidential data leaks, their comparison and capabilities, as well as the functionality of modern information flow control systems.

Key words: DLP, incidents, forensics, information systems, Big Data, SORM.

Сегодня все шире используются технологические процессы обработки больших данных, интегрирующиеся, в частности, в DLP-решения и позволяющие изучать все информационные потоки компаний и предприятий. Однако появление этой функции превращает продукты защиты от утечек в инструменты расследования инцидентов.

Типичный инструмент DLP (защита от утечки данных) специализируется на устранении утечек конфиденциальных данных и, по сути, представляет собой систему для управления потоком информации в компании. Для решения всех задач такого контроля разработчики DLP-продуктов сформировали большое количество перехватчиков, агентов и поисковых роботов, которые собирают данные об информационных системах компании и деятельности отдельных ее сотрудников. При этом, как правило, все эти продукты фактически не защищают от потерь, а лишь помогают службе безопасности выявить факт нарушения правил обработки конфиденциальных данных. Именно по этой причине разработчики новых решений DLP начали внимательно изучать вопросы расследования инцидентов, для решения которых они начали объединять технологии больших данных в свои продукты.

Но расследование несчастных случаев - это не просто деятельность по предотвращению утечек или, скорее, судебная экспертиза - компьютерная криминалистика.

В функции судебно-медицинской экспертизы входит сбор и запись электронных доказательств. Для вашего последующего тщательного анализа с целью выяснения скрытых взаимосвязей и структур данных все это в точности покрывается функциональностью систем DLP, которые собирают информацию из различных источников и теперь могут быстро идентифицировать основные факты большого потока. различная информация. Следует иметь в виду, что инструменты анализа данных для визуализации обнаруженных структур, которые появились в продуктах DLP, по-прежнему представляют собой лишь небольшой набор инструментов судебной экспертизы. Для поставщиков DLP может не иметь смысла внедрять полный набор инструментов расследования, но наиболее популярные компоненты этих инструментов могут помочь командам по кибербезопасности быстро реагировать на инциденты.

Решение DLP со встроенными инструментами анализа больших данных было представлено InfoWatch в своем флагманском продукте Traffic Monitor, который теперь имеет возможность отслеживать действия сотрудников, определять их связи, оценивать

переписку и каналы для распространения информации среди сотрудников. Кроме того, был предложен интерфейс для руководителя корпоративного отдела, позволяющий просматривать все инциденты, связанные с подчиненными. Информация, полученная в ходе анализа, накапливается в специальном хранилище для дальнейшего изучения в ходе расследования.

МФИ-Софт, компания, специализирующаяся на производстве продуктов для организации СОРМ, представила новую версию своего продукта Garda Enterprise 3.0, традиционно также известного как DLP. Однако это типичный криминалистический инструмент. Продукт может исследовать собранные данные - в частности, вы можете быстро проанализировать отношения между сотрудниками по электронной почте. Garda Enterprise позволяет отследить, например, цепочку распространения определенного документа на предприятии, чтобы определить возможные каналы утечки. Для этого анализируется не только электронная переписка, но и записи журналов доступа к определенным файлам. В результате сотрудники службы информационной безопасности могут быстрее расследовать инциденты и устранять утечки, выявляя людей, которые могут быть готовы украсть ценную информацию.

Компания постаралась создать интерфейс, понятный всем категориям пользователей. Для продукта Garda Enterprise очень интересны графические инструменты для создания структур в исходных данных и инструменты для интерактивного изучения. Компания не раскрывает подробностей реализации, утверждая, что все функции новой версии основаны на технологиях больших данных - возможно, речь идет о параллельной обработке данных, которая позволяет нам выявлять скрытые зависимости в базе данных, построенной с использованием инструментов, близких к Hadoop, с использованием HDFS.

Компания «Инфосистемы Джет» представила версию продукта «Дозор-Джет», ознаменовавшую переход к аварийной модели. Этот продукт отслеживает поведение сотрудников на постоянной основе и создает синтетический индикатор - уровень доверия к сотруднику, который позволяет графически представить взаимодействие сотрудников. Создатели считают, что новая версия продукта - это не только способ защиты информации, но и решение проблем экономической безопасности.

Cisco пошла по другому пути, интегрировав аналитику в межсетевой экран Cisco ASA и дополнив ее технологиями Fire POWER от приобретенного SourceFire. В результате брандмауэр научился выявлять многовекторные угрозы как посредством динамического анализа событий в бизнес-системе, так и с помощью инструментов ретроспективного анализа, которые можно использовать для расследования инцидентов.

В частности, модуль Advanced Malware Protection (AMP) обеспечивает ретроспективный анализ распространения вредоносных программ на предприятии. Информация, собранная в AMP, позволяет анализировать путь проникновения вредоносного ПО в корпоративную сеть, что упрощает расследование инцидентов.

Разработка DLP-систем направлена на добавление функциональности, связанной с углубленным анализом контролируемых данных, для чего используется несколько исследовательских технологий, но разработчики не спешат раскрывать конкретные детали реализации, заявляя, в частности, что они создают собственные механизмы для. Однако для анализа больших информационных потоков используется арсенал инструментов для работы с большими наборами данных.

Таким образом, под влиянием судебной медицины функциональные возможности современных систем управления информационными потоками дополнились рядом новых функций.

Сбор информации о социальных связях от сотрудников. Хотя эта информация поступает из электронной почты, производители DLP смогли использовать

практически все каналы благодаря технологиям из арсенала инструментов для работы с большими данными, таким как Hadoop, распределенная база данных Hbase и платформа MongoDB NoSQL, которые обеспечивают параллельную обработку больших медиа-потоков. Контроль практически. Общение. в том числе мобильные устройства.

Таким образом, сроки взаимодействия сотрудников с течением времени могут значительно увеличиться за счет средств унифицированного общения и информации из социальных сетей. Благодаря этому вы можете контролировать каналы распространения информации в команде и выделять наиболее проблемные группы сотрудников.

Анализ распространения документов. Собирая информацию об отправленных файлах, DLP-система может определять каналы распространения конкретного документа, что важно для выявления случайных инцидентов, а затем корректировки прав доступа, шаблона, которому нужно следовать, и корпоративных политик безопасности. Современные решения DLP также имеют инструменты для анализа хранилища информации, чтобы определить, где сотрудники могут спрятать ценные документы, чтобы организовать отходы. Схема распространения информации по компании позволяет в ходе расследования определить, кто из сотрудников компании нарушил правила работы с информацией и политику безопасности доступа к данным.

Анализ распространения программ. В сегодняшних хорошо защищенных системах практически невозможно организовать утечку с использованием традиционных методов, таких как запись на внешний носитель или обычная печать, и даже инсайдерам приходится использовать специализированные программы для организации утечки. В то же время внешние злоумышленники также могут использовать вредоносное ПО. Таким образом, то, как такая программа проникает в корпоративную сеть, может быть полезно при расследовании инцидентов, а также при настройке поведения используемых защитных механизмов. Это правда, что контроль распространения программ - это задача сетевых устройств, которые записывают перемещения, в том числе коды, в корпоративной сети, но те же функции могут быть возложены на систему DLP.

В будущем все производители DLP-систем могут включать в свои продукты функции, приближающие их решения к инструментам отслеживания сотрудников. Однако следует иметь в виду, что программа специально разработана для проведения исследований на основе четко определенных критериев и отображения реляционных данных в соответствии с сетями. Отдельные лица или группы лиц определяются как предметы двойного назначения, распространение которых должно контролироваться регулирующим органом. Неясно, будут ли отечественные производители инструментов DLP предоставлять инструменты двойного назначения; в любом случае западные общества вряд ли приложат усилия.

1. Черняк Л. М. Барьеры на пути утечек данных: учебное пособие / Л. М. Черняк. - М.: Открытые системы, 2016. с. 24–31.
2. Семенин Д. Стекло для Больших Данных: учебное пособие / Д. Семенин. - М.: Открытые системы, 2016. с. 42–43.
3. Коржов В. Большие Данные в службе безопасности: учебное пособие / В. Коржов. - М.: Открытые системы, 2016. с. 48–49.
4. Бондаренко А. Политика информационной безопасности. [Электронный ресурс]. - Режим доступа: http://www.leta.ru/press-center/publications/article_295.html
5. Джей Б. Snort 2.1. Обнаружение вторжений: учебное пособие / Б. Джей. - М.: Бином-пресс, 2017. - 656 с.