деятельности ветеранов войны. Данные были представлены на сайте (www.poisk65.ukoz.ru). Материалы оформлены в виде проекта для учащихся базового звена школы.

При обзоре учебных пособий особое внимание было уделено работе исполнителей в среде JavaScript [2].

Материалы, рассмотренные на курсах повышения квалификации, можно использовать при работе учителей информатики в общеобразовательных школах и на практических занятиях для студентов вуза.

Библиографический список

1. Федеральный государственный образовательный стандарт общего образования: проект. – М.: Просвещение. 2008. – 21 с.

2. *Быкадоров Ю.А*. Информатика и ИКТ. 9 кл.: учеб. для общеобразовательных учреждений. – М.: Дрофа, 2008. – 319 с.

Е.Д. Шамонин

ВРЕМЕННЫЕ ОТМЕТКИ ФАЙЛОВЫХ ОБЪЕКТОВ

shamonined@mail.ru

Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, г. Екатеринбург

В некоторых случаях возникает необходимость восстановить предисторию того или иного файлового объекта (ФО). Наиболее часто такая потребность возникает в случае, когда есть подозрение на то, что в систему внедрен какой-либо вредоносный программный код. Анализ временных меток (ВО) ФО в большинстве случаев позволяет выявить новые внедренные, либо модифицированные ФО с последующим парированием их вредоносного воздействия.

Вне зависимости от развернутой на компьютере ОС и используемой файловой системы (ФС) все ФО имеют определенный набор временных отметок (ВО), которые условно можно разделить на две группы: внешние ВО и внутренние ВО. Группа внешних ВО хранится вне структуры файлового объекта (например, для ФС NTFS внешние ВО размещаются в атрибутах файловой записи объекта $MFT), а набор внутренних ВО хранится в структуре файлового объекта.

Количество временных отметок у одного файлового объекта составляет от трех ВО в ФС FAT до двенадцати в NTFS. Обычно регистрируют время создания (create, ctime, или время C), время последней записи (сохранения) данных (modify, mtime, или время M) и время последнего доступа (access, atime, или время A), которое можно понимать как время открытия файла в какой-либо программе, или запуска исполняемого файла. Кроме этого, в ФС NTFS предусмотрена метка последнего изменения метаданных файла (последней записи в файловую таблицу $MFT), которую условимся обозначать xtime или время X. В ФС NTFS внешние ВО хранятся в 8-байтовом формате FILETIME в атрибутах $STANDARD_INFORMATION ($SI) и $FILE_NAME ($FN) каждой файловой записи. Разработанная Хорьковым Д.А. утилита FTA (File Time Analyzer) позволяет извлекать ВО из файловой записи (рис. 1).

ВО выводятся утилитой FTA в двух видах, а именно, в привычном для восприятия человеком и в виде количества 100-наносекундных интервалов.

Временные отметки файла \.\FTA\dir0\1.txt
SI: Время создания 30.10.2011 1:35:02 C = 129644121027079711
SI: Время посл. модификации 30.10.2011 1:35:02 M = 129644121027235961
SI: Время последнего доступа 30.10.2011 1:35:02 A = 129644121027079711
SI: Время модификации записи 30.10.2011 1:35:02 X = 129644121027235961
FN: Время создания 30.10.2011 1:35:02 C = 129644121027079711
FN: Время посл. модификации 30.10.2011 1:35:02 M = 129644121027079711
FN: Время последнего доступа 30.10.2011 1:35:02 A = 129644121027079711
FN: Время модификации записи 30.10.2011 1:35:02 X = 129644121027079711

Рис. 1. Внешние ВО файла 1.txt, извлеченные утилитой FTA

Внутренние ВО могут присутствовать в структуре файлов таких форматов, как документы, созданные с использованием программ пакетов Microsoft Office [1] (рис. 2), файлов формата PDF, цифровых фотоснимках [2] и некоторых других типах файлов.

Исследования показали, что ВО, выводимые на вкладке «Общие», с точностью до секунды воспроизводят ВО, хранящиеся в файловой записи, в то время как ВО, выводимые на вкладке «Подробно», несут информацию, отличную от ВО файловой записи («Создан»), либо вообще не представленную в ней («Напечатан») (рис. 2). Это как раз и есть внутренние ВО, сохраненные в структуре файла. Таким образом, в зависимости от формата рассматриваемого файла, он может содержать в своей структуре от одной до трех внутренних ВО.

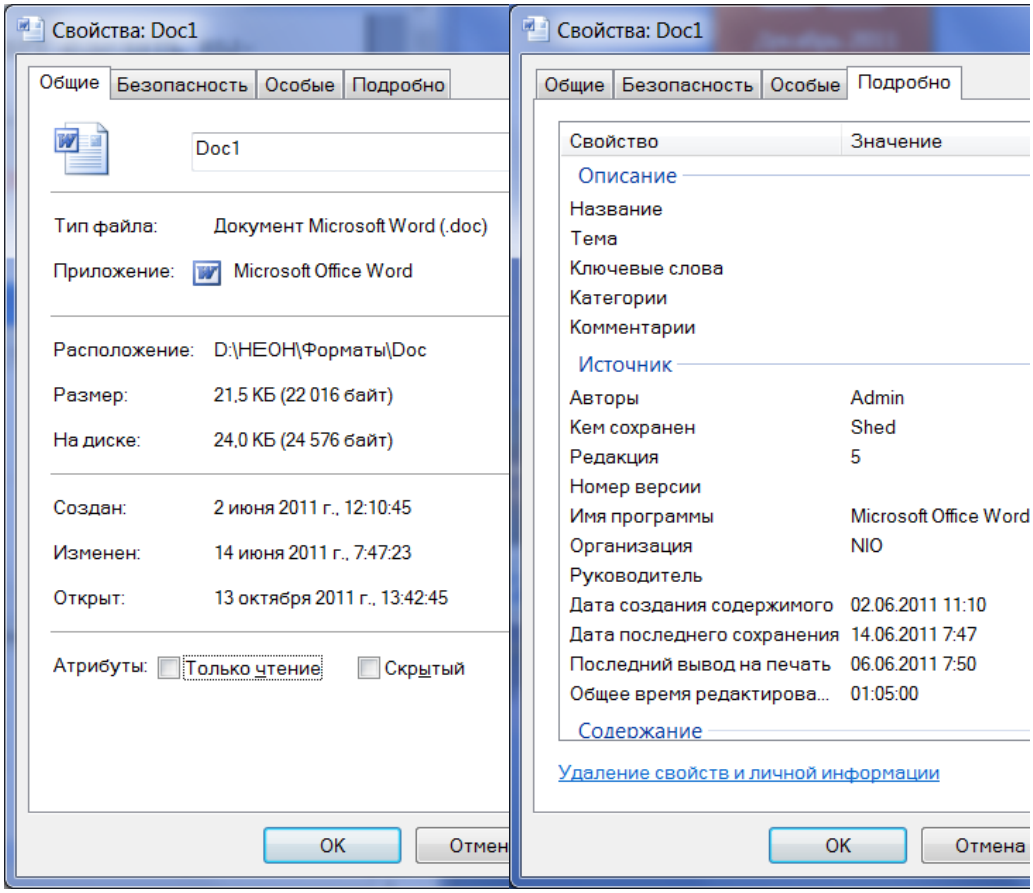

Рис. 2. ВО на вкладках «Общие» и «Подробно» окна «Свойства»

Естественно, подготовленные злоумышленники имеют представление о том, что внедренные ФО можно отследить по ВО. С целью воспрепятствования таким действиям кракерским сообществом разработан ряд методов и утилит, позволяющих фальсифицировать ВО.

Наиболее доступный способ фальсификации ВО файловых объектов заключается в изменении системного времени компьютера, либо использовании возможностей файловых менеджеров Total Commander или Far.

На данный момент существует несколько утилит, позволяющих осуществлять модификацию ВО. Одной из таких программ является утилита TimeStomp (James C. Foster, Vincent Liu). Аналогичной функциональностью обладает еще одна утилита с графическим интерфейсом FF File Time v1.1 от компании Fast Forward Projects.

Таким образом, злоумышленники имеют возможность манипулировать ВО ФО. Однако в виду того, что как файловые менеджеры, так и специализированные утилиты позволяют оперировать с ВО в формате hh:mm:ss, то модифицированные ВО имеют округление до количества секунд относительно формата FILETIME (семь нолей в младших разрядах). Файловый менеджер Far позволяет оперировать и с миллисекундами, поэтому округление ВО в результате модификации не такое значительное (четыре нуля в младших разрядах), но, тем не менее, позволяющее выявить вмешательство в атрибуты файлового объекта.

Наличие внутренних ВО позволяет уточнить ВО создания и модификации файлов, а для некоторых форматов файлов выяснить, выводился ли файл на печать.