ELCOMSOFT
PROACTIVE SOFTWARE

ПРОФИ АКТИКА УЧШЕ ЕЧЕНИЯ

ТЕСТИРОВАНИЕ СТОЙКОСТИ ПАРОЛЕЙ – КЛЮЧЕВОЙ ЭЛЕМЕНТ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

ELCOMSOFT
PROACTIVE SOFTWARE

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время защите информации уделяется повышенное внимание. Многие уже осознали, что информация – это ценность, с которой не только нужно уметь обращаться, но уметь ее защищать.

Как известно, разумная профилактика угроз и минимизация рисков на порядок превосходит возможные последствия. Это правило применимо и к информационной безопасности любого предприятия.

Мизерные средства, потраченные сейчас на предупреждение угрозы, позволят в будущем сэкономить крупные суммы на устранение последствий, а то и вовсе обезопасить бизнес от краха вследствие утечки ключевой информации.

Известно, что общий уровень защиты корпоративной сети равняется уровню защиты самого слабого ее звена. Поэтому наличие на предприятии хотя бы одного слабого пароля значительно снижает уровень безопасности всего предприятия в целом.

В данной статье пойдет речь о том, какие риски связанны с использованием слабых паролей в корпоративной сети предприятия, а также как их можно минимизировать.

НЕ ВСЕ ПАРОЛИ ОДИНАКОВЫ

Парольная защита – это по-прежнему самый распространённый из-за своей простоты и удобства способ аутентификации, используемый в ОС Windows. Хотя существуют и другие способы, например, смарт-карты или биометрия, на большинстве рабочих станций для защиты продолжают использовать именно комбинацию логин-пароль.

Иногда на предприятиях к паролям предъявляется ряд формальных требований, объединяемых в так называемое «Password Policy» (политика управления паролями), которое является частью общей политики безопасности. Такая политика может определять, например, длину, состав и время жизни пользовательских паролей.
Но, как правило, в большинстве организаций нет четкой политики управления паролями, или же конечные пользователи ею пренебрегают. При этом сложность паролей может сильно отличаться.

Даже если администрация на предприятии под влиянием регламентирующих законодательных актов Sarbanes-Oxley (США), HIPAA (США), J-SOX (Япония), LSF (Франция) и других, ввели формальные требования к длине или составу пароля, то это еще не говорит о том, что используемые пользователями пароли на деле окажутся стойкими к взлому.

Обычно большая часть паролей состоит из слов и символов на родном или знакомом человеку языке. Эти слова часто имеют отношение к личной жизни пользователя: год рождения, имя любимой собаки, номер телефона или банковской карты и т.д. Знание этих фактов играет на руку злоумышленникам, для которых такие пароли становятся легкой добычей.

Необходимо сразу отметить, что при смене пароля ничего толком не меняется. Новый пароль чаще всего представляет собой незначительную модификацию старого или составлен по одному принципу (например, было John1, а стало Mary2). Именно таким образом большая часть пользователей решает для себя проблему регулярной смены пароля, предусмотренной политикой безопасности компании.

Кроме того, один раз взломав компьютер жертвы, опытный злоумышленник может стать ее «невидимым хозяином» очень надолго, используя шпионские программы, утилиты удаленного доступа и другие средства.

КАК МОЖНО ОБНАРУЖИТЬ СЛАБЫЙ ПАРОЛЬ?

В настоящее время основными методами для подбора паролей программными средствами являются:

1. Простой перебор.
2. Перебор по маске.
3. Атака по словарю.
4. Rainbow-атака.

Давайте рассмотрим эти методы подробнее, так как это важно для понимания термина «слабый пароль».

Простой перебор

Суть метода прямого перебора или «грубой силы» (brute force) проста: программа перебирает все возможные комбинации символов, пытаясь подобрать подходящий пароль. Поиск можно несколько ограничить, указав количество символов в пароле, их тип (буквы, цифры, другие знаки), а также, если задать символы, с которых должен начаться поиск.

Время подбора пароля методом «грубой силы» зависит от его предполагаемой длины, набора использованных в нем символов и мощности компьютера, используемого для взлома.

Конечно, может случиться так, что правильный пароль удастся найти быстро, и все возможные комбинации перебирать не придется. Но все же, при попытке подбора длинного пароля с использованием «brute force» атаки на обычном компьютере могут потребоваться годы. Продемонстрируем это.

Скорость перебора паролей Windows logon на современном компьютере составляет около 10 миллионов комбинаций в секунду. В случае LM-хэша, максимальная длина пароля может быль 7 символов (длина пароля ограничивается 14, и пароль разбивается на две половинки по 7), при этом не различаются большие и маленькие буквы. Если пароль состоит из 7 букв/цифр, то максимальное время перебора составит всего около 2 часов.

В случае NTLM-хэша для тех же 7 символов потребуется уже гораздо больше времени – около 4 дней, поскольку в пароле могут уже использоваться буквы нижнего регистра. Если пароль будет состоять уже из 8 символов на его «вскрытие» уйдет порядка 8 месяцев. Если же пароль ещё сложнее, в него включены ещё и знаки препинания, то на его подбор методом грубой силы потребуются годы.

Поэтому адекватной защитой от этого метода атаки служит в первую очередь длина используемого пароля.

Перебор по маске

В случае если о пароле удалось собрать какие-то данные, например, узнать его длину или часть символов, то есть шанс попробовать быстро взломать его по маске. При этом сильно сужается область поиска.

Например, зная, что пароль может начинаться с имени «иван» или заканчиваться годом рождения «1977», для поиска можно задать шаблоны «иван???» и «????1977». Неизвестные символы обозначены в шаблоне вопросительными знаками.
Смысл использования маски очевиден: программе приходится перебирать меньшее количество возможных комбинаций, а значит, срок, за который может быть найден пароль, значительно сокращается.

Чтобы надежнее защититься от этого метода взлома, необходимо избегать использования в пароле слов или сочетаний, которые могут легко быть получены из каких-либо других источников.

Атака по словарю

Можно другим методом – атакой по словарю. Дело в том, что часто пользователи используют в качестве пароля обычные слова. Как правило, это слова из английского языка или родного для пользователя: open, access, password и т.д. Ведь такой пароль запомнить значительно проще, чем бессмысленные комбинации букв и цифр. Готовые словари для такого вида атак можно легко найти в сети или составить самостоятельно. Во многих случаях может подойти небольшой словарик с наиболее популярными паролями – такими, как admin, 1234, abc123, password, 12/3/75, asdf, qwerty, aaaa и т.д.

В дополнение к этому, злоумышленник перед попыткой взлома может изучить персоналии пользователей. Здесь пригодится любая информация: имена, фамилии, даты рождения, клички домашних животных и т.д. Что-то может быть найдено из открытых источников, таких как блоги, а что-то под тем или иным предлогом от жертвы. Пригодится любая информация о пользователях, которая будет использоваться при составлении словаря.

Преимущество этого вида атаки очевидно – это скорость. Список слов, которые пользователи вводят в качестве пароля, весьма и весьма ограничен и его размер редко превышает сто тысяч. А перебрать сотню тысяч вариантов для современного компьютера – вполне посильная задача.

Для защиты от этого вида атаки необходимо избегать паролей, состоящих из простых слов или сочетаний, а также тех, которые могут легко быть получены при подробном изучении вашей личности.

Rainbow-атака

Для решения этой проблемы применяется так называемая rainbow-атака (rainbow attack), основная идея которой состоит в использовании предвычислений при поиске пароля: для поиска пароля используют результаты предварительных вычислений возможных его вариантов для некоторого набора символов.

Мысль о замене ресурсоемких вычислений обычным поиском по предварительно подготовленной таблице поиска (lookup table), не нова. Таблицы поиска применяются в тех случаях, когда данные гораздо проще извлекать из памяти, чем создавать. Основной сложностью при использовании таблиц поиска является их размер – не каждая компания располагает ресурсами для хранения терабайтов информации. Именно поэтому и появились радужные таблицы, представляющие собой оптимизированные таблицы поиска. Их размер на порядок меньше, чем обычных таблиц поиска.

Размер таблицы можно указать при ее генерации: чем больше размер, тем больше вероятность успеха при поиске пароля, и наоборот. Таким образом, за сравнительно небольшое время можно получить таблицы, по которым с очень высокой вероятностью можно в тысячи раз быстрее найти любой пароль из проверенного диапазона.

Справедливости ради стоит признать, что вероятность, как правило, составляет менее 100%, но результат того стоит. Например, при использовании таблицы для семи алфавитно-цифровых символов (на ее создание потребуется около недели), метод rainbow-атаки позволит восстановить практически любой пароль из семи алфавитно-цифровых символов за 20-30 секунд. А вот прямой перебор в этом случае займет уже более суток.

Вероятность восстановления пароля в результате rainbow-атаки ниже, чем при использовании обычных методов. Защититься от rainbow-атаки, можно только, пожалуй, используя более длинные пароли.

КАКИЕ ПАРОЛИ МОЖНО СЧИТАТЬ СЛАБЫМИ?

Учитывая возможные варианты атаки на существующую парольную защиту, можно сформулировать основные выводы о том, какие именно пароли можно считать слабыми.

Итак, слабыми паролями мы будем считать:

1. Все пароли, используемые в продуктах по умолчанию;
2. Популярные пароли (qwerty, 123, password, p@$$\/\/0rd, abc123, monkey и т.д.);
3. Комбинации из повторяющихся символов (aabbcc, 123123, aaaa т.д.);
4. Инверсия простых слов (drowssap, nimda и т.д.);
5. Пароли, совпадающие с именем пользователя, или представляющие его модификацию;
6. Короткие пароли длиной до 7 символов, которые можно достаточно быстро подобрать обычным перебором или по радужным таблицам;
7. Пароли, состоящие из простых слов или их комбинаций, быстро подбираемые атакой по словарю;
8. Пароли, основанные на персональных данных и характеристиках пользователя, модифицированные старые пароли, быстро подбираемые атакой по словарю и/или по маске;
9. Пароли, которые могут быть взломаны с помощью относительно распространённых rainbow-таблиц;
10. Пароли, сохранённые в различных системных файлах Windows, и кэшированные в памяти (сами по себе они могут быть и стойкими, но если неправильно настроены некоторые параметры системы, то пароли могут быть восстановлены практически мгновенно).

Как видно, очевидных критериев слабости парольной зашиты довольно много. На деле практически невозможно учесть их все в корпоративной политике управления паролями, если таковая вообще существует. Поэтому для обнаружения слабых паролей лучше на регулярной основе проводить их аудит.

СЛАБЫЕ ПАРОЛИ – РЕАЛЬНАЯ ОПАСНОСТЬ

КАКИЕ ПАРОЛИ МОЖНО СЧИТАТЬ СЛАБЫМИ?

Согласно исследованию известной консалтинговой компании Deloitte Touche[1], проводимый ими аудит информационной безопасности на крупных предприятиях показывает, что с проблемой использования слабых паролей сталкивались в течение последних 12 месяцев 14% компаний. В 9% случаев были использованы пароли по умолчанию, а еще в 7% случаев – простые, как правило, известные злоумышленникам пароли.

Суммируя данные этого исследования, можно говорить о том, что 30% всех предприятий ежегодно сталкиваются с проблемами использования слабых паролей. Из них 16% - это грубые пренебрежения элементарными правилами безопасности и культурой работы с паролями.

По данным исследования Брюса Шнайдера[2] 3.8% пользователей использую простые односложные пароли, легко подбираемые по словарю. Еще 12% также используют в составлении паролей простые слова, но с добавление одного специального символа в конце. 28% используют в паролях только буквы нижнего регистра и цифры, что значительно ускоряет их взлом простым перебором.

Приведенные цифры лишь демонстрируют существующие риски, связанные со слабой парольной защитой. Реальный масштаб угрозы для каждого конкретного случая может сильно разнится.

ВОЗМОЖНЫЕ УГРОЗЫ, СВЯЗАННЫЕ СО СЛАБЫМИ ПАРОЛЯМИ

Давайте рассмотрим возможные угрозы более подробно. Здесь можно выделить две большие категории угроз:

1. **Внешняя угроза**. Атака осуществляется извне, подбор пароля происходит вследствие прямой хакерской атаки.
2. **Внутренняя угроза**. Несанкционированный доступ к охраняемой информации вследствие подбора чужого пароля недобросовестным или специально внедренным на предприятие сотрудником.

В первом случае слабый пароль может стать всего лишь источником прямого взлома, начальной точкой взлома для злоумышленника. Ведь получив незаметно доступ к какому-либо ресурсу информационной инфраструктуры предприятия-жертвы, можно легко развить атаку дальше. Этому будет содействовать сама информация, к которой получен несанкционированный доступ, использование шпионских программ (например, кейлоггеров для записи вводимых легитимными пользователями реквизитов доступа и другой конфиденциальной информации) или методы социальной инженерии.

[1] «2007 Global Security Survey», Deloitte Touche,
[2] «MySpace Passwords Aren't So Dumb», Bruce Schneier, 2006

Необходимо понимать, что целью атаки уже давно не является развлечение или простое любопытство. Хакеров интересует доступ к ресурсам компании, представляющую реальную стоимость. Именно эти ресурсы и будут представлять собой конечную цель, начальной ступенькой к которой может служить один единственный слабый пароль.

Еще опаснее может обстоять дело, если внутри компании будет орудовать инсайдер. В его распоряжении могут изначально находится существенные вычислительные ресурсы. Они могут быть использованы для более «грубых» атак на защищенные паролем ресурсы. Инсайдеру доступны, пожалуй, все известные методы – атака простым перебором, по словарю, по маске или с использованием личной информации о пользователях (даты рождения, имена, фамилии и т.д.). При этом инсайдер в принципе не ограничен в физическом доступе к компьютеру, что позволит ему при желании сломать достаточно стойкую парольную защиту.

Потери от взлома, несанкционированного доступа к конфиденциальной информации и финансового мошенничества могут составлять огромные суммы, которые очень сильно зависит от размеров и отрасли бизнеса.

Для иллюстрации приведем еще некоторые цифры. По данным опроса представителей 370 американских компаний, проведенного авторитетным Американским Институтом Компьютерных Исследований[3] (Computer Security Institute), средние потери вследствие одного индента по нарушению безопасности составили $345 тысяч в 2007 году. По сравнению с предыдущим годом эта цифра увеличилась более чем вдвое.

Для некоторых отраслей бизнеса, например, финансовых или страховых организаций, решающую роль будут играть репутационные потери. Одного скандала, связанного с утечкой данных клиентов, часто уже достаточно, чтобы поставить компанию на грань банкротства.

Самое страшное, что в отличие от, например, вирусных атак взлом парольной защиты может быть не обнаружен вовсе, при этом злоумышленник и стоящие за ним заказчики из числа конкурентов могут долгое время иметь доступ к конфиденциальным данным предприятия, стратегической или финансовой информации. В лучшем случае, взлом и утечка будут обнаружены уже по факту использования, когда предотвратить угрозу уже невозможно.

Регламенты по смене паролей, часто действующие на крупных предприятиях, будут в большинстве случаев бесполезны перед опытными хакерами, которые при вводе нового пароля тут же получат его от заблаговременно внедренного кейлоггера.

Для того чтобы минимизировать риски, связанные со слабыми паролями, необходимо на регулярной основе проводить аудит используемых на предприятии паролей. Как это сделать, мы расскажем в следующей главе.

[3] «Computer Crime and Security Survey», Computer Security Institute (CSI), 2007

ОБНАРУЖЕНИЕ СЛАБЫХ ПАРОЛЕЙ

Как уже было отмечено выше, одной только корпоративной политики безопасности, регулирующей длину и состав пароля недостаточно! Это не спасает от быстрого подбора пароля при помощи словаря или по определенному шаблону (например, при составлении сложного пароля чаще всего вначале обычно идут буквы, затем цифры и/или последним один из символов в верхнем регистре).

Более того, при регулярной смене паролей по расписанию, предусмотренной политикой безопасности в крупных организациях, пользователей как будто вынуждают упрощать пароли, используя постоянные конструкции и незначительные модификации предыдущих паролей.

Минимизировать все описанные выше риски можно. Для этого всего лишь нужно на регулярной основе проводить превентивный аудит используемых в корпоративной сети паролей.

Как это сделать? Очень просто. Для этого нужно поставить себя на место злоумышленника и попытаться выполнить его работу, т.е. подобрать пороли к учетным записям пользователей.

Для этой цели существуют специальные программные средства, которые широко используются отделами безопасности крупных компаний, а также специальными службами в различных странах мира.

Запуская по расписанию специальные программы по аудиту паролей, можно достаточно быстро выявлять слабые точки в парольной защите предприятия и устранять их. Кроме этого, это позволит выявить недисциплинированных или неграмотных с точки зрения безопасности сотрудников, нуждающихся в разъяснении важности стойкой парольной защиты.

КАКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЛУЧШЕ ВЫБРАТЬ?

Решать задачу аудита используемых в сети предприятия паролей можно разными программными средствами, которых сейчас существует достаточно много, начиная от самописных и бесплатных решений и заканчивая специально предназначенными для этой цели коммерческими решениями. При их выборе необходимо руководствоваться в первую очередь их функциональными возможностями, а также удобством работы.

Из функционала в первую очередь важны возможности по моделированию различных видов атак, которые мы подробно обсуждали выше, а также поддержка удаленной работы по сети, различных языков и платформ.

Одним из наиболее удобных и функциональных решений на рынке является программа Proactive Password Auditor компании «ЭлкомСофт», что будет наглядно продемонстрировано дальше.

АУДИТ ПАРОЛЕЙ ПРИ ПОМОЩИ PROACTIVE PASSWORD AUDITOR

Продукт Proactive Password Auditor (PPA) позволяет быстро и эффективно решить задачу аудита используемых в сети паролей. PPA поддерживает различные методы подбора паролей: атака по словарю, brute-force и rainbow-атака.

Он представляет собой специальное средство для тестирования качества парольной защиты в операционных системах Windows NT, Windows 2000, Windows XP, Windows 2003 Server, Windows Vista и новейшем Windows Server 2008, что позволяет использовать ее на любом парке рабочих станций.

Proactive Password Auditor предназначен для корпоративного использования и позволяет системным администраторам находить учётные записи пользователей, имеющие нестойкие пароли.

Вследствие природы хеширования невозможно восстановить оригинал пароля из его хеша (будь то LM или NTLM). Однако возможно найти пароль, используя атаку brute-force или по словарю, пробуя все возможные варианты паролей в заданном диапазоне или по списку слов соответственно. Таким образом, для нахождения пароля необходимо:

- собрать хеши паролей;
- найти пароли, соответствующие найденным хешам.

Для получения хешей паролей в PPA могут использоваться несколько способов:

- чтение памяти локального компьютера;
- чтение памяти удаленных машин (поддерживаются компьютеры с Active Directory);
- чтение реестра локального компьютера;
- использование готовых дамп-файлов полученных утилитами pwdump, pwdump2 и pwdump3;
- дамп хешей при помощи программы Elcomsoft System Recovery.

Proactive Password Auditor позволяет произвести аудит паролей в максимально сжатые сроки, используя уникальные алгоритмы оптимизации скорости перебора.

Необходимо отметить, что по результатам работы PPA недостаточно только поменять слабые пароли. Что если новые пароли тоже окажутся слабыми? Главное – сделать выводы о том, насколько правильная в компании политика управления парольной защитой. Если при регулярной проверке PPA взламывается слишком много паролей, то политику, очевидно, надо улучшать.

В дополнение к своему прямому назначению, в случае служебной необходимости (для восстановления доступа к зашифрованным данным EFS, сохраненных паролей интернет и т.д.) с помощью PPA системный администратор может найти пароль любого пользователя, используя прямой перебор, атаку по словарю или rainbow-атаку.

Скачать пробную версию Proactive Password Auditor можно здесь.

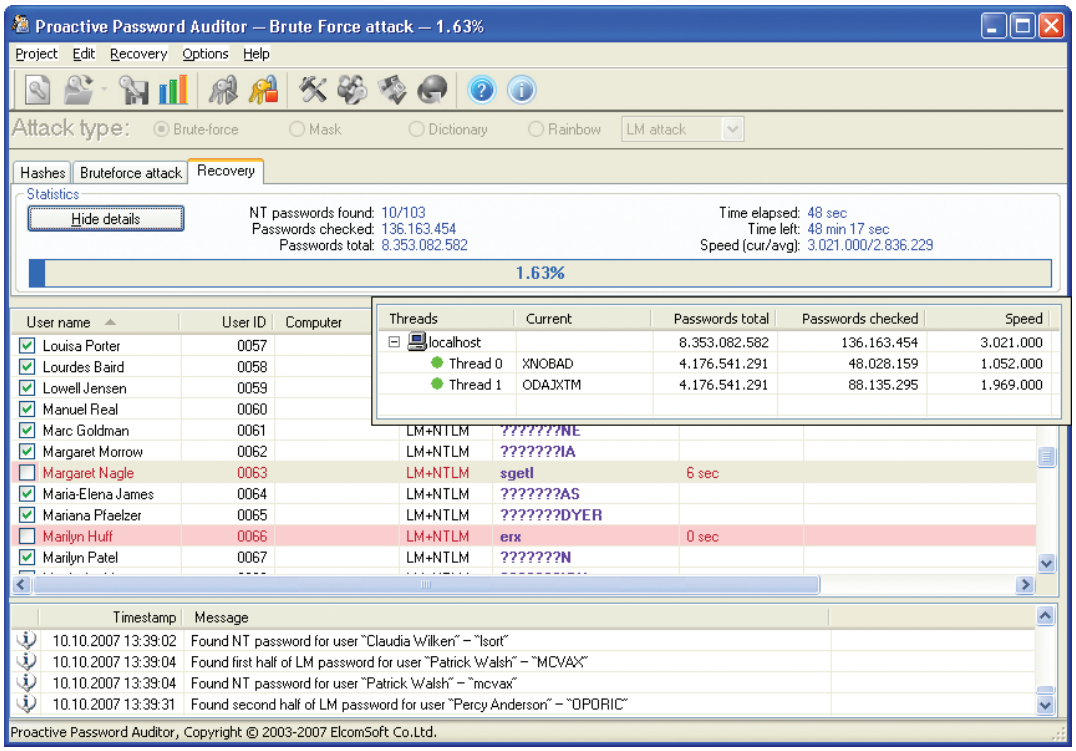

Рис.1. Работа Proactive Password Auditor по аудиту паролей пользователей.

ELCOMSOFT
PROACTIVE SOFTWARE

О КОМПАНИИ «ЭЛКОМСОФТ»

Основанная в 1990 году, российская компания «ЭлкомСофт» является одним из лидеров рынка программного обеспечения для восстановления доступа к системам, приложениям и документам. Благодаря уникальным технологиям, продукты компании получили широкое признание как в России, так и за рубежом.

В число клиентов «ЭлкомСофт» входят многие известные в мире из следующих отраслей:

High Tech: Microsoft, Adobe, IBM, Cisco
Governmental: FBI, CIA, US Army, US Navy, Department of Defence
Consulting: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finance: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telecommunications: France Telecom, BT, AT&T
Insurance: Allianz, Mitsui Sumitomo
Retail: Wal-Mart, Best Buy, Woolworth
Media&Entertainment: Sony Entertainment
Manufacturing: Volkswagen, Siemens, Boeing
Energy: Lukoil, Statoil
Pharmaceuticals: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

Компания имеет статусы Microsoft Gold Certified Partner, Intel Software Partner, а также является членом Российской криптографической ассоциации, Computer Security Institute (CSI), Association of Shareware Professionals (ASP).

Компания «ЭлкомСофт» является признанным экспертом на рынке, на ее технологические разработки ссылаются во многих известных книгах, например, «Microsoft Encyclopedia of Security», «The art of deception» (Kevin Mitnick), «IT Auditing: Using Controls to Protect Information Assets» (Chris Davis), «Hacking exposed» (Stuart McClure).

Чтобы узнать больше, посетите сайт компании.

АДРЕС:
ООО «ЭлкомСофт»
Звездный б-р, 21, офис 541
129085 Москва

ФАКСЫ:
US (toll-free): +1 (866) 448-2703
United Kingdom: +44 (870) 831-2983
Germany: +49 18054820050734

ВЕБ-САЙТЫ:
http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr