TRANSLATED VERSION BELOW

Тех задание для Ифрейм системы [redacted]
Task for IFRAME system (further details redacted)

Итак для начала я опишу как должен работать основной софт, который будет обрабатывать компьютер юзера.
OK, to begin let me describe how should work the main module which will be dealing with user's computer.

Что нам нужно на данный момент ?
What do we want at given moment?

А нужно нам заразить юзера, который зайдет к нам на сайт с наибольшей эффективностью.
Well, we need to infect user's computer that visits our web site with maximum efficiency.

И сделать это как можно быстрее.
And this must be done as fast as possible.

Для начала нам понадобится маленький лоадер (это такая программка, которая весит чуть больше 2кб. пишется по моему на ACM-е если не ошибаюсь)
To begin we would need a very compact loader program (small application, no larger than 2KB which can be written in Assembly language if I'm not mistaken).

Функция маленького лоадера будет одна – закачать большой лоадер.
The only purpose of compact loader is to download a real loader.

Для этого нам нужен будет серьезный лоадер- т.е. большой лоадер, весить он будет думаю побольше и функций у него будет намного больше.
However real loader that we need for that purpose will be much larger in size but will support more functionality.

Во первых этот лоадер будет невидим в процессах.
First of all this loaded won't be visible by other processes. (Comment by Sunbelt – this means it probably won't be in the task list.)

Он будет рубить все фаерволы и антивирусы как только сможет.
It will disable all firewall and antivirus software in all possible ways.

Он умеет подкачивать любые файлы и запускать их для любого нашего адверта (об адвертах расскажу попозже).
Loader must be smart enough to download and run any file for any our Advertiser (I'll come back to Advertisers later in this text).

Ну и немаловажная функция лоадера – быть неубиваемым в системе. (каким-то образом или размножаться или иметь своего клона, короче прятаться от всяких прог, которые могут его потереть)
One of the most important loader functions is to resist to any attempt to terminate it (somehow it should either copy itself somewhere or clone itself or in other words to hide itself from any software that can remove it).

Итак что мы видим глазами ОПЫТНОГО юзера.
Alright, let's take a look at what ADVANCED user might see.

А мы видим следующую картину.
The picture is as following.

Юзер заходит на сайт, где стоит ифрейм код.
User visits the site where our IFRAME code is installed.

Естественно срабатывает эксплоит.
Of course this will result in exploit activation.

И загружает маленький лоадер, в свою очередь маленький лоадер загружает большой лоадер и удаляет себя.
This in turn will load compact loader on user's PC and then compact loader will download real loader and erase itself.

После этого большой лоадер начинает работу с того, что перерубает всю защиту на компе, а именно пытается вырубить фаервол, антивирус и тд тп.
After that real loader starts its job with disabling on deactivating any security and protection and in particular – attempts to disable firewall anti-virus and so on.

Сильно влезает в систему.
It infects system deeply.

Потом он сразу после этих функций начинает усердно скачивать все файлы, которые ему были заданы в админке. (об админке будем говорить так же попозже)
Right after that real loader begins to download all files which were requested by loader Admin program (we well talk about it later as well).

Ну короче скачал он все файлы, запустил их и сидит себе потехоньку пингует наш сервер, что бы показывать, что он в онлайне и еще может нормально работать(это нужно что бы мы знали какое количество ботов в онлайне)
When loader is done with files it should ping our server. This will tell us that given loader is alive on online and also will let us to find out how many such loaders are online at the moment.

Итак на данный момент я описал самую основную стадию нашего задания – работу лоадеров.
OK, by this moment I've described the most important functionality of our task – how loaders work.

Следующая стадия это админка или панель управления на сайте, короче называйте как хотите дело ваше.
Next step is Admin program or site control panel tool, you name it.

Панель управления будет двух видов : 1) Адинская 2) Адверская.
There are two kinds of Panels: 1) Admin; 2) Advertiser.

1) В админской панели управления можно видеть всю статистику по адвертам ,а именно : количество уникальных посетителей зашедших на сайт адверта с ифреймом.

Admin panel displays all stats on ads, namely total number of single users who visited Advertiser's site via IFRAME.

2) Количество не уникальных посетителей.

Total number of users visited Advertiser's site.

Количество уникальных загрузок **БОЛЬШОГО ЛОАДЕРА** т.е. обращу внимание на то, что загрузка будет выполнена тогда, когда будет установлен большой лоадер.

Total number of Loader downloads not counting the number of compact loader downloads (per user's PC)

Количество не уникальных загрузок большого лоадера.

Total number of Loader downloads.

Количество машин находящихся в онлайне.

Total number of infected PCs which are currently online.

Для данного адврета.

This is for given Advertiser.

А так же будет суммарная статистика по всем адвертам.

There also must be a summary for all Advertisers.

Т.е. будут складываться все цифры и показаны общие результаты по всей системе.

In other words we will count

Установка % редирекченного траффа глобально по всей системе

% of all installations and redirected traffic

и установка % конкретно для каждого адверта.

% of installation for given Advertiser

+ установка % реферала также как и выше, по всей системе и по конкретному адверту.

% of referrals for entire system and for each Advertiser.

Забеись конечно еще сделать статистику по странам.

It would be fucking great to gather stats for all countries where our software is deployed.

Т.е. какие страны заражаются, хотя бы в процентном соотношении.

For example it would be interesting to know computers in what countries are infected and the percentage of infected computers comparing to other countries.

Внимание ! лоадер не должен ставиться по второму разу.

Important! Loader must not infect the same computer more than once.

То есть он должен как-то определять свое нахождение в системе или еще как...

In other words Loader must detect whether given computer is already infected.

Но тем не менее в стастике должны отображаться неуникальные инсталлы.

Either way our stats should show if Loader was installed more than once anyway.

2) В адверской панели будет видно:

Advertiser's panel will show:

количество уникальных посетителей зашедших на сайт адверта с ифреймом.
Total number of unique users visited Advertiser's site contained IFRAME.

Количество не уникальных посетителей.
Total number of all users visited Advertisers site.

Количество уникальных загрузок **БОЛЬШОГО ЛОАДЕРА** т.е. обращу внимание на то, что загрузка будет выполнена тогда, когда будет установлен большой лоадер.
How many times Loader was installed (number of unique installations).

Количество не уникальных загрузок большого лоадера.
Total number of all Loader installations.

Количество машин находящихся в онлайне.
Total number of PCs which are currently online.

Для данного адврета.
This would be Advertiser specific info.

Забеись конечно еще сделать статистику по странам.
Т.е. какие страны заражаются, хотя бы в процентном соотношении. (короче повторяюсь)

I'm repeating myself but it would be great to gather stats for countries as well.

Естественно адверту нужно сделать новости, что бы он мог видеть сообщения от нас.
Of course, Advertiser should be given a possibility to get a feedback from us and communicate with us.

Новости будем писать из админки.
Our Admin console should provide an ability to communicate with Advertiser.

Регистрацию сделаем немного иначе.
Registration process will be done in a little bit different way.

Пусть будет все автоматизированно
I want everything to be automated.

Т.е. смотри юзер зарегился и после регистрации должен подтвердить ее у себя на мыле (к нему будет приходить специальный урл с кодом).
After registration Advertiser will receive an e-mail with a special URL that contains registration code.

После подтверждения он сможет спокойно зайти в админку.
After confirming registration Advertiser will be allowed to log in to Admin Console.

В админке он сразу получит ифрейм код, на который можно сливать трафик.
Admin console will let Advertiser to receive IFRAME code which allows him to redirect traffic.

Функции которыми владеет адверт.

Advertiser's Console:

Во первых у него в статистике будет такая панель, где он сможет вписывать урлы на exe файлы, которые ему надо подгрузить большим лоадером.
Advertiser will be able to specify all URLs that point to EXE files which she wants to load.

И нажимать кнопку типа : Load
А так же сможет устанавливать напротив каждого файла время, через которое повтороно подгружать этот файл (ну и естественно зарпускать)
Advertiser will be able to load those EXE in some very simple way for example by pressing "Load" button on her console. Advertiser will also be able to schedule EXE downloads.

Адверту будут доступны некоторые модули, которые он сможет галочкой добавлять лоадеру. (лоадер уже сам будет подгружать для этого адверта нужный ему модуль.)
Advertiser will have access to certain program modules which she'll be able to deploy to user's PCs via our loader.

Модуль консолей. (он у нас уже есть, просто его надо вшить в систему что бы там все само создавалось.)
Console module (we already have it and we simply should integrate it to our system to automate process).

Опишу вкратце
Briefly,
С помощью этого модуля он сможет добавлять нужные ему урлы в Trusned Zone (хорошо для устанавливания тубларов, дайлеров)
With this module Advertiser will be able to add any URL to Trusted Zone (which is useful to install Toolbars or Dialers on users PCs).

А затем вводить список урлов на тулбары, которые нужно установить.
After that Advertiser will be able to enter the list of URLs where Toolbars can be downloaded to users PCs.

Допустим он хочет поставить юзеру 2 тулбара.
For example if Advertiser wants two Toolbars to be installed on User's PC.

Прописывает их домены в Trusned Zone и вписывает урлы, которые будут открываться в виде невидимой консольки у юзера и установится тулбар.
To do that she would enter domain names where Toolbars can be downloaded and types the URLs which will be opened in invisible console on User's PC and will install these Toolbars.

Теперь описываю реферальную систему.
Now I'll describe the referral system.

Итак! Каждому адверту будет выдаваться особый урл.
Each Advertiser will get a special URL.

С присвоенным ему кодом.
This URL will be assigned certain ID.

Этот урл он может давать своим друзьям знакомым или просто где-то светить и привлекать других вебмастеров.
Advertiser may share that URL with anybody else or just put it on a web site for example or involve Web Masters in a process.

За то что с этого урла зарегается какой-либо вебмастер, адверт будет получать 10% его траффика.
If Web master registers at that URL then Advertiser gets 10% of given Web master's traffic.

Вебмастер же, который зарегистрируется по этому урлу будет получать законные 80% траффика.
Web Maser who registered at that URL gets 80% of traffic.

Терять % трафика будет только система, т.е. она будет уже получать не свои законные 20%, а всего лишь 10% от траффика адверта.
System will lose some traffic because it will no longer get 20% of traffic but rather 10% out of Advertiser's traffic.

(Напомню что наша система берет 20% **ИНСТАЛЛЯЦИЙ** от трафика вебмастрера)
(I want to remind that our system takes 20% of installations out of the whole Web master's traffic).

Реферальная система придумана для привлечения других вебмастеров. Так сказать для рекламмы.
Referral system is intended to involve other Web masters.

Итак на чем же будет зарабатывать наша система ?
How our system will earn money?

Во первых это 20% инсталяций от вебмастеров привлеченных нашей рекламной кампанией .
Firstly, all it's 20% out of all installations coming from site Web Masters who would be involved in process by our advertisement campaign.

И 10% от рефералов.
10% will come from referrals.

Сделаю важную пометочку! % трафика мы можем менять в любой момент ☺
I want to make an important note – we can change the percentage of traffic at any moment ☺

Во вторых абсолютно во все лоадеры т.е. 100% инсталляций, мы имеем право через свою админко подгрузить все что захотим.
Secondly, absolutely in all Loaders (meaning 100% of installations) we can inject our own code which will do whatever we want.

Т.е. параллельно с вебмастерами пользоваться их лоадерами можем еще и мы ☺
This means that we can use Loaders installed by Web Masters for our own benefit as well.

Это огромный плюс т.к. мы можем например подгружать какой-то новый тулбар и тд и с этого неплохо иметь денег.

That's a huge advantage because we can, for instance install our software such as Toolbars and earn money on it.

Теперь расскажу немного о черезвычайных ситуациях.
Now let's talk about force-major circumstances.
Бывает такая хуйня как абьюзы (т.е. жалобы юзеров) из-за этого могут снести сервер или хостинг на который пришла жалоба.
There is one fucking thing out there called abuse (meaning user's complaints). This may result in server shutdown in case of numerous complains or due to the nature of server's activity.

Следовательно Сам сайт, статистика и тд будет находиться на одном сервере, а exe файлы, и прочее на другом сервере.
To prevent that the site itself, stats and so one will be deployed to one dedicated server but executable files and other stuff will be deployed to the different server.

Нужно так же продумать что бы при сносе этих серверов, мы не теряли всех своих ботов.
We must come up with the idea of how to keep our software on a server even if server was shut down.

И смогли за сутки все восстановить на новых серверах. Вот.
And we want to recover everything within 24 hours on new servers. That's it.