TREND MICRO

Securing Your Web World



Rogue DNS servers – a case study

Feike Hacquebord
Forward Looking Threat Research, Trend Micro
Cupertino, CA, USA
feikehayo_hacquebord@trendmicro.com

Contents

- Introduction to DNS
- DNS Changer Trojans
- Rogue DNS servers
- A large rogue DNS network
  - replacing advertisements with DNS tricks
  - fraud with search engines
  - personal information leakage
  - installing a Trojan via update functions
  - click fraud with referral / affiliate programs
- The role of Esthost.com
- Reconstructing the zone file of the rogue DNS servers.
- Remedies
- Concluding remarks

Introduction to DNS

Domain Name System servers translate domain names to IP addresses. This is essential for the internet to work.

Most internet users automatically use DNS servers of their ISP.

DNS has not been designed with security in mind. Internet users implicitly trust the DNS servers they use.

What happens when DNS settings of internet users are silently changed to foreign DNS servers?

Rogue DNS servers

Rogue DNS servers resolve certain domain names to malicious IP addresses.

Victims of rogue DNS servers may be directed to malicious websites without them noticing it.

The surfing habits of victims of rogue DNS servers may be monitored for a long time. This makes targeted attacks possible.

DNS Changer Trojans

DNS Changer Trojans silently change DNS settings on the victim's computer to foreign DNS servers.

An example are the fake Video Codec Trojans which are supposedly needed to view video content.

Some websites install a "unique" DNS Changer Trojan for each victim (this was originally posted on a Unisog mailing list: http://lists.sans.org/pipermail/unisog/2006-November/026937.html)

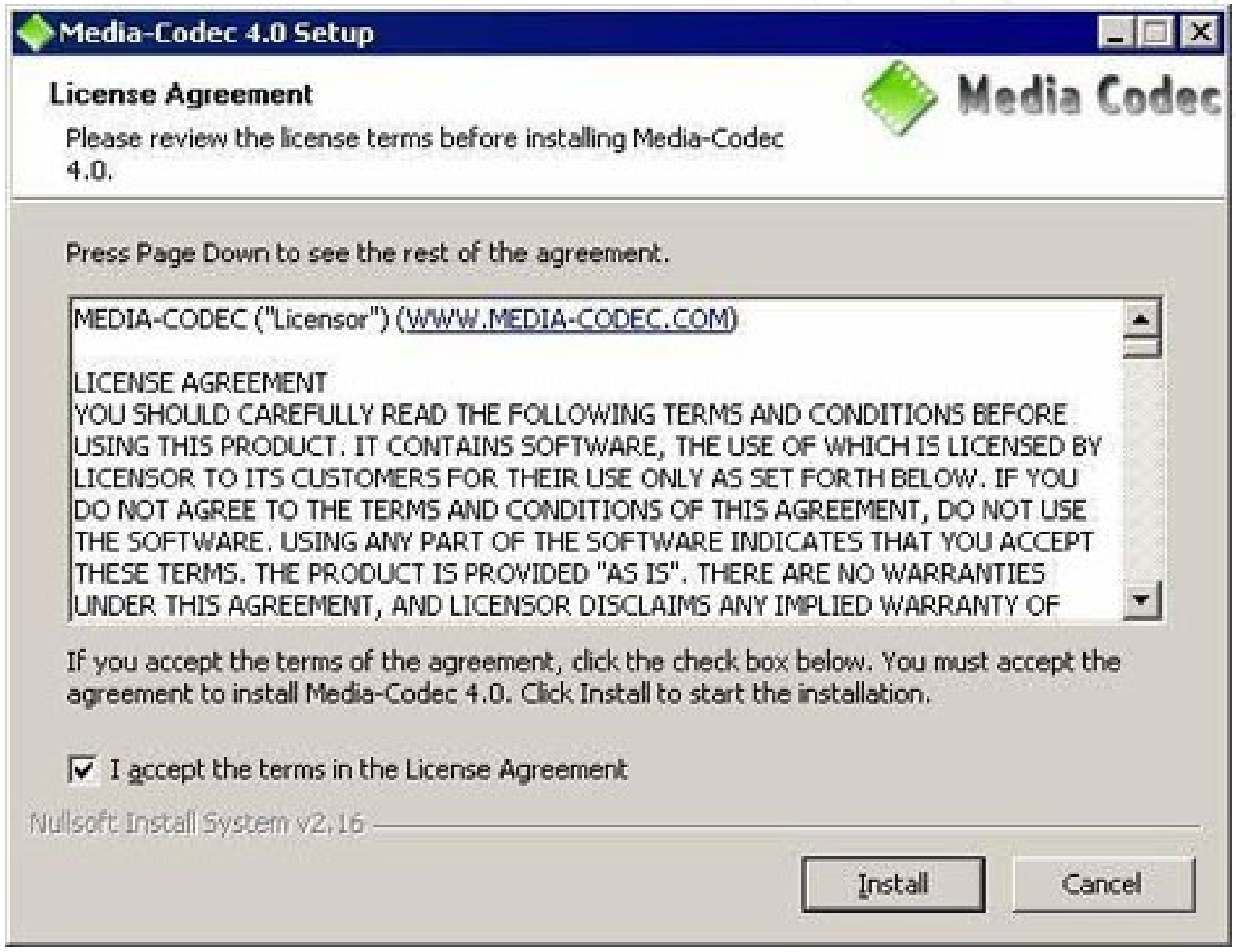
.

A typical website of a DNS Changer Trojan

Professional looking websites attempt to lure internet users into installing a fake codec.

An EULA of a DNS Changer Trojan

A License Agreement of a DNS Changer Trojan

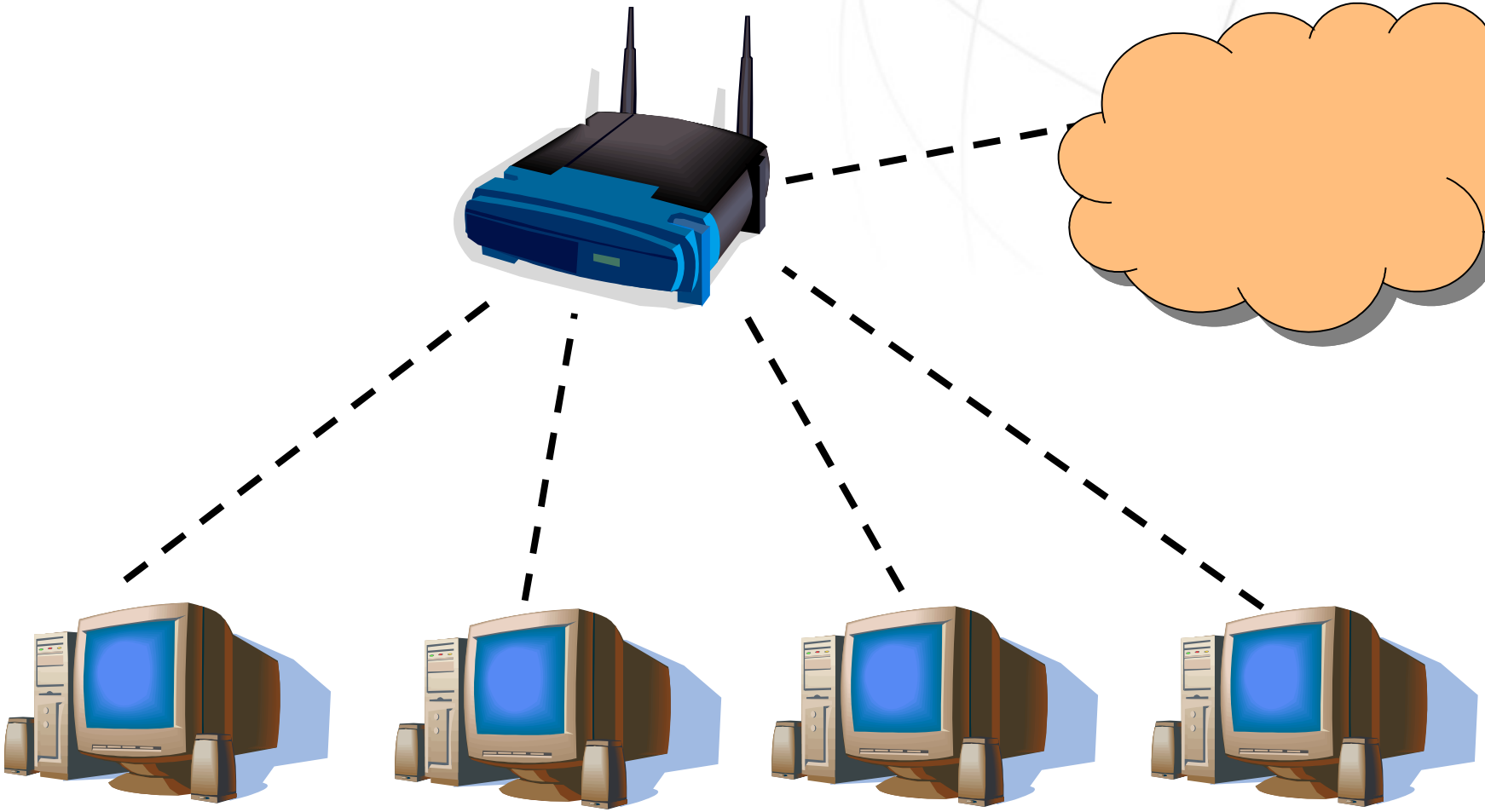


Spreading rogue DNS settings

Some of the DNS Changer Trojans attempt to modify DNS settings of routers by brute force password attacks.

This means that once 1 client in a network is infected all other clients will be using rogue DNS servers once the Trojan is able to modify DNS settings on the router

Spreading rogue DNS settings (cont.)



Spreading rogue DNS settings (cont.)

Some of the DNS Changer Trojans install a rogue DHCP server that will reply to DHCP requests of other clients in the same network that come online. These rogue DHCP servers propagate rogue DNS settings

(DHCP is a protocol that assigns network parameters like DNS servers to clients in a network).

Spreading rogue DNS settings (cont.)

So rogue DNS settings can spread in a network when only 1 client is infected.

Result:

Other clients in the same network are at great risk because of modified DNS settings.

Clients might even get infected through (automatic) update functions of legitimate software that has been installed.

A large network of rogue DNS servers

- We found more than **1175** rogue DNS servers most of them hard coded in DNS changer Trojans.
- These rogue DNS servers exhibit the same kind of behavior.
- Rogue resolution of **14,000+** domains to **200+** IP addresses.
- Internet connectivity by Pilosoft (2005 -), Cernel (2007 -), Intercage (2005 - 2008), UkrTeleGroup (2008).
- This network is stable and about 4 years old.
- Estimated number of victims ~ **4,000,000** Feb 2009.

Behavior of rogue DNS servers

- Most domain names get resolved correctly
- Non existent domain names got resolved
- Some domain names get resolved to foreign IP addresses

  These include domain names of:

  - search engines
  - advertising companies
  - popular dating sites
  - financial institutions
  - legitimate software
  - other malware and C&C servers

Targets of rogue DNS network

- Google, Yahoo, AOL, MSN, Live.com, Ask.com
- Google Ads, Doubleclick, AOL Advertising, yieldmanager.com, CCbill.com, Fastclick.net, Webpower.com, Alexa.com, digg.com
- Credit Suisse, Mortgage / insurance brokers
- Adobe flash
- Friendfinder Inc, UK Dating,…
- All Music, musicload.de, …
- Travel Channel, Travelocity,
- AV companies / Microsoft

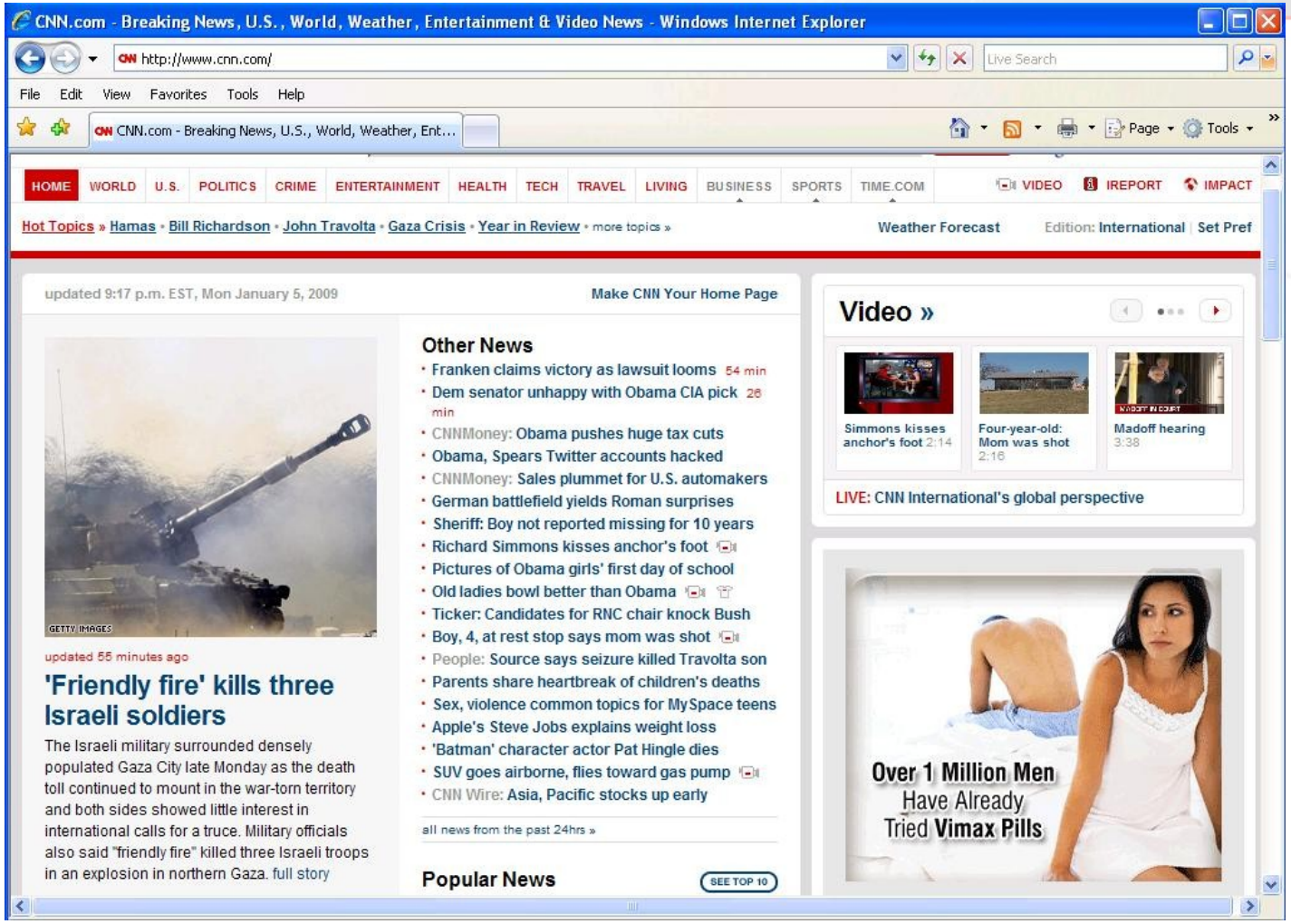
Targets of rogue DNS network (Cont.)

- Pornography distributors (Penthouse, Hustler, porn.com + many many more)
- Domain names known for hosting C&C servers
- Domain names of rogue (fake) AV software
- Some domain parking FQDNs that host scripts

Stealth click fraud – replacing ads

CNN.com on January 5th 2009 with a Double Click ad related to a car

Stealth click fraud – replacing ads (cont)



CNN.com loaded by a DNS Changer victim on January 5th 2009. Double Click Ad is replaced by a Vimax pills Ad from a foreign server.

Stealth click fraud – replacing ads (cont.)

The rogue DNS servers can resolve any advertising domain name to a foreign IP address and let victims load ads from there.

This is very hard to detect click fraud

- no automated clicks
- fraud happens outside the network of advertisers

Negative impact:

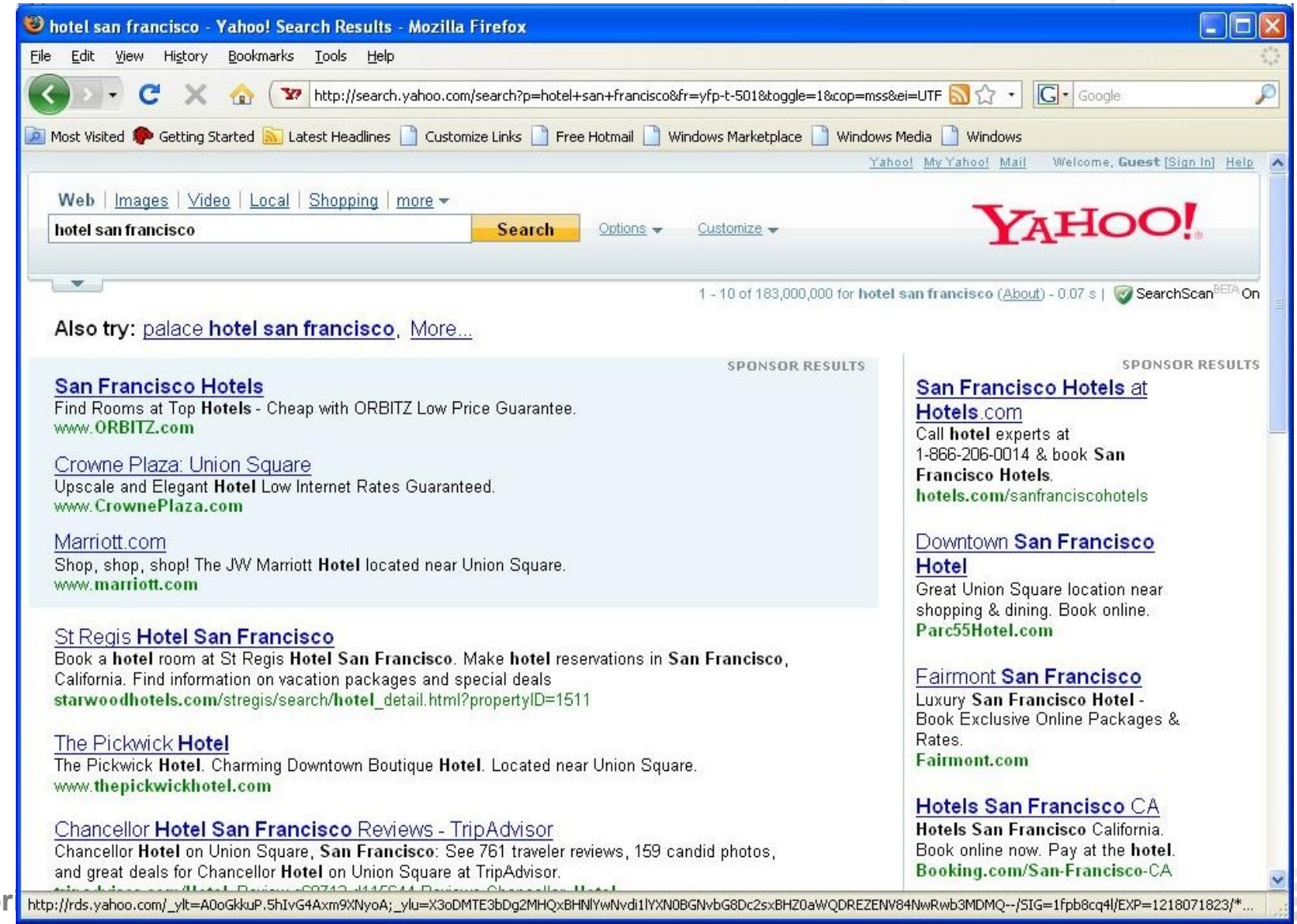
- loss of revenue
- reputation damage

Hijacking search engine results

We search for a hotel in San Francisco at Yahoo.

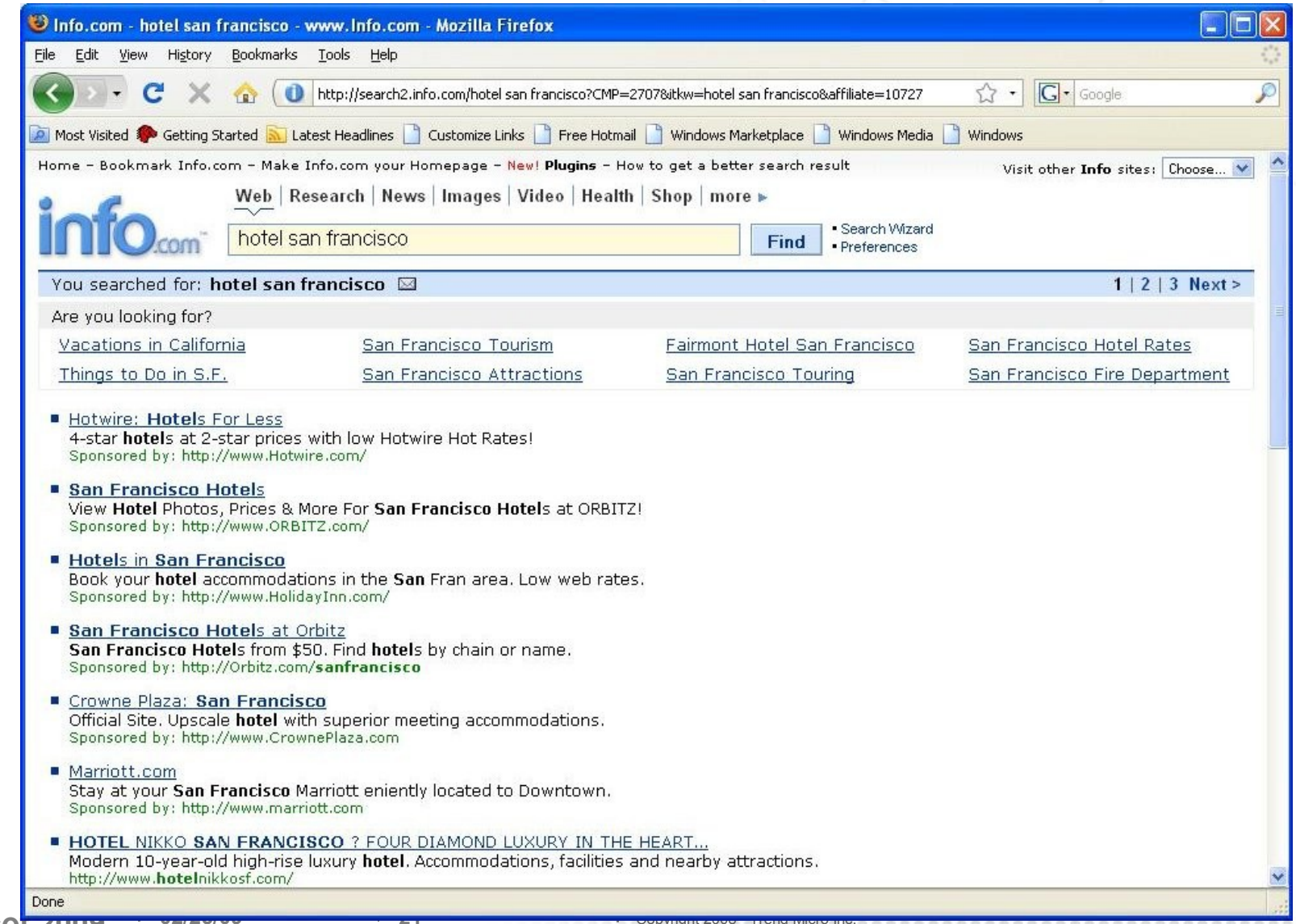
Hijacking search engine results (cont.)

We get search results back. Then we click on a sponsored result.



Hijacking search engine results (cont.)

We get redirected via a rogue version of rds.yahoo.com -> theft of traffic.



Hijacking search engine results (cont.)

The rogue DNS servers target major search engines, like Google, Yahoo, MSN, AOL, Ask.com

Example: a DNS Changer victim enters a search query into www.yahoo.com

- www.yahoo.com gets resolved normally by the rogue DNS servers; the victim gets back search results from Yahoo
- When he clicks on a (sponsored) search results he gets redirected via rds.yahoo.com to the site found in the search results. This is all normal.

BUT

- rds.yahoo.com gets resolved to a foreign IP address (currently 67.210.12.167). This foreign server may redirect the internet user to any site → hijacking of (sponsored) search results.

Example of *possible* information theft

August 2008 the rogue DNS network started to resolve www.credit-suisse.com and several British mortgage broker sites to a foreign IP address.

This was for a relatively short period. However personal information might have been stolen during this period.

Other finance related domain names got rogue resolution for a short period in February 2009:

finance.yahoo.com, finance.google.com, www.marketwatch.com

Example of Information theft (2007)

- Friendfinder accepted login data on two FQDNs

  www.friendfinder.com and friendfinder.com

  http://friendfinder.com/p/login.cgi was the login script of site www.friendfinder.com
- The related rogue DNS servers resolved:
  - friendfinder.com to IP 216.255.180.130 (foreign)
  - www.friendfinder.com to IP 209.185.12.47 (normal)
  - IP 216.255.180.130 parsed login data sent by victims to http://friendfinder.com/p/login.cgi and redirected victims to http://www.friendfinder.com/p/login.cgi with the login data -> leakage of personal information.
- Friendfinder claims to have ten millions of users.
- This problem has been fixed by Friendfinder in 2008

Installing Trojans via update function

Legitimate software frequently polls a website for updates. Updates might even be installed automatically.

What happens when the domain name that hosts updates of legitimate software gets resolved to a foreign IP address?

Instead of an update a Trojan might get installed.

Installing Trojans via update function (cont.)

January 2009: attempts to abuse the update function of Adobe's flash:

Rogue resolution:

fpdownload2.macromedia.com. 600 IN A 87.118.122.xx

87.118.122.xx is hosting a Trojan called cab.our

Installing Trojans via update function (cont.)

From a log file of the foreign spoofed Adobe site:

78.135.32.241::fpdownload2.macromedia.com/pub/shockwave/cabs/flash/swflash.cab::/home/hosting/87.118.122.95/www/htdocs/files/fpdownload2.macromedia.com/cab.our::Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506)
69.226.106.26::fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflash.cab::/home/hosting/87.118.122.95/www/htdocs/files/fpdownload2.macromedia.com/cab.our::Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; SpamBlockerUtility 4.8.4; .NET CLR 2.0.50727)
208.120.85.152::fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflash.cab::/home/hosting/87.118.122.95/www/htdocs/files/fpdownload2.macromedia.com/cab.our::Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)

Referrer click fraud

The rogue DNS servers use a vulnerability in the setup of some advertising companies.

Some advertising companies accept clicks on several FQDNs.

- http://one.foo.com/register_click.php?affiliate=1
- http://two.foo.com/register_click.php?affiliate=1

The rogue DNS servers resolve one.foo.com to a foreign IP address 1.2.3.4 and two.foo.com correctly.

http://one.foo.com/register_click.php?affiliate=1

gets loaded from foreign IP address 1.2.3.4 by a DNS Changer victim. This foreign IP address redirects to

http://two.foo.com/register_click.php?affiliate=2.

Domain two.foo.com gets resolved normally so the victim will load this URL from the real advertising company -> click fraud

Referrer click fraud (Cont.)

- Example (2009):
  - Refer.ccbill.com gets resolved to foreign IP 78.47.234.33
  - Refer2.ccbill.com gets resolved to IP 64.38.240.20 (normal)
  - A DNS Changer infected user will load the advertisement link

    http://refer.ccbill.com/cgi-bin/clicks.cgi?CA=912675-0000&PA=14
    "

    from foreign server 78.47.234.33. This foreign server changes the PA tag and then redirects the victim to

    http://refer2.ccbill.com/cgi-bin/clicks.cgi?CA=912675-0000&PA=***1524911&HTML=http://www.foo.com***
  - As a result the wrong party will be paid for showing the advertisement.

Referrer click fraud (cont.)

- Details where PA tag of ccbill.com gets changed:

  * About to connect() to 78.47.234.33 port 80

  * Trying 78.47.234.33... connected

  * Connected to 78.47.234.33 (78.47.234.33) port 80

  > GET /cgi-bin/clicks.cgi?CA=912675-0000&PA=1470590&HTML=http://www.foo.com HTTP/1.1

  > Host: refer.ccbill.com

  >

  < HTTP/1.1 302 Found

  < Date: Mon, 05 Jan 2009 ..:..:.. GMT

  < Server: Apache/2.2.3 (Debian) PHP/5.2.0-8+etch13

  < X-Powered-By: PHP/5.2.0-8+etch13

  < Location: http://refer2.ccbill.com/cgi-bin/clicks.cgi?CA=912675-0000&PA=**1524911&HTML=http://www.foo.com**

  < Content-Length: 0

  < Connection: close

  < Content-Type: text/html; charset=UTF-8

  * Closing connection #0

Esthost.com and DNS Changers

- *Esthost* is an Estonian Webhosting company operating in the US using several names like

  Esthost, Estdomains, Cernel, Rovedigital, Internet Path Inc. , Infradata,…

  Esthost has been hosting DNS Changer Trojans, C&C servers, rogue DNS servers and backend servers of the rogue DNS network from 2005-2009, mainly in Intercage, Cernel and Pilosoft IP space.

  Is there more to say about the role of Esthost?

Esthost.com and DNS Changers (cont)

The role of Esthost has been VERY suspicious. Some of the more interesting evidence:

- Numerous FQDNs in the Esthost.com zone file appeared to host crucial back end servers for the rogue DNS network (until Intercage went down in September 2008).
- Probable involvement of Esthost employees in the “Mega Traffic Distribution” (megatds.com) system that redirects DNS Changer victims.

Interesting FQDNs at Esthost.com

- dns-repos.esthost.com

  management system for rogue DNS network.
- dns1.esthost.com, dns2.esthost.com, dns3.esthost.com,… dns52.esthost.com

  52 backend servers for rogue DNS servers
- apdns1.esthost.com, apdns2.esthost.com, apdns3.esthost.com,… apdns26.esthost.com

  26 backend servers for rogue DNS servers
- testdns1.esthost.com, testdns2.esthost.com

  Confirmed rogue DNS servers. For testing purposes?
- testapdns1.esthost.com, testapdns2.esthost.com

  Confirmed rogue DNS servers. For testing purposes?
- codecsys.esthost.com, ucodecsys.esthost.com

  Backend systems of codec Trojan servers.
- megatds.esthost.com

  “Mega Traffic System?” Click fraud system? Related to www.megatds.com

Interesting FQDNs at Esthost.com (cont.)

- banex1.esthost.com – banex7.esthost.com

  "banner exchange" servers? These servers were (DNS) back ends for the spoofed version of pagead2.googlesyndication.com, media.fastclick.net, a.tribalfusion.com,…

- xgallery1.esthost.com – xgallery10.esthost.com

  (DNS) back end servers for porn leading to Zlob.

+ *more*

Who controlled the zone file of Esthost.com?

Intercage went offline – what happened?

Saturday, September 20 2008, Intercage went offline. What happened with the rogue DNS network?

- 655 (out 1178) rogue DNS servers went down
- most of the 14,000+ rogue resolutions disappeared…

However from Monday, September 22 2008 onwards rogue versions of major search engines moved to 67.210.12.0/24.

January 2009: the spoofed websites of advertising companies, porn distributors etc are spread over several IP addresses of multiple webhosting companies.

Estimated number of DNS Changer victims: ~ 4,000,000 (February 2009).

Reconstructing the rogue DNS zone file

The zone file of the rogue DNS servers can be reconstructed by:

- passive DNS data (look for DNS mismatches / discrepancies)
- resolving numerous domain names with the rogue DNS servers

We found 14,000+ rogue resolutions

Contact me for details.

Remedies for ISPs

- ISPs can protect their internet users by
  - Dropping DNS queries to known rogue DNS servers
  - Detecting DNS queries to foreign DNS servers on the gateway
  - Forcing their customers to use the DNS servers of the ISP, much like forcing outgoing email to be relayed through the mail servers of the ISP.

Conclusion

Rogue DNS servers are a major threat. They may be used for:

- Click fraud
- Theft of personal information
- Targeted attacks
- Installing Trojans

The Zlob related rogue DNS network is

- very large (1100+ rogue DNS servers)
- well connected to the internet
- Very stable and about 4 years old

the bad guys must make a lot of revenue here …

There is evidence that Esthost is part of the rogue DNS gang

ISPs can protect their users by

- blocking DNS queries to rogue servers
- forcing their users to use the DNS servers of the ISPs

Thank You

Trend Micro | Securing Your Web World



TREND MICRO™