безопасный wëb-серфинг
(дополнения и врезки)

>>> врезка атас! нас поимели!

…после секса без презерватива, в смысле блуждания по сети с IE (а ведь мыщъх же предупреждал!) душу начинают терзать смутные сомнения — а не подцепили ли мы чего?! тут же устанавливаются самые свежие версии антивирусов, которые, естественно, ничего не находят, от чего подозрения только усиливаются, распространяя устойчивый запах паранойи. нам кажется, что компьютер ведет себя как-то не так и любой сбой трактуется как "ну все, конец, это вирус", хотя конец находится совсем в другом кармане.

Достаточно простым, но эффективным тестом на внедрение заразы был и остается поиск по вновь созданным файлам. 99,9% троянских и шпионских компонент не утруждают себя модификацией даты создания файла (не путать с так называемой "MS-DOS" датой), а потому и палятся еще на излете.

Как можно быстрее после посещения "подозрительных" уголков сети, нажимам на "пуск", где видим "найти → файлы и папки". Ищем файлы, созданные за последний день на диске C: (ну или, для надежности, можно охватить и другие диски). Там будем много всего, но нас в первую очередь интересуют исполняемые файлы, динамические библиотеки и прочие программные компоненты, расположенные в Program Files и каталоге Windows.

Вот например:

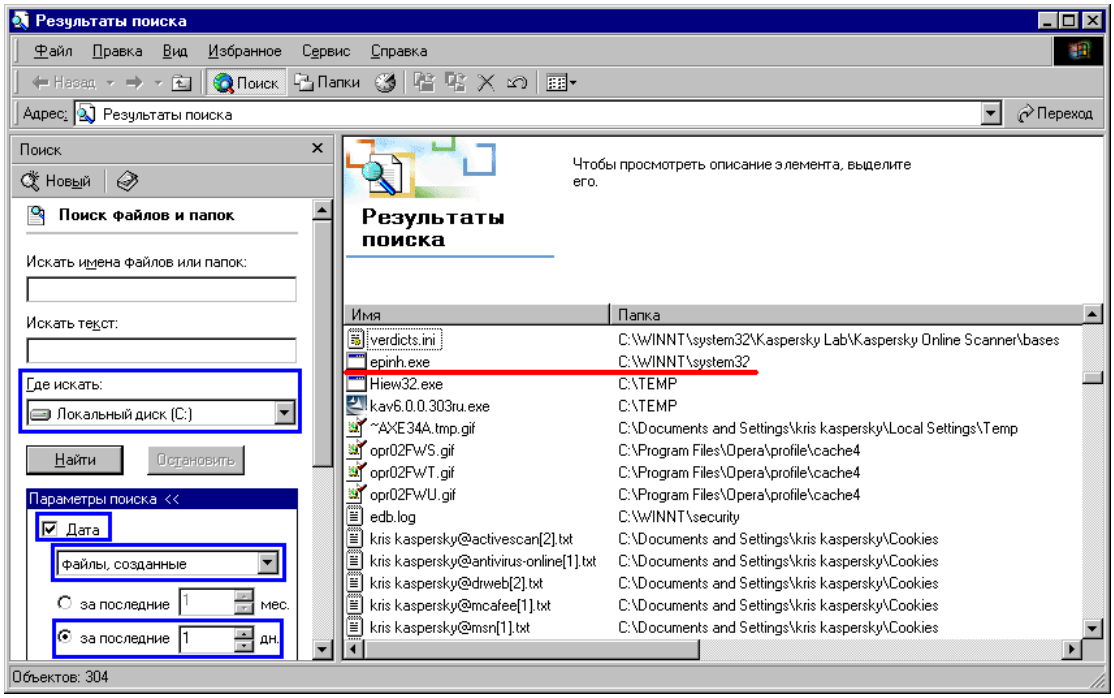

Рисунок 1 поиск внедренной заразы

В глаза сразу же бросается epinh.exe, расположенный в C:\WINNT\System32, который мы туда не клали. За hiew32.exe и ka6.0.0.303ru.exe в TEMP'e можно не опасаться — это мы сами только что их скачали. Остальные файлы представляют собой файлы данных (кучи, содержимое кэша браузера, логи безопасности) и к вредоносным компонентам никакого отношения не имеют.

А вот epinh.exe нас все-таки поимел. Что делать?! Если есть опыт — дизассемблировать самим, если нет — отсылать в Лабораторию Касперского. По моим наблюдениям она реагирует на поступление новой заразы оперативнее других.

>>> врезка двойной презерватив — двойная защита!

Для достижения наивысшей безопасности (в плане атаки) следует установить виртуальную машину типа VM Ware, настроить виртуальную сеть (благо она это позволяет) и выходить в сеть только через нее. Тут можно поступить двояко — либо дать VM Ware физический доступ к сетевой карте, USB/COM модему или установить на основной операционной системе proxy-сервер, через который виртуальная машина будет общаться с внешним миром.

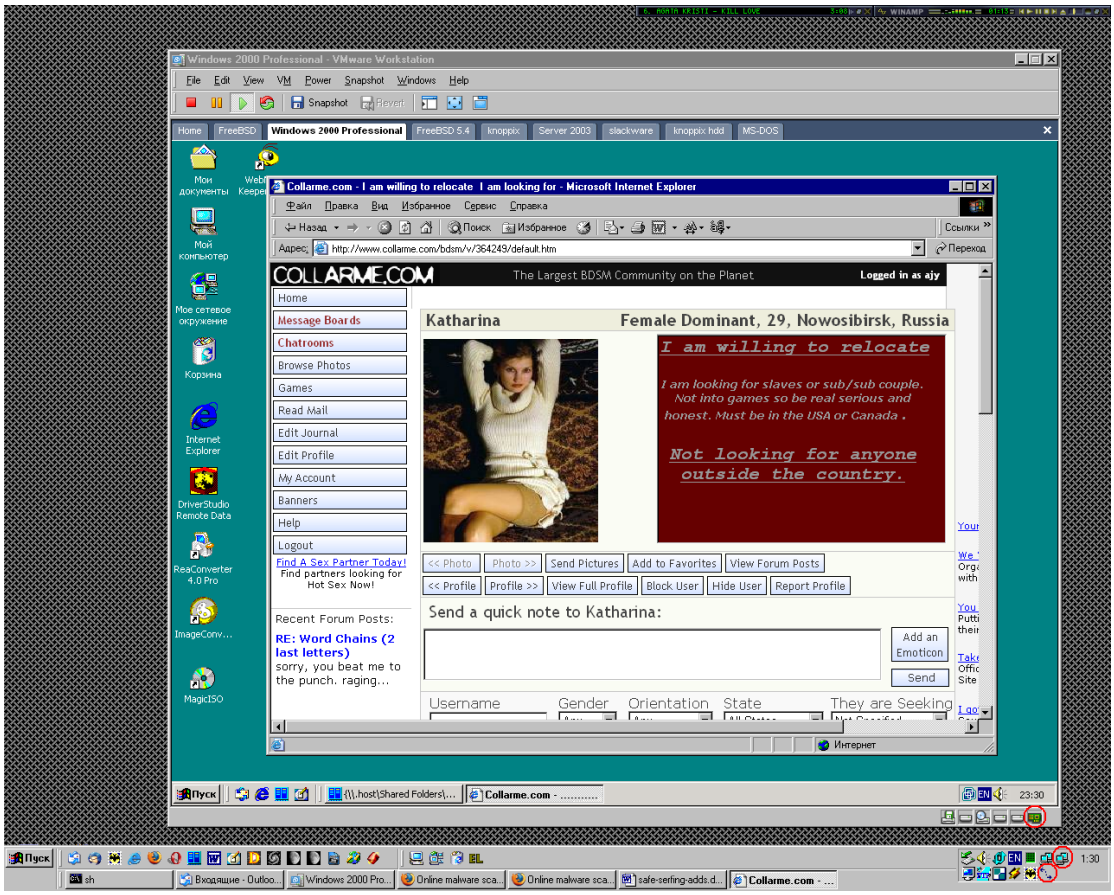

Рисунок 2 виртуальная машина сделает блуждание по сети чуть более медленным, но зато _абсолютно_ безопасным, поскольку вырваться из ее "застенок" никакому троянскому коню не под силу

Proxy серверов, изначально заточенных под домашних пользователей очень много. Лично мыщъх предпочитает быстрый, компактный и нетребовательный к ресурсам Etlin HTTP Proxy: http://www.eternallines.com/httpproxy. Вообще-то он не совсем бесплатен и по истечении испытательного срока требует регистрации, но нашего пользователя это обстоятельство еще никогда не останавливало!

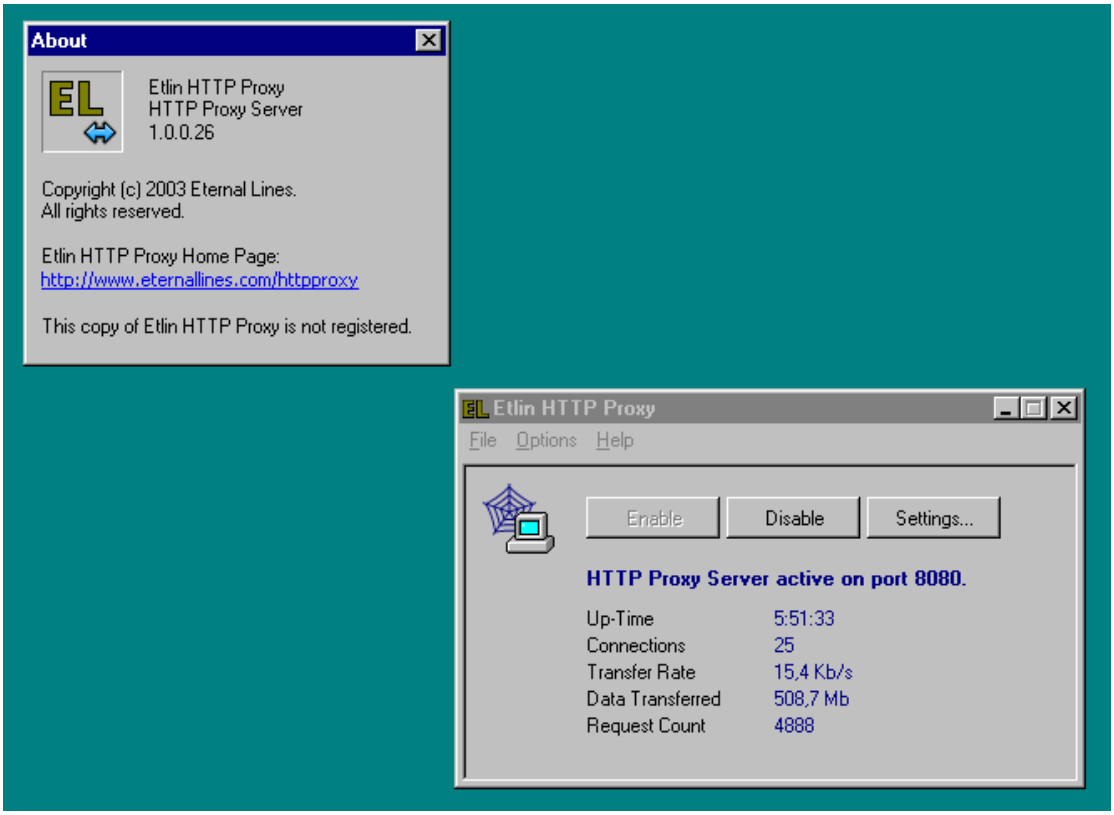

Рисунок 3 внешний вид Etlin HTTP Proxy сервера

По соображениям сохранения полной конфиденциальности, виртуальные машины лучше всего создавать на съемных носителях (типа картах FLASH-памяти) или зашифрованных дисках (типа PHP-Disk), тогда на основном жестком диске никаких следов нашего пребывания на порнографических серверах не останется (естественно, это справедливо только в том случае, если VM Ware имеет прямой доступ к сетевой карте или модему, а при работе через Proxy он может откладывать в логах все, что угодно).

>>> врезка раскопки жесткого диска

При работе с конфиденциальными (или порочащими репутацию) данными важно удостовериться, что они физически отсутствуют на жестком диске и никакая утилита восстановления не в состоянии "откопать" их.

Берем любой дисковый редактор (например, Microsoft Disk Probe, входящий в состав бесплатно распространяемого набора Support Tools, обычного присутствующего на лицензионном диске с Windows), открываем все физические диски один за другим (при этом, естественно, мы должны обладать правами администратора!) и ищем "сакраментальные" фразы (например, адреса серверов, факт посещения которых мы хотели бы скрыть). Поиск необходимо с игнорированием регистра как в ASCII, так и в Unicode кодировках, поскольку никогда заранее неизвестно в каком формате их записывает та или иная программа.

Чем больше следов будет обнаружено, тем сильнее повод задуматься о собственной (не)безопасности и приступить к активному внедрению защитных мер, описанных в этой статье.

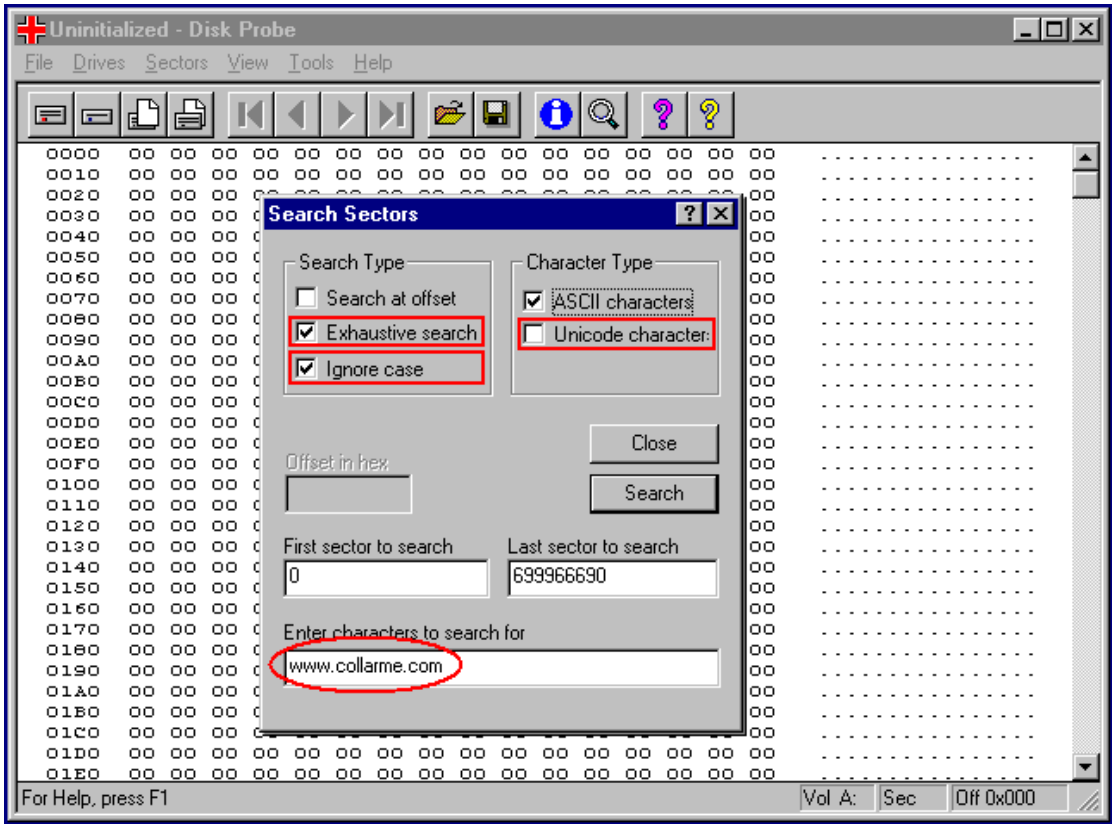

Рисунок 4 поиск следов нашего пребывания на www.collarme.com в DiskProbe

>>> врезка как избежать ложной компрометации

Хорошо, допустим мы как законопослушные граждане никуда не ходим, жене не изменяем, а если даже и изменяем, то делаем это с умом, как вдруг… некий неизвестный "доброжелатель" звонит начальству и сообщает, что мы смотрим детскую порнографию за казанный счет. Начальник вызывает администратора, администратор смотрит в кэш нашего браузера и точно! обнаруживает в нем кучу компромата. Такое часто случается… обиженный коллега перебросил свой собственный кэш по локальной сети (или через DVD/CR-RW при наличии физического доступа к компьютеру).

Как отличить настоящий кэш от его грубой подделки?! Да очень просто — по датам создания! При естественном наполнении кэша все файлы имеют различные даты, а при "варварском копировании" — одну. И хотя несложно написать программу, копирующую файлы с сохранением всех атрибутов (дата создания, дата последнего обращения и дата последней модификации) рядовые обиженные сотрудники на это не способны. Но все-таки. Чтобы обезопасить себя от вандалов, никогда не используйте IE, а выберете какой-нибудь экзотический бразуер, которого ни у кого нет и тогда все обвинения разлетаться в пух и прах!!! А… быть может, и нет...