Inside view of Lyposit aka (for its friends) Lucky LOCKER

malware.dontneedcoffee.com/2012/11/inside-view-of-lyposit-aka-for-its.html

2012-11-29 - Panel

The Lyposit Ransomware appeared wild in second week of September 3 days after this post :

Lucky LOCKER advert (note the IR)

Text of the Advert *(click to unfold)*

1)Чистый Вин Апи.

2)Практическая неубиваемость локера, в том числе и через безопасный режим, и даже если грузится с загрузочного диска.

То есть тот же локер от гансты можно отрубить через ctrl+alt+delete)) о уровне можете судить сами...

Смысл в чем что локер делает такие изменения системы - что даже если юзер каким то образом умудриться убить процес - ему прийдеться реинстал винды делать - так как система нормально работать не будет, либо перезагрузиться

и заплатить чек)

3)Я беру 20% от вашей прибыли - вмз или либерти. то есть чеки вы налите Сами. и уже сами переводите мне мой процент.

4) Качественно промо которое постояно изменяется - смотрим конверты и выбираем наиболее оптимальное. страны : IR CH ES AT BE FR GB PL DE DK PT

формат промо html и USA - основной упор сделан на ней как раз

вообще интересует 3-5 человек с котрыми на постоянке буду работать. продукт может быть изменен по вашим советам и как угодно дописан.

обращаться в джабер

Quote:

Установка

=========

При запуске выполняется установка по следующим направлениям:

1) при достаточных правах (администратор для WinXP, Elevated Integrity Level / Admin для Win Vista+) осуществляется запись в параметр Shell раздела

*****

обеспечения автозапуска как в обычном, так и в безопасном режиме

2) при недостаточных правах осуществляется запись в доступный раздел *****

3) в любом случае используется дополнительный автозапуск путем модификации настроек командного процессора (не требуется особых привилегий)

В результате при запуске командного процессора в ходе обычного процесса установки/ удаления программ, осуществляется автозапуск

Работа

======

Проверяется наличие файла конфигурации, который представляет из себя архив ZIP с локальной копией страницы для отображения пользователю, в формате ***.

При отсутствии файла, выполняется его запрос из панели управления через технологии BITS и Wininet, что позволяет выполнить обход некоторой части защитного ПО.

Полученный файл распаковывается во временную папку, и выполняется запуск скрипта

В дефолтном примере использованы настройки скрипта, которые разворачивают страницу на весь экран, отключают прокрутку и т.п. При изготовлении специализированных

под страны страниц необходимо использовать аналогичные настройки

Параллельно с запуском страницы с сообщением, выполняется циклическая смена цветового оформления ОС (все элементы черные/красные), отключение визуальных и иных

эффектов, а также сокрытие всех не относящихся к процессу страницы окон. В результате, даже при недостаточных привилегиях, осуществляется существенное затруднение

доступа к элементам интерфейса. Настройки цветового оформления сохраняются лишь до момента выхода пользователя из ОС.

В формате страницы предполагается наличие поля для ввода кода . При их разработке необходимо иметь в виду, что цветовые настройки ОС будут изменены

и для видимости поля и текста необходимо принудительно определить цвет шрифта / фон поля ввода, а также не использовать стандартную кнопку отправки формы (вместо

нее следует использовать изображение).

Скрипт внутри страницы должен выполнить базовую проверку введенного кода (длина, цифры и т.п.) и при положительной проверке - выполнить вывод его через

javascript:alert(); Приложение перехватит появившееся окно, считает код и закроет его.

Полученный код будет отправлен и сохранен на сервере. В случае успешной отправки страница будет заменена на - в котором рекомендуется подготовить

текст о временном отключении блокировки и просьбе осуществить выход из системы / перезагрузку, если она не произойдет ближайшие 10 секунд.

По прошествии 10 секунд страница принудительно закрывается и инициируется процедура выхода пользователя из системы. При недостаточных привилегиях получится

просто пустой экран или экран с некоторыми окнами.

Выход из системы и последующий вход необходимы для автоматического восстановления цветового оформления.

Перед выходом устанавливается специальный флаг, который сигнализирует о необходимости отложения визуальных эффектов блокировки доступа к ОС. При его наличии

приложение в фоновом режиме осуществляет запросы к серверу с интервалом 15 минут для получения информации о результате обработки оператором данных от клиента.

Оператор через админ интерфейс может дать команду на повторное отображение страницы при неверных данных, либо на самоудаление, если проверка данных прошла

успешно.

вообще продукт готовился для себя.

---

translated by google as : (click to unfold)

Our advantages:
1) Net Win Api.
2) Practical indestructibility locker, including a safe mode, and even if the boot from the startup disk.
That is the same locker from gangsta can cut off a ctrl + alt + delete)) on the level you can judge for yourself ...
What is the meaning of that locker makes such changes in the system - even if the user somehow manage to kill the process - he will have to reinstal Windows to do - because the system does not work properly, or reboot

and pay check)
3) I take 20% of your profits - wmz or liberty. that is, checks can nalite themselves. and already I translate my own interest.
4) Qualitatively promo is always changing - see the envelopes and select the most optimal.
country: IR CH ES AT BE FR GB PL DE DK PT
html format promotional and USA - the main focus is on her right
3-5 people generally interested with KOTRA on postoyanke will work. product can be changed by your advice and somehow appended.

contact Jaber

Quote:
Installation
==========
When you run you are installing in the following areas:
1) with sufficient privileges (administrator for WinXP, Elevated Integrity Level / Admin for Win Vista +) writes to the parameter section Shell
*****
ensure autorun both in normal and safe mode

2) the failure of the right of the recording available in section *****

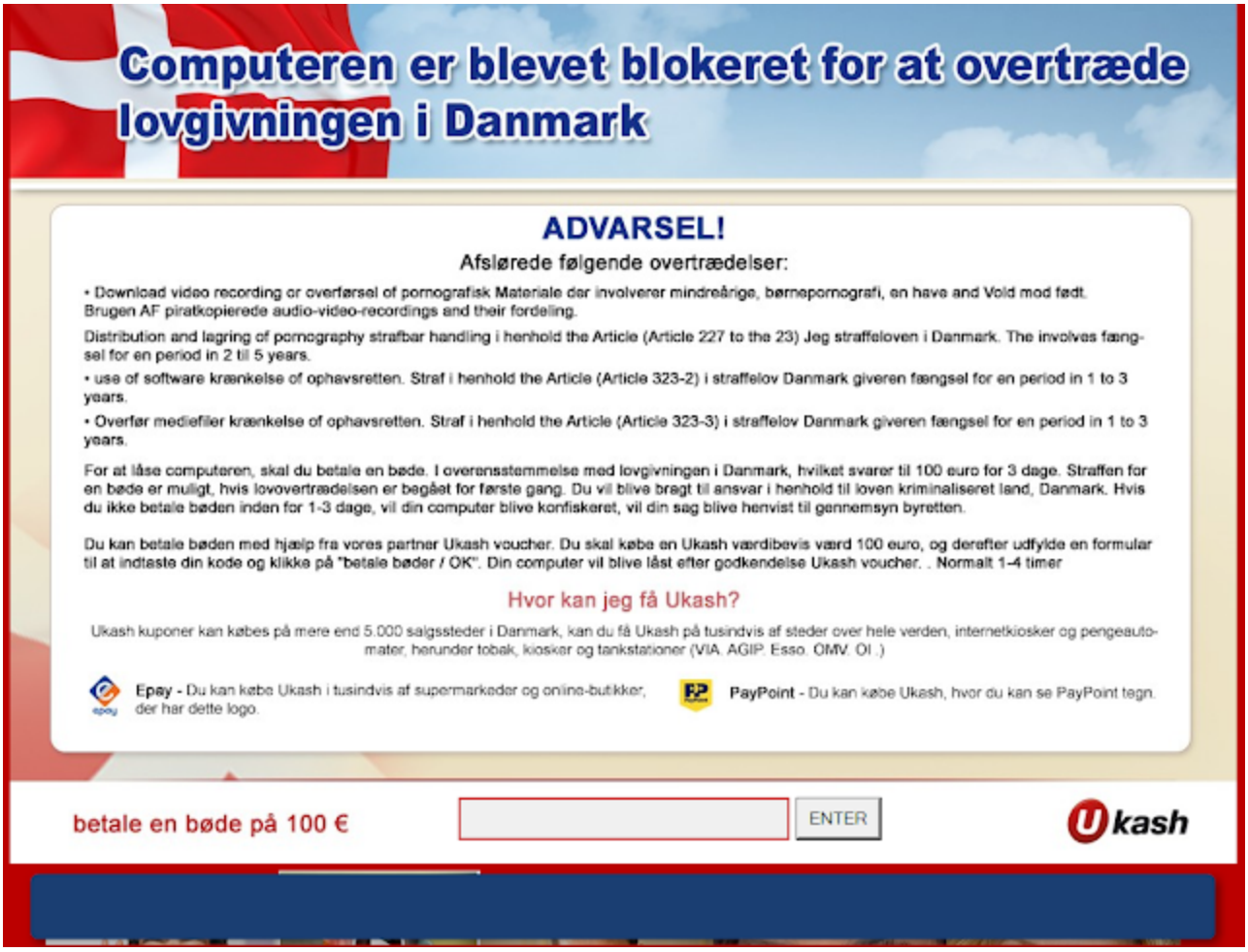
3) In any case, the additional auto settings by modifying the shell (no special privileges)
As a result, when you start a shell in the normal course of the installation / removal of software, by auto

Work
======

Checks for a configuration file, which is a ZIP archive with a local copy of a page to display to the user in the format. ***
In the absence of a file, it runs a query from the control panel through the BITS technology and Wininet, that allows you to bypass some of the security software.
The resulting file is extracted to a temporary folder, and you are running a shell script
Example used in the default configuration script that deflect the page on the screen, turn off scrolling, etc. In the manufacture of specialized
under the country pages to use the same settings
In parallel with the launch of the page message, the cyclic change colors of the OS (all the black / red), disabling visual and other
effects, and the secrecy of the process of non-page windows. As a result, even with insufficient privileges, is a significant difficulty
access to user interface elements. Setting color schemes remain only until the user logs out of the OS.

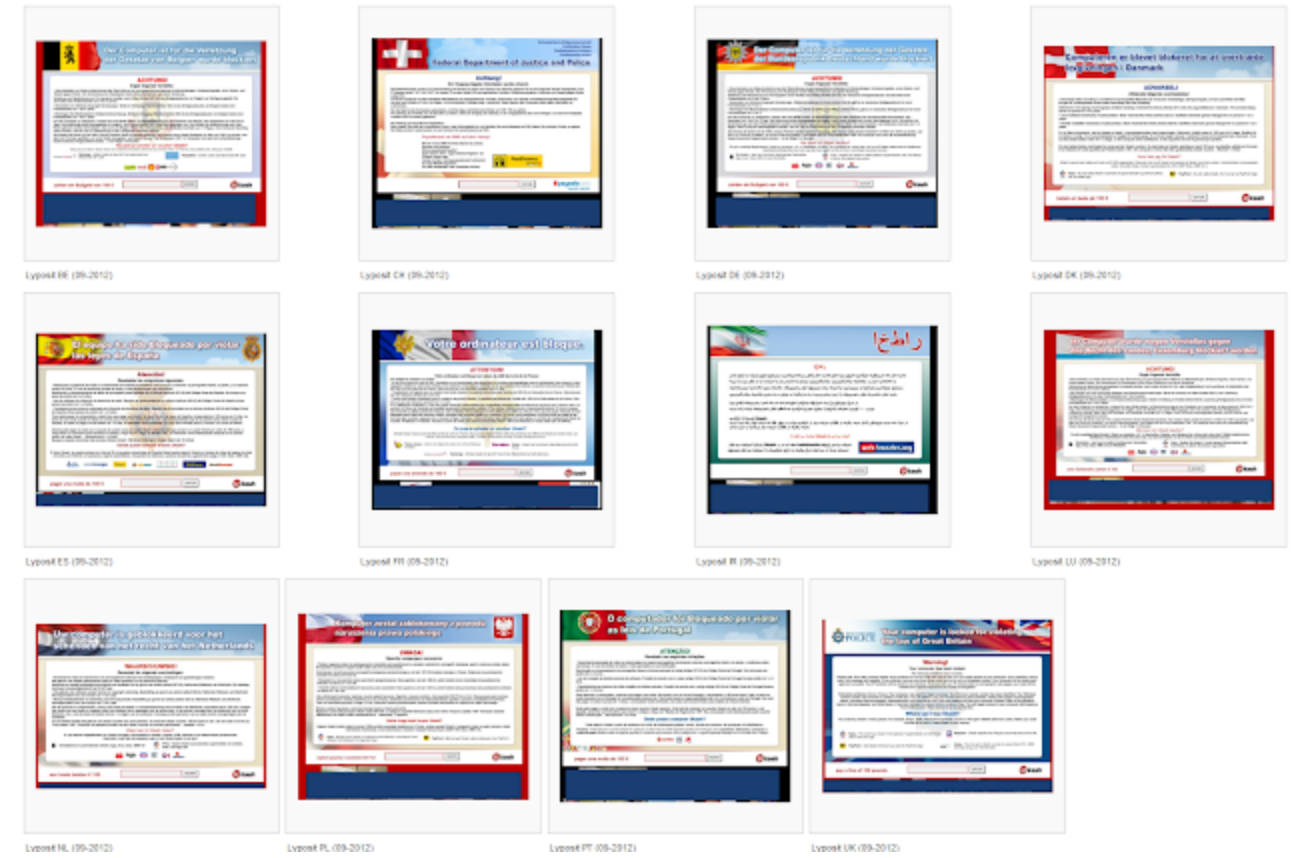
In the format of the page assumes a field to enter the code. In their development must be borne in mind that the color settings of the OS will be changed
and visibility of the field and the text you want to force to identify the font color / background input field, and do not use the standard submit button (instead of
She should use the image.)
Script within the page should perform basic validation code entered (length, numbers, etc.) and with a positive test - run its output through
javascript: alert (); application intercepts the window that appears, according to the code and close it.
The resulting code will be sent to and stored on the server. If successful, the page is submitted will be replaced - which is recommended to prepare
text to temporarily disable blocking and request to implement logout / reboot, if it does not happen the next 10 seconds.
After 10 seconds Page forcibly closed and the procedure is initiated logout. If there is insufficient privileges will
just a blank screen or a screen with several windows.
The output from the system and the subsequent input required for the auto recovery color choices.
Before the release are indicated by a flag that indicates if a pending visual effects to block access to the OS. If available
application in the background, makes a request to the server every 15 minutes to provide information about the result of processing the data from the client.
Operator through the admin interface can give the command to re-display the page with incorrect data, either on samoudalenie if the test data was successfull.
all products are ready for you.

What make Lyposit different from others :
- it seems to be the first one to target Denmark,



Lyposit DK (09-2012)

- it was targeting Irish (IE) people with a poor Iranian (IR) design
- it was showing images (gathered from the browser cache?) at the bottom of the screen
- the design downloaded from the C&C was conditioned by the Regionals Settings of the infected computer
- the Background was blinking from Black to Red



Lyposit Design in September 2012
(The sample I used to gather design was catched by Malekal and spotted as a new Ransomware by S!ri)

Now we should talk about Ransom Casier but I think you'll get seriously bored so let's move on.

1 week ago :

Text:

на днях тестил траф:

USA 2970 ботов

12300$ - монейпака

наберу новых адвертов

3-5 человек.

Основное направление ЮСА

От вас:

от 5к юса ботов в сутки,

скрин статы сплоита на фоне вашей жабы в ПМ. я стукну к вам в джабер.

возможна установка софта полнолстью на ваш сервер. то есть никакого шейва в принципе быть не может.

---

translated by google as

---

recently testil cores:

USA 2970 bots

$ 12,300 - moneypaka

gathering a new adverts

3-5 people.

The main direction of JSA

From you:

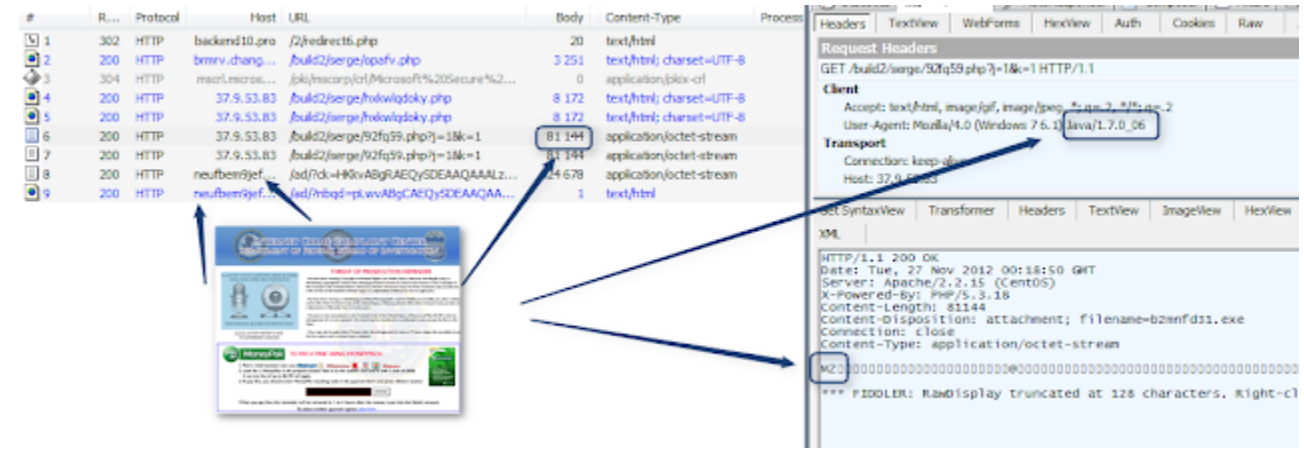
Yusa bots from 5k a day

screen sploita stats against your toad in the PM. I knock to you Jaber.

polnolstyu optional software on your server. that is, no sheyva in principle can not be.

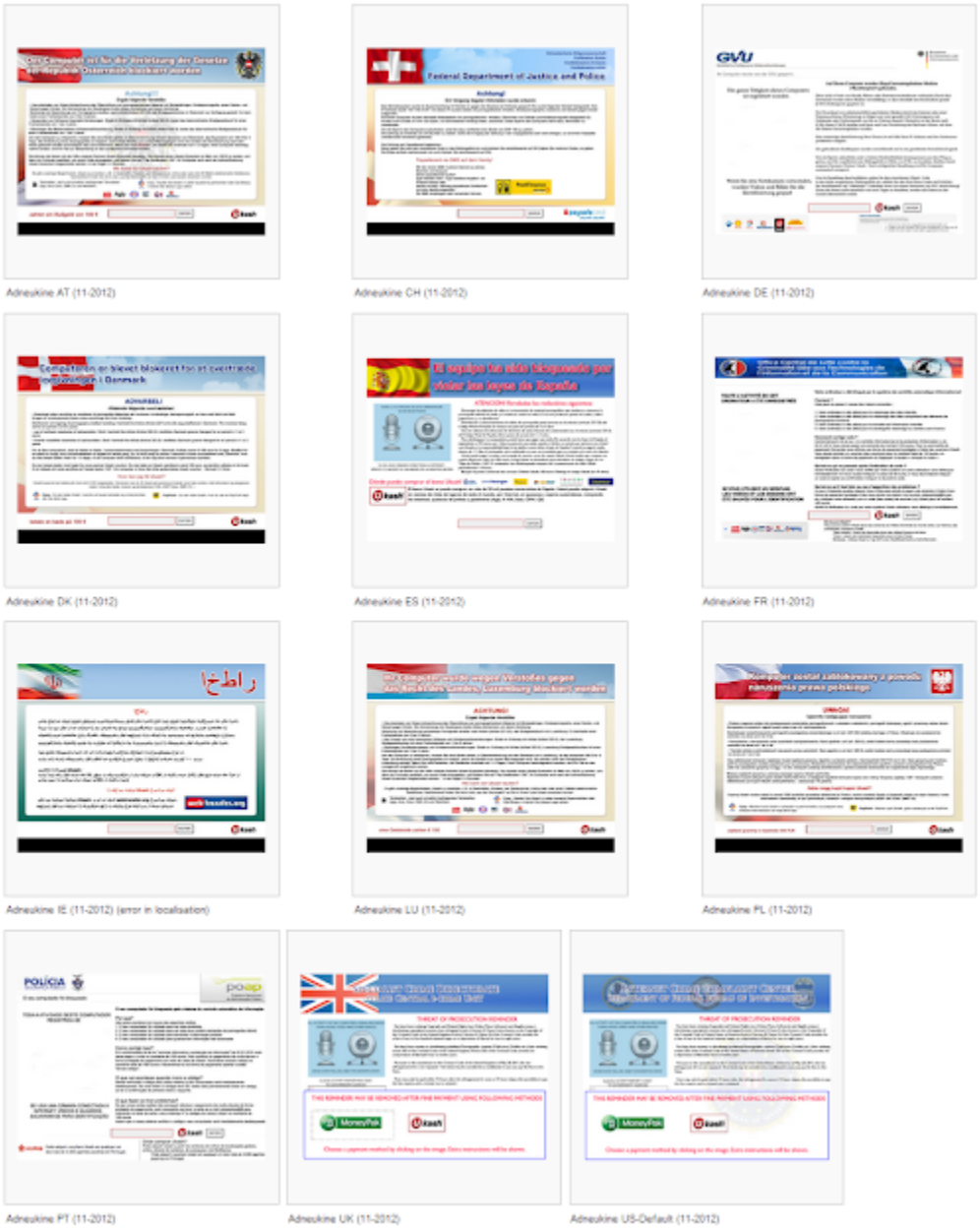
---

3 days after ...here is it, pushed by ProPack :



ProPack pushing Lyposit with a New Design

Named few hours Adneukine by Microsoft and then renamed to Lyposit.B here are the design



Lyposit.B design in November 2012.
2 new design (US, UK), reuse of Epubb design for FR, PT and DE...and it's still showing an iranian Flag to people living in Ireland

v0.2

Panel Title - v0.2...
they plan a big future it seems.

Not that much to see inside :

Loads stats

[reload] [download new data from [redacted]] logout

locales

country	count
United States	3497
[redacted]	38
	10
	8
	6
	5
	5
United Kingdom	5
Ukraine	5
France	4
[redacted]	
unk locale id all	3634

build ids

build id	count
[redacted]	3634

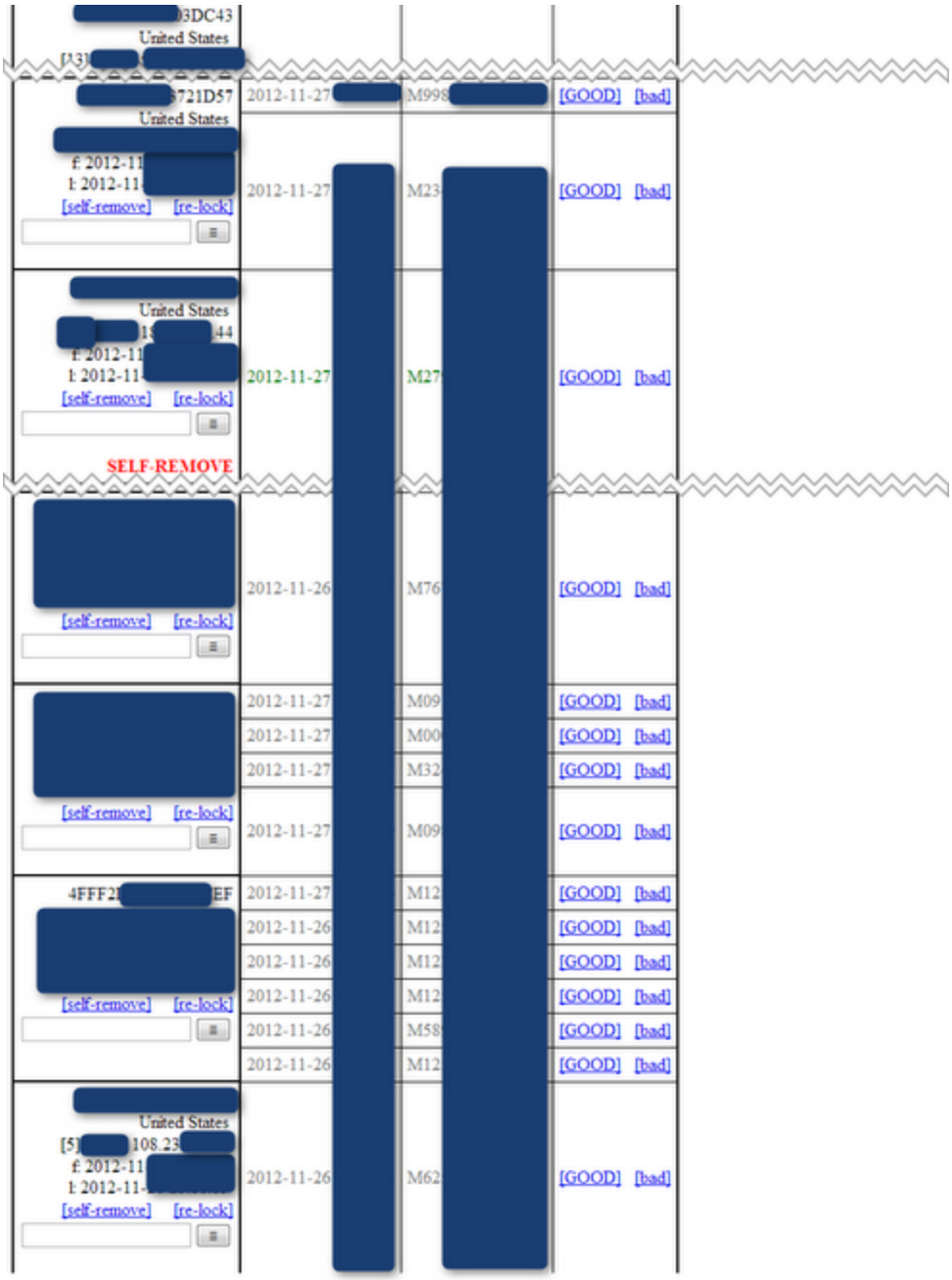
bulk results parser

Paste here a list of parsed vouchers, one on a line, adding **g** or **b** at the end of the line, after a space, to indicate a good or bad result.
Parser will set the state for all found vouchers and issue unlock command for machines with at least one valid voucher.

Parse

Incoming data

client info	added	data	mark record
AA2801EAD573[redacted] United States [5][redacted]190.148 f: 2012-11-2[redacted] l: 2012-11-27 [self-remove] [re-lock]	2012-11-27 [redacted]	M395282[redacted]	[GOOD] [bad]



LuckyLocker Control Panel v0.2

Lyposit.A
e2569d952c0c48976c20758fd13e6155 12/09/12
da9e23912e82eaa865527cdaebef49e5 10/09/12
c3ae37d3e970e6b7aee99b1c144ca6fc 14/09/12

Lyposit.B :
e2569d952c0c48976c20758fd13e6155 26/11/12
6d4dd63d0290b83c1f8cbd40b368b349 27/11/12
c33987e0a9043f33dae133d2586b0253 27/11/12

Some C&C Call :
Lyposit.A:
windowsonlypositives .org GET /ad/?eaisx=Somebase64encodedData 91.218.231.196 - 12/09/12
orp-pro.org GET /ad/?vzos=Somebase64encodedData 46.254.19.102 -- 14/09/12
Lyposit.B :
neufbem9jefnike .com GET /ad/?ck=Somebase64encodedData 37.143.12.145 -- 26/11/12
kiribati91 .org GET /ad/?sshe=Somebase64encodedData 37.143.12.145 -- 27/11/12

Files (private password) :
http://goo.gl/E9beI (Mega)