Восстановление паролей. Часть 1

Безмалый Владимир

MVP Consumer Security

Microsoft Security Trusted Advisor

Практика показывает: чем масштабнее сеть и чем более ценная информация доверяется подключенным к ней компьютерам, тем больше находится желающих нарушить ее нормальное функционирование ради материальной выгоды или просто из праздного любопытства. Идет постоянная виртуальная война, в ходе которой организованности системных администраторов противостоит изобретательность компьютерных взломщиков.

Основным рубежом аутентификации сегодня является система парольной защиты, которая имеется во всех современных программных продуктах. В соответствии с установившейся практикой, перед началом сеанса работы с операционной системой пользователь обязан зарегистрироваться, сообщив ей свое имя и пароль. Имя требуется для идентификации пользователя, а пароль служит подтверждением правильности произведенной идентификации. Информация, введенная пользователем в диалоговом режиме, сравнивается с той, что имеется в распоряжении операционной системы. Если проверка дает положительный результат, то пользователю становятся доступны все ресурсы операционной системы, связанные с его учетной записью.

Вместе с тем хотелось бы подчеркнуть, несмотря на то, что о парольной защите и ее недостатках сказано много, все же на многих предприятиях именно пароль – основной механизм аутентификации. Именно от устойчивости вашего ключа зависит стойкость вашей криптографической защиты, да и во многих других случаях пароль остается пока, увы, универсальным механизмом безопасности. Хорошо это или плохо – не мне судить.

В данной статье мы поговорим об устойчивости паролей к взлому методами подбора по словарю и brute force (грубой силы, перебором).

Итак. К вам на исследование (расследование) попал чужой ПК, работавший под управлением ОС Windows. Вам нужно извлечь пароли данного пользователя. Как быть? (Надеюсь, читатели понимают, что проведение расследования – исключительная компетенция правоохранительных органов, поэтому в дальнейшем мы с вами будем использовать термин исследование).

Естественно, вначале вы сделали посекторную копию жесткого диска (чтобы не испортить что-то на оригинале, ведь это же доказательство) и приступили к исследованию.

Давайте вначале рассмотрим, а что же представляет собой ПО для восстановления (взлома) парольной защиты

Что такое парольный взломщик?

Наиболее эффективным является метод взлома парольной защиты операционной системы (в дальнейшем – ОС), при котором атаке подвергается системный файл, содержащий информацию о легальных пользователях и их паролях. Однако любая современная ОС надежно защищает

пользовательские пароли, которые хранятся в этом файле, при помощи хеширования[1]. Кроме того, доступ к таким файлам, как правило, по умолчанию запрещен даже для системных администраторов, не говоря уже о рядовых пользователях операционной системы. Тем не менее, в ряде случаев злоумышленнику удается путем различных ухищрений получить в свое распоряжение файл с именами пользователей и их зашифрованными паролями. И тогда ему на помощь приходят так называемые парольные взломщики - специализированные программы, которые служат для взлома паролей операционных систем.

Как работает парольный взломщик?

Криптографические алгоритмы, применяемые для хеширования паролей пользователей в современных ОС, являются слишком стойкими, чтобы можно было надеяться отыскать методы их обращения хеш-функции (т.н. поиск прообраза для хеш-функции), которые окажутся более эффективными, чем тривиальный перебор возможных вариантов. Поэтому парольные взломщики иногда просто хешируют все пароли с использованием того же самого криптографического алгоритма, который применяется для их засекречивания в атакуемой ОС.(Для Windows такие способы существуют — см. Rainbow Tables.

Радужная таблица (англ. Rainbow Table) – специальный вариант таблиц поиска, который использует механизм уменьшения времени поиска за счет увеличения занимаемой памяти (time-memory tradeoff). Используются для вскрытия паролей, преобразованных при помощи необратимой хеш-функции.

Радужная таблица создается построением цепочек возможных паролей. Каждая цепочка начинается со случайного возможного пароля, затем подвергается действию хеш-функции и функции редукции. Данная функция преобразует результат хеш-функции в некоторый возможный пароль. Промежуточные пароли в цепочке отбрасываются и в таблицу записывается только первый и последний элементы цепочек. Создание таблиц требует времени и памяти (вплоть до сотен гигабайт), но они позволяют очень быстро (по сравнению с обычными методами) восстановить исходный пароль.

Для восстановления пароля данное значение хеш-функции подвергается функции редукции и ищется в таблице. Если не было найдено совпадения, то снова применяется хеш-функция и функция редукции. Данная операция продолжается, пока не будет найдено совпадение. После нахождения совпадения, цепочка содержащая его, восстанавливается для нахождения отброшенного значения, которое и будет искомым паролем.

В итоге получается таблица, которая может с высокой вероятностью восстановить пароль за небольшое время.

Таблицы могут взламывать только ту хеш-функцию, для которой они создавались, то есть таблицы для MD5 могут взломать только хеш MD5. Теория данной технологии была разработана Philippe Oechslin как быстрый вариант time-memory tradeoff. Впервые технология использована в программе Ophcrack для взлома хешей LanMan, используемых в Microsoft Windows. Позже была разработана более совершенная программа RainbowCrack которая может работать с большим количеством хешей, например LanMan, MD5,SHA1 и др. [1].

---

[1] Хеширование (в криптографии) – необратимый процесс, т.е. имея хеш, вычисленный на основе некоторых данных, злоумышленник не может восстановить исходные данные никаким другим способом кроме атаки методом полного перебора.

Затем они сравнивают результаты хеширования с тем, что записано в системном файле, где находятся хеши паролей пользователей этой системы. При этом в качестве вариантов паролей парольные взломщики используют символьные последовательности, автоматически генерируемые из некоторого набора символов. Данный способ позволяет взломать все пароли, если известно их представление в хешированном виде, и они содержат только символы из данного набора.

За счет очень большого числа перебираемых комбинаций такие атаки парольной защиты ОС могут отнимать слишком много времени[2]. Однако хорошо известно, что большинство пользователей операционных систем особо не затрудняют себя выбором стойких паролей, то есть таких, которые трудно взломать. Поэтому для более эффективного подбора паролей взломщики обычно используют специальные словари, которые представляют собой заранее сформированный список слов, наиболее часто используемых на практике в качестве паролей. (Большой набор словарей можно найти на сайте http://passwords.ru) К каждому слову из словаря парольный взломщик применяет одно или несколько правил, в соответствии с которыми оно видоизменяется и порождает дополнительное множество опробуемых паролей, например:

1. производится попеременное изменение буквенного регистра, в котором набрано слово;
2. порядок следования букв в слове меняется на обратный;
3. в начало и в конец каждого слова приписывается цифра 1;
4. некоторые буквы изменяются на близкие по начертанию цифры.

В результате, например, из слова password получается pa55w0rd.

Это повышает вероятность нахождения пароля, поскольку в современных ОС, как правило, различаются пароли, набранные заглавными и строчными буквами, а пользователям этих систем настоятельно рекомендуется выбирать такие, в которых буквы чередуются с цифрами. Одни парольные взломщики поочередно проверяют каждое слово из специального словаря, применяя к нему определенный набор правил для генерации дополнительного множества опробуемых паролей. Другие предварительно обрабатывают весь словарь при помощи этих же правил, получая новый словарь большего размера, из которого затем черпают проверяемые пароли. Учитывая, что обычные словари естественных человеческих языков состоят всего из нескольких сотен тысяч слов, а скорость шифрования паролей достаточно высока, парольные взломщики, осуществляющие поиск по словарю, работают очень быстро.

Первый пароль, который вы хотите получить – пароль учетной записи пользователя. Для этого существует масса инструментов. Вы можете спросить, а зачем нам пароль пользователя? Ведь жесткий диск уже у нас, а, следовательно, мы имеем доступ ко всей хранящейся там информации. Безусловно. Однако не стоит забывать, что зачастую пользователи довольно беспечны, а следовательно, есть вероятность того, что данный пароль будет использован этим пользователем неоднократно, в том числе и к почте и к другим приложениям. Кроме того, стоит помнить, что пользователь мог применить EFS шифрование, а значит восстановить пароль пользователя гораздо эффективнее на первом шаге

Для этого вначале вспомним, где же хранятся наши искомые пароли.

---

[2] Сложность пароля =(количество символов в наборе)^(длина), т.е. пароль длиной 8 символов состоящий из больших и маленьких букв английского алфавита и цифр от 0 до 9 имеет сложность 62^8= 218340105584896 комбинации

Взлом операционных систем (на примере Windows XP/Vista/7)

База данных учетных записей пользователей

Одним из основных компонентов системы безопасности Windows XP/Vista/7 является диспетчер учетных записей пользователей. Он обеспечивает взаимодействие других компонентов системы безопасности, приложений и служб Windows XP/Vista/7 с базой данных учетных записей пользователей (Security Account Management Database, сокращенно SAM). Эта база обязательно имеется на каждом компьютере с Windows XP/Vista/7. В ней хранится вся информация, используемая для аутентификации пользователей Windows XP/Vista/7 при интерактивном входе в систему и при удаленном доступе к ней по компьютерной сети. База данных SAM представляет собой один из разделов (hive) системного реестра (registry) Windows XP/Vista/7. Этот раздел принадлежит ветви (subtree) HKEY_LOCAL_MACHINE и называется SAM. Он располагается в каталоге \winnt_root\System32\Config (winnt_root -условное обозначение каталога с системными файлами Windows XP/Vista/7) в отдельном файле, который тоже называется SAM. Основная часть информации в базе данных SAM хранится в двоичном виде. Доступ к ней обычно осуществляется с помощью диспетчера учетных записей. Изменять записи, хранящиеся в базе данных SAM, при помощи программ, которые напрямую редактируют реестр Windows NT/2000/XP(REGEDT или REGEDT32), не рекомендуется. По умолчанию этого и нельзя делать, т. к. доступ к базе данных SAM запрещен для всех без исключения категорий пользователей Windows XP/Vista/7.

Хранение паролей пользователей

Именно в учетных записях базы данных SAM находится информация о пользовательских именах и паролях, которая необходима для идентификации и аутентификации пользователей при их интерактивном входе в систему. Как и в любой другой современной многопользовательской ОС, эта информация хранится в зашифрованном виде. В базе данных SAM каждый пароль пользователя обычно бывает представлен в виде двух 16-байтовых последовательностей, полученных разными методами (LM и NTLM).

Возможные атаки на базу данных SAM

Обычно основным объектом атаки являются административные полномочия. Их можно получить, узнав в хешированном или символьном виде пароль администратора системы, который хранится в базе данных SAM. Поэтому именно на базу данных SAM бывает направлен главный удар взломщика парольной защиты.

По умолчанию в Windows доступ к файлу \winnt_root\System32\Config\SAM заблокирован для всех без исключения ее пользователей. Тем не менее, с помощью программы NTBACKUP любой обладатель права на резервное копирование файлов и каталогов Windows может перенести этот файл с жесткого диска на магнитную ленту. Резервную копию реестра можно также создать утилитой REGBAK из состава Windows NT Resource Kit. Кроме того, несомненный интерес для любого взломщика представляют резервная копия файла SAM (SAM.SAV) в каталоге \winnt_root\System32\Config и сжатая архивная копия SAM (файл SAM._) в каталоге \winnt_root\Repair.

Также указанный файл можно получить, загрузившись с внешнего носителя. В случае наличия загрузки двух операционных систем процесс копирования файла SAM существенно упрощается. При наличии физической копии файла SAM извлечь хранимую в нем информацию не представляет большого труда. Загрузив файл SAM в реестр любого другого компьютера с Windows (например, с помощью команды Load Hive программы REGEDT32), можно детально изучить учетные записи пользователей, чтобы определить их значения PID и шифрованные варианты хешированных паролей. Зная PID пользователя и имея зашифрованную версию его хешированного пароля, компьютерный

взломщик может попытаться расшифровать этот пароль, чтобы использовать его для получения сетевого доступа к другому компьютеру. Однако для интерактивного входа в систему одного лишь знания хешированного пароля недостаточно. Необходимо получить его символьное представление. Для восстановления пользовательских паролей ОС Windows в символьном виде существуют специальные парольные взломщики. Они выполняют как прямой подбор паролей, так и поиск по словарю, а также используют комбинированный метод взлома парольной защиты, когда в качестве словаря задействуется файл с заранее вычисленными хешированными паролями, соответствующими символьным последовательностям, которые часто применяются в качестве паролей пользователей операционных систем.

Для получения хешей паролей учетных записей, используемых на исследуемом ПК можно воспользоваться программой ElcomSoft System Recovery. При этом вы загрузитесь с предлагаемого CD-R и кроме всего прочего сможете получить хеши паролей. Сами пароли при этом вы сможете восстановить с помощью **Proactive System Password Recovery**.

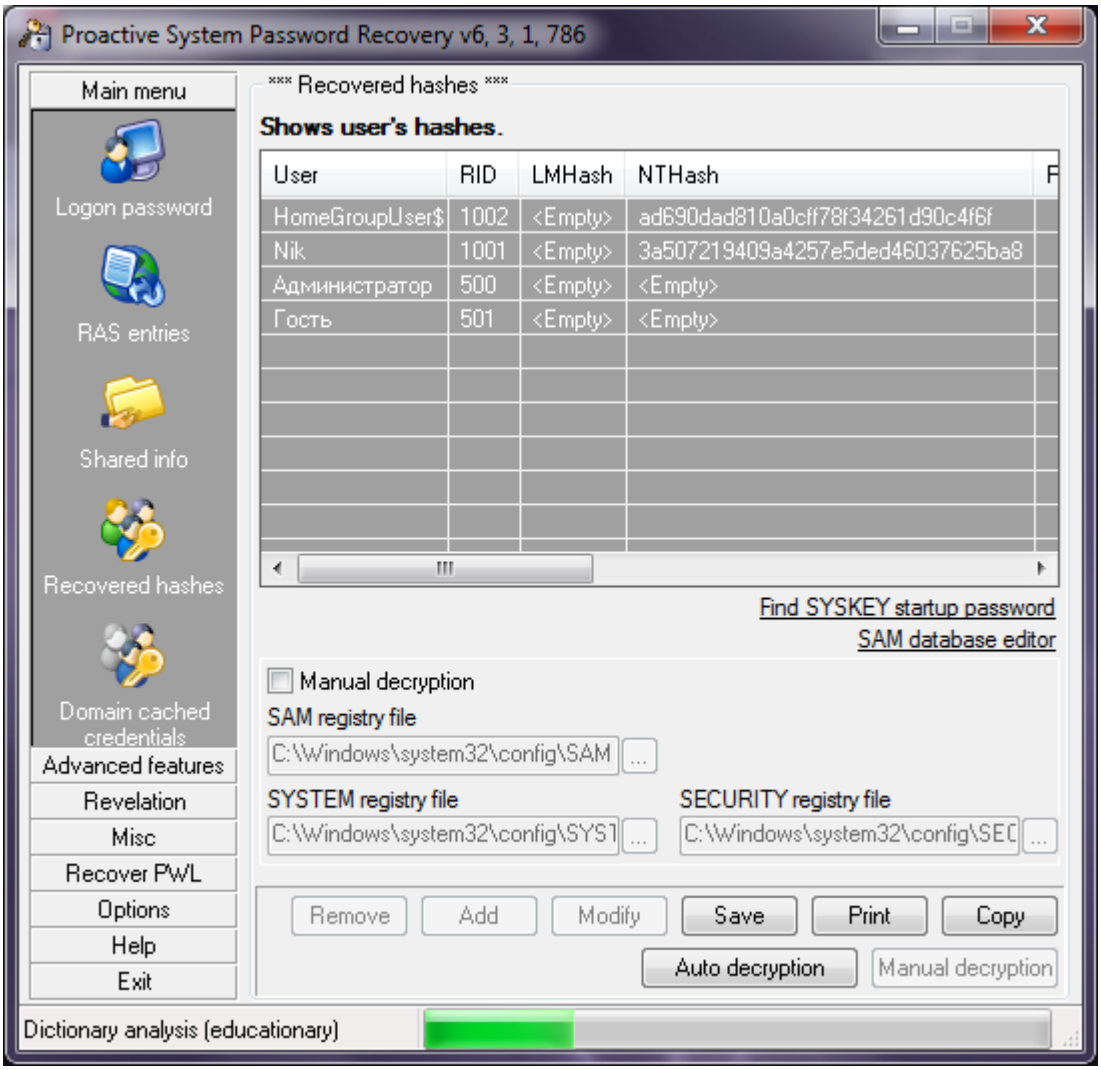

Рисунок 1 Proactive System Password Recovery

Хотелось бы сказать, что на самом деле данное ПО предоставляет гораздо больше возможностей, чем обычное восстановление пароля к учетной записи пользователя (как доменного, так и локального).

В частности:

1. мгновенному восстановлению подлежат следующие типы паролей:
   1.1. Пароли на вход Windows 95/98/ME (пользователь должен быть авторизован в системе)
   1.2. Пароли на вход Windows NT4/2000 (пользователь должен быть авторизован в системе с правами Администратора)
   1.3. Пароли на автоматический вход Windows 95/98/ME/NT4/2000/XP/2003
   1.4. Пароли .NET Passport
   1.5. Ключи шифрования и пароли для беспроводных сетей (WEP и WPA-PSK), хранимые с WZC
   1.6. Хранимые пароли пользователей Windows XP (множественные мандаты)
   1.7. Пароли на экранную заставку
   1.8. Пароли RAS и пароли доступа к Интернет-провайдерам (dial-up)
   1.9. Пароли на соединения VPN (Virtual Private Network)
   1.10. Пароли и права доступа к разделяемым (shared) ресурсам
   1.11. Пароли, скрытые под звездочкам
   1.12. Пароли, хранимые на диске сброса паролей
   1.13. Пароли к Remote Desktop Connections
2. Быстрому восстановлению
   2.1. Пароли к учётным записям пользователей Windows NT/2000/XP/2003/Vista/2008/Windows 7
   2.2. Пароли на этапе загрузки (SYSKEY)
   2.3. Пароли, сохранённые в Domain Cached Credentials
   2.4. Пароли WPA-PSK
   2.5. Пароли к удаленному помощнику Windows
   2.6. Пароли Windows 9x из файлов PWL

Кроме того, с помощью данного ПО вы можете проводить определенные манипуляции с пользовательскими настройками и файлами реестра:

- Запуск любой программы с привилегиями другого пользователя
- Отображение хешей предыдущих паролей
- Чтение и расшифровка хешей паролей непосредственно из файлов реестра (SAM и SYSTEM)
- Сохранение резервной копии файлов реестра и базы данных Active Directory с локального или удаленного компьютера
- Расшифровка скриптов Windows, защищенных при помощи Script Encoder
- Отображение списка пользователей, их групп и привилегий
- Расшифровка и просмотр защищенного хранилища (Windows Protected Storage), в котором хранятся пароли и строки для автоматического заполнения форм для Internet Explorer, Outlook и Outlook Express
- Просмотр записей ‘LSA Secrets’
- Отображение инсталляционных ключей к установленным продуктам Microsoft (Product ID и CD Key для установленных на компьютере экземпляров Windows и Microsoft Office)
- Полная поддержка Windows 7 (включая пароль HomeGroup, кэшированный logon-пароль и кэши предыдущих паролей, использовавшихся в системе)

- Извлечение сохранённых паролей из Apple Safari (и использование их в движке Intelligent Password Recovery)

Восстановление паролей к почте и веб-сайтам

В случае если пользователь для получения почты использовал браузер, нам потребуется ПО Elcomsoft Internet Password Breaker от компании Elcomsoft.

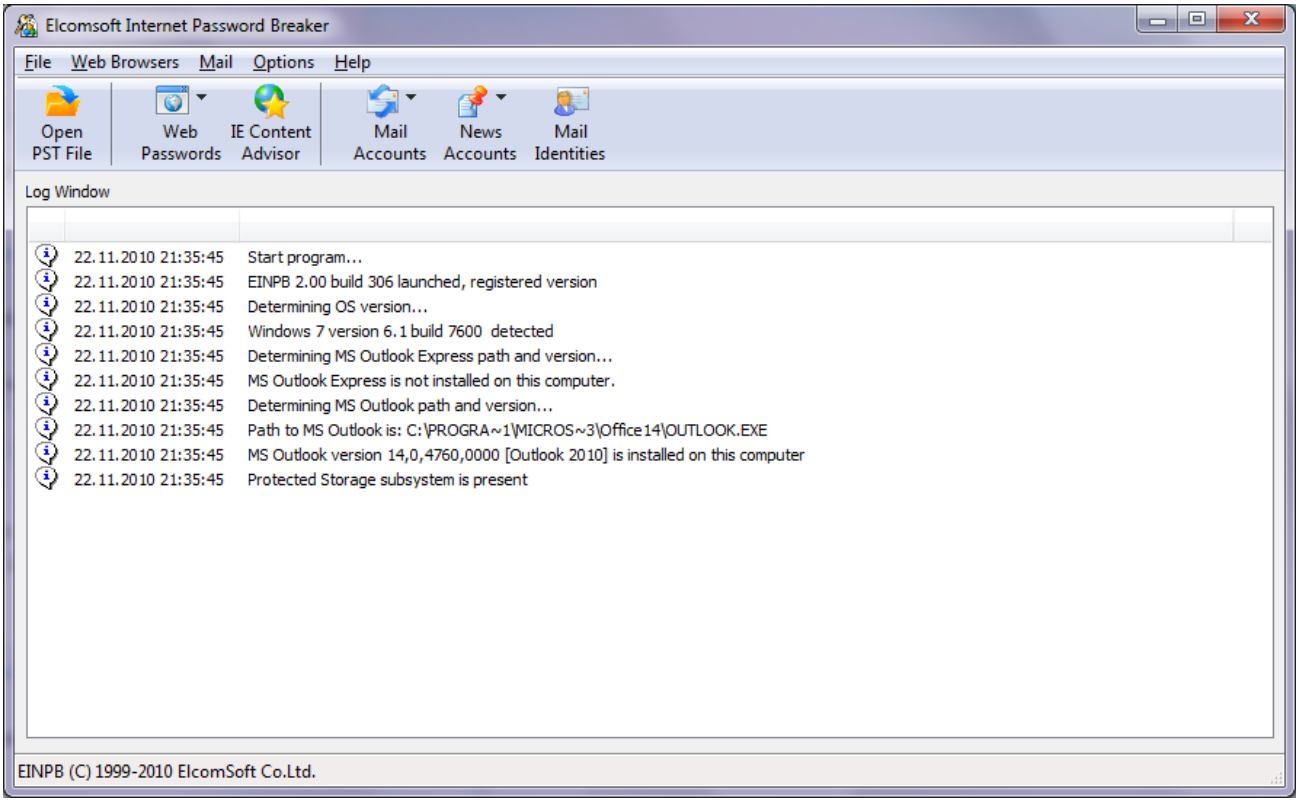

Рисунок 2 Elcomsoft Internet Password Breaker

С помощью данного ПО мы можем восстановить пароли, сохраненные для входа на различные веб-сайты или веб-почту.

Если допускается сохранение паролей, то пароль будет сохранен (зашифрован) в реестре Windows (для более старых версий Internet Explorer) или зашифрован в специальных файлах на жестком диске (для IE7 и IE8). Так что в следующий раз, когда вы будете обращаться к той же самой странице, ваш вход в систему будет произведен автоматически, но пароль будет скрыт под звездочками.

Для восстановления паролей достаточно выбрать – Web Passwords – IE Passwords. В появившейся итоговой таблице вы увидите адрес сайта, логин и пароль.

Кроме того, пароли можно увидеть, используя Web Passwords – IE AutoComplete. Если эта функция была включена в браузере, то вы также сможете увидеть имена пользователей и их пароли.

В случае если на ПК использовались сторонние браузеры такие как Opera, Firefox, Google Chrome, Safari, пароли оттуда также можно восстановить.

Обратите внимание, что если вам необходимо вернуть пароли, которые пользователь сохранил в Mozila Firefox, вы должны иметь установленным сам Firefox. Кроме того, эти пароли не должны быть

защищены с помощью мастер-пароля; если мастер-пароль установлен, вы должны вначале удалить его в параметрах настройки Firefox (или если мастер-пароль не известен, вы можете пробовать восстановить его с помощью Elcomsoft Distributed Password Recover http://www.elcomsoft.com/edpr.html).

Восстановление паролей к почте и новостям

Elcomsoft Internet Password Breaker отображает пароли почтовых ящиков, учетных записей POP3, IMAP, SMTP и NNTP. Поддерживаются все версии Microsoft Outlook, Outlook Express, Windows Mail и Windows Live Mail, включая пароли Microsoft Passport в Windows Live Mail. Для всех версий Microsoft Outlook, включая 2010, Elcomsoft Internet Password Breaker обнаруживает пароли к файлам PST.

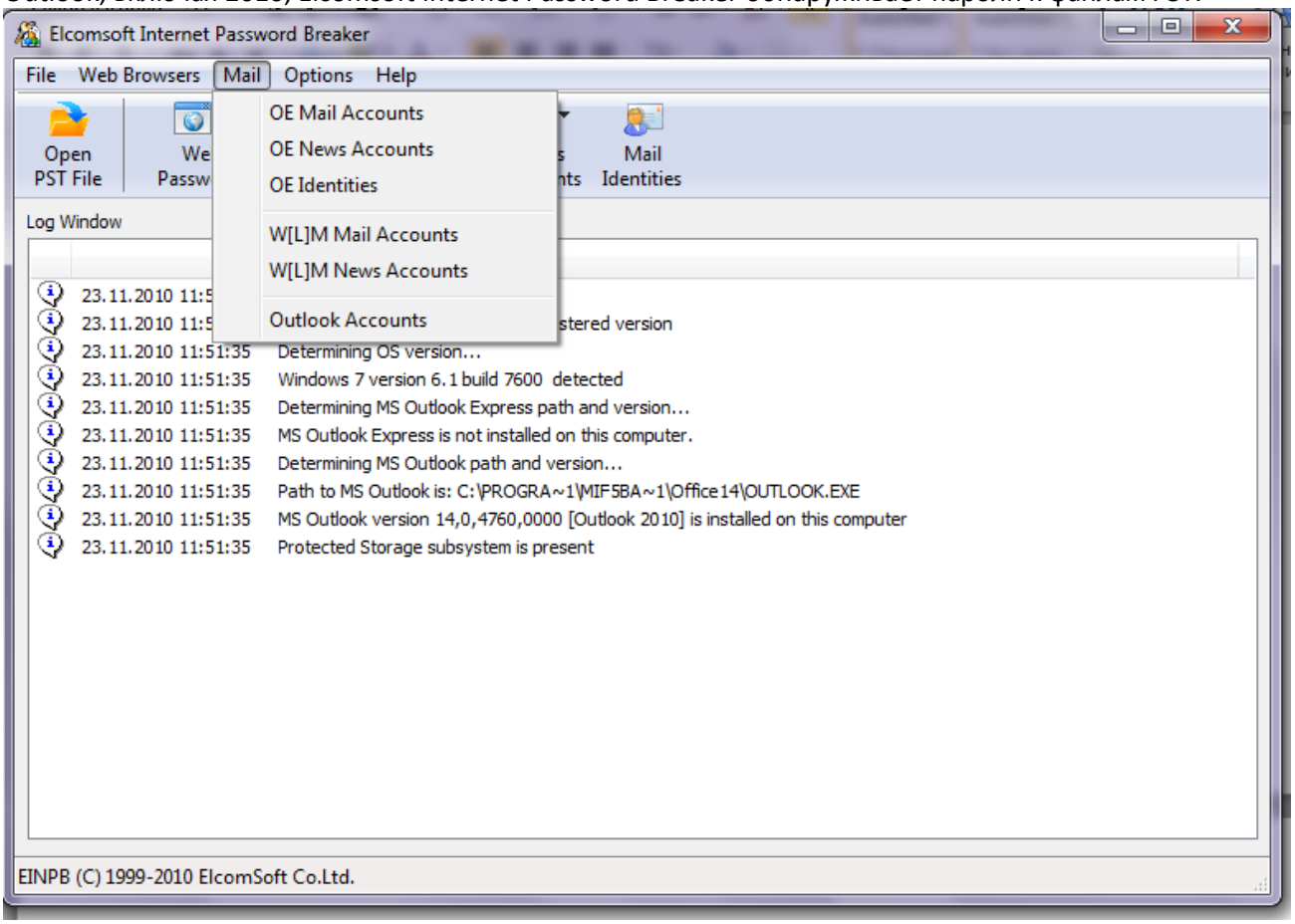

Рисунок 3 Восстановление паролей к почте

Восстановление паролей к документам MS Office

Следующей важной задачей может стать восстановление паролей к документам MS Office. В этом случае вам необходимо воспользоваться программным обеспечением **Advanced Office Password Recovery** (рис.4).

Атака на пароль осуществляется с помощью словаря, по маске, а также прямым перебором.

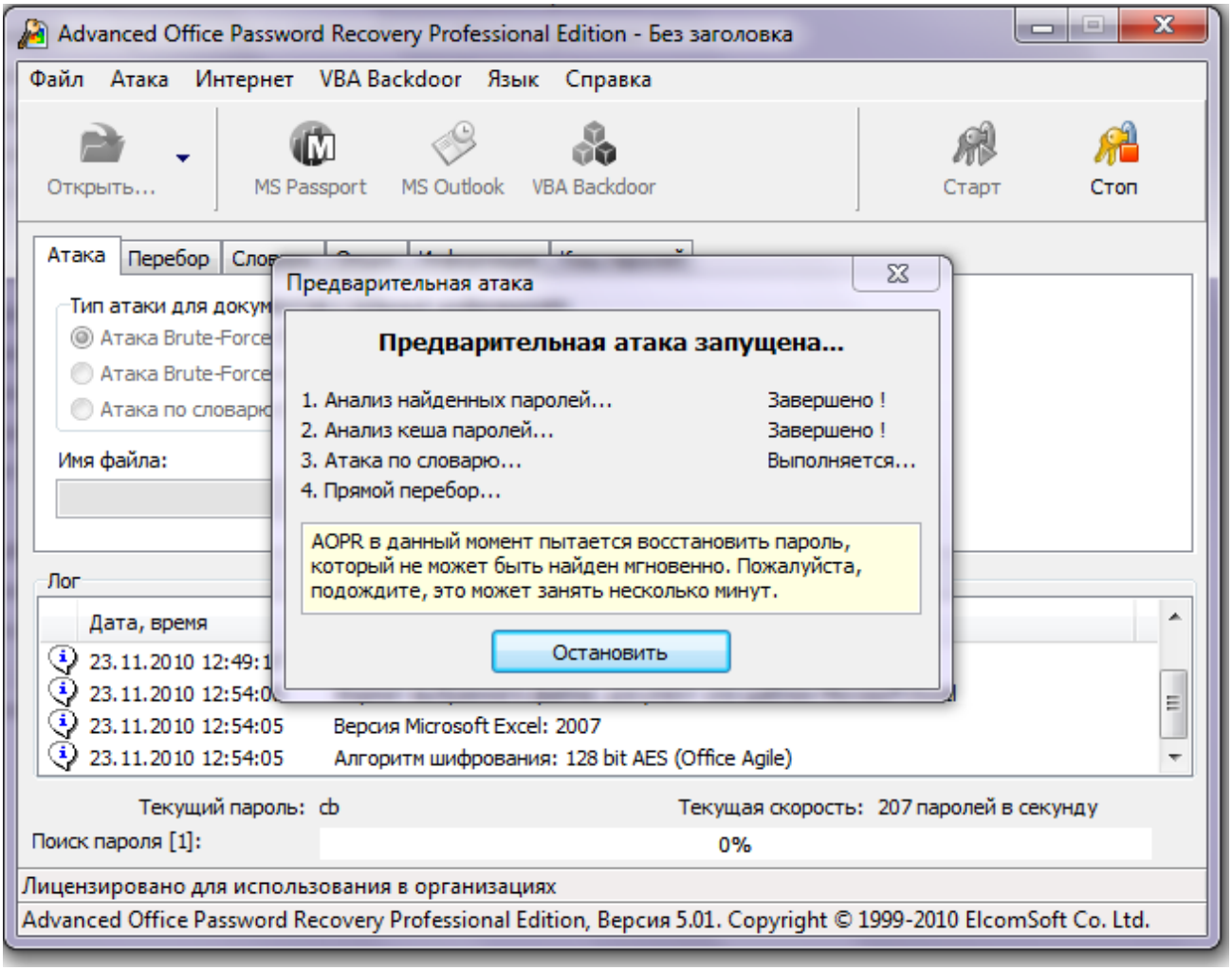

Рисунок 4 Атака прямым перебором

При попытке восстановления паролей на открытие документа Office 2007 и Office 2010 стоит учесть, что в данном случае для шифрования документов используется алгоритм AES с длиной ключа 128 бит, а также используется хеширование по алгоритму SHA-1 (пароли к Word, Excel, PowerPoint, Access). Только простые и короткие пароли могут быть обнаружены простым перебором. Кроме того, при восстановлении паролей Office 2010 процесс восстановления будет медленнее, чем при восстановлении паролей Office 2007. Для ускорения процесса восстановления паролей рекомендуется применять современные графические карты от NVIDIA и AMD/ATI. (рис.5).

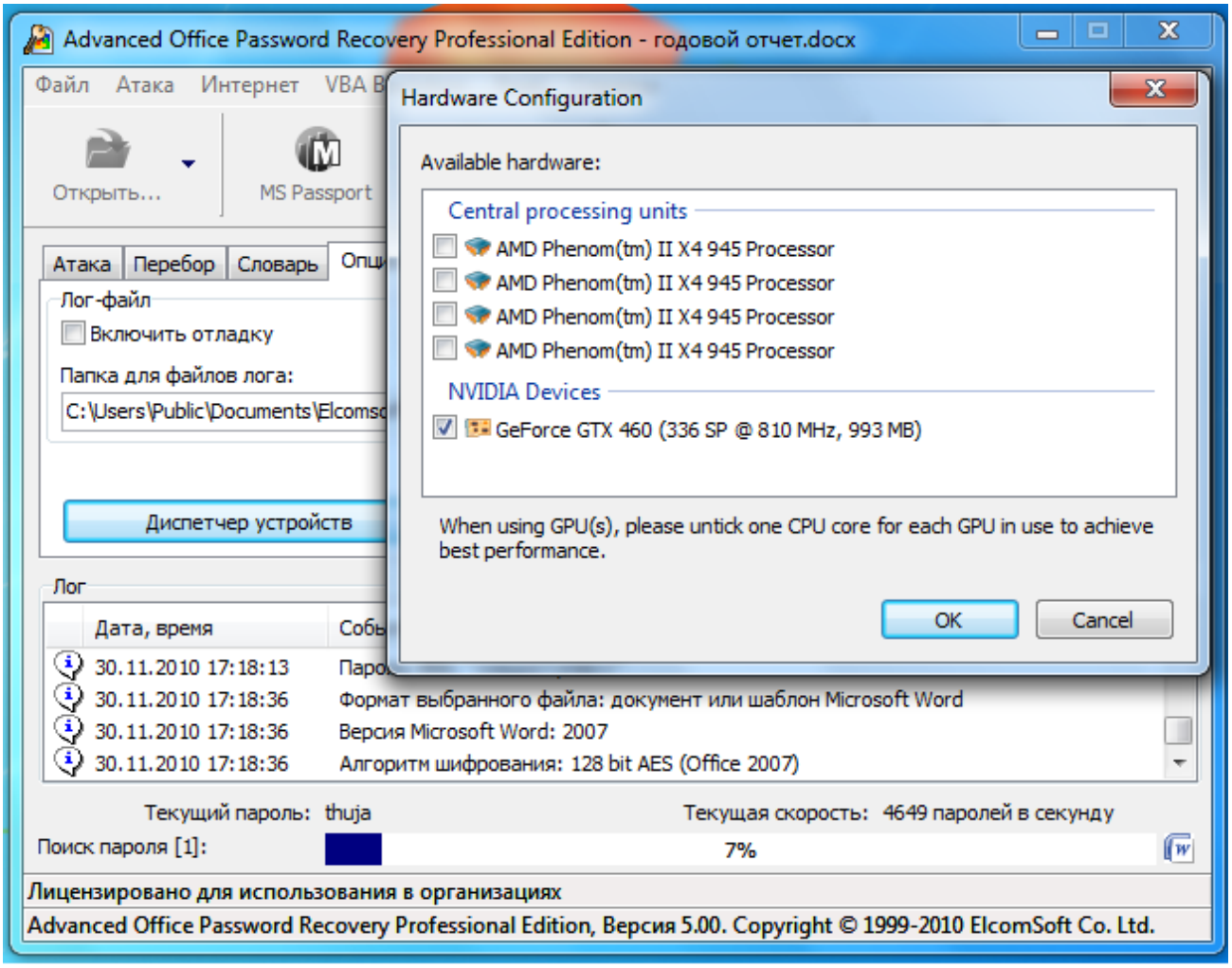

Рисунок 5 Восстановление пароля к документу Office 2007 с использованием видеокарты

Однако гораздо чаще нам нужен не сам пароль к тому или иному документу, а само содержимое документа. Для удаления пароля с документов Office предназначено программное обеспечение **Advanced Office Password Breaker**

Восстановление доступа к зашифрованным документам Microsoft Office

Удаление парольной защиты возможно с файлов, которые сохранены в формате .doc и .xls. Т.е. форматы файлов Word 2007-2010 и Excel 2007-2010 не поддерживаются!

Главное окно Advanced Office Password Breaker представлено на рис. 6.

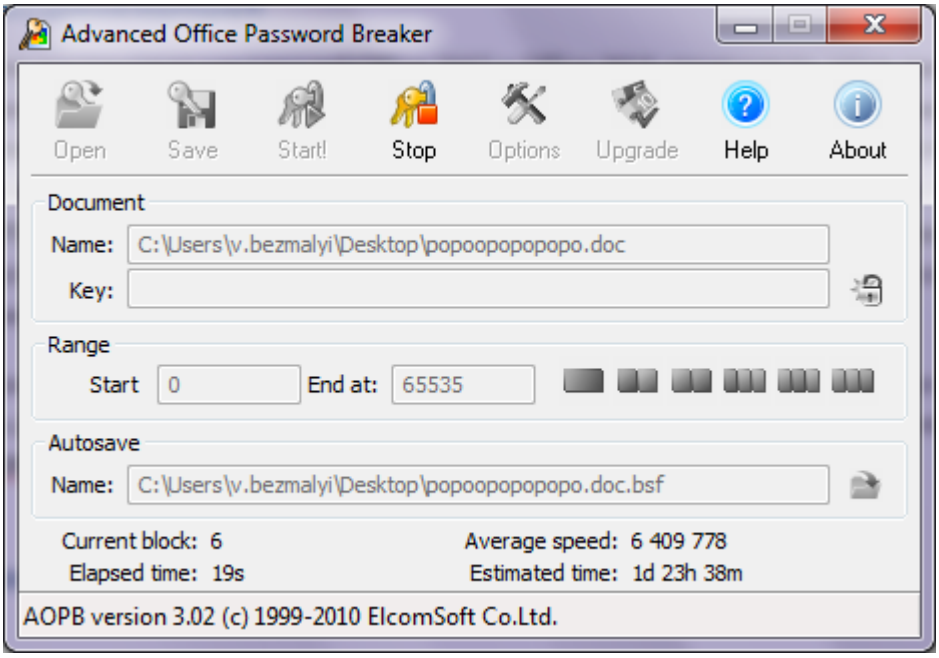

Рисунок 6 Удаление пароля документа Word 2000

Защита документов Microsoft Word и Microsoft Excel далеко не всегда позволяет быстро найти забытый пароль. Используя атаку по словарю, прямой перебор паролей и другие методы, восстановить пароль можно, однако этот процесс может занять огромное время. Вместе с тем, в случае если защита документа совместима с форматом Microsoft Office 97, существует решение, позволяющее гарантировано открыть документ в течение небольшого промежутка времени. Данный формат защиты уязвим, так как в нем используется ключ шифрования длиной всего 40 бит.

Перебор 40-битных ключей может быть произведен за заранее известный промежуток времени, зависящий от мощности процессора и количества ядер. Время нахождения ключа составляет около 5 дней для одноядерного процессора. В случае использования процессоров Core 2 Duo и Core 2 Quad время поиска ключа уменьшается пропорционально количеству ядер.

Advanced Office Password Breaker Professional поддерживает до 4 процессоров или ядер, позволяя ускорить процесс перебора ключей в 4 раза. Enterprise версия поддерживает до 32 процессоров.

Для ускорения процесса перебора ключей шифрования фирма Elcomsoft разработала технологию использования заранее вычисленных таблиц (Thunder Tables). Используя эти таблицы, вы можете найти ключ шифрования документу Word версий 97-2000 всего за несколько минут.

В случае если вам необходим пароль к Microsoft Excel 97-2000, используются классические радужные таблицы. Вероятность расшифровки документа за несколько минут составляет 97%.

Заключение

В одной статье невозможно рассмотреть все продукты и все случаи, когда нам потребуется восстановить пароли, поэтому о других возможных вариантах восстановления пароля мы поговорим в следующей части.

Литература

1. Радужные таблицы http://winprot.ru/publ/10-1-0-40