

DNS Changer Attacks

Diane Bickram, Elizabeth Lamb, & Heer Trivedi

What is a DNS Changer attack?

DNS Changer attacks changes DNS server entries in infected computers to point to malicious servers under the control of the attackers, rather than the DNS servers provided by any ISP or organization without the users' knowledge nor consent.

When a user of an infected system visits a legitimate website on the Internet (say, amazon.com), the malicious DNS server will lead you to a phishing site.

There were two types of major attacks that happened in 2012 and again in 2016 that worked differently.

2012 Attack – DNSChanger

How Did It Work?

‘DNSChanger’ a trojan by Rove Digital, infected millions of computers between 2007 and 2012.

The trojan was used to divert Web traffic from its intended destination to that of advertisers who paid for traffic delivery—thinking that it was being provided through paid links.

Victims’ computers became infected with the malware when they visited certain websites or downloaded certain software to view videos online.



Vladimir Tsastsin, the CEO of Rove Digital

2012 Attack – DNSChanger

How Did It Work?

The trojan attempted to install drive-by-downloads on users' computers, claiming to be a codec required for watching website video content, especially on rogue websites.

It then redirects its DNS requests to a server and effectively takes control of all of the outbound Internet traffic.

And it attempts to change DNS settings of other uninfected computers on the network that use the Dynamic Host Configuration Protocol (DHCP).

2016 Attack - Stegano

How Did It Work?



From 2014 to 2016, a DNS Changer attack, dubbed 'Stegano', reappeared and was being distributed via advertisements that hide malicious code in image data of advertisements placed on mainstream websites via ad networks using steganography.

This DNS Changer exploit kit, called 'Astrum EK', is unique because the malware in it does not target browsers, rather it targets routers that run unpatched firmware or are secured with weak admin passwords.

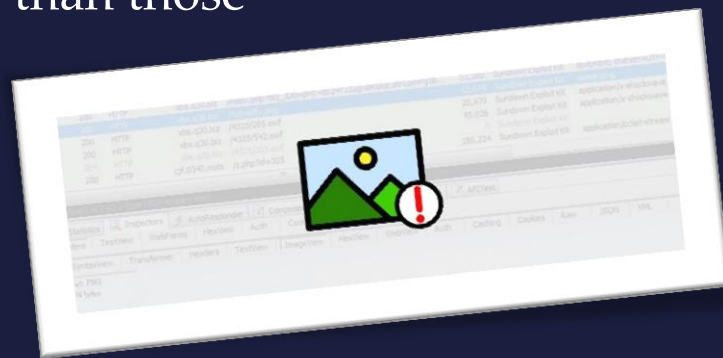
2016 Attack - Stegano

How did it work?

Using Stegano Technique, exploit code bitstream is encoded into lesser significant bits of RGB values.

On clicking the ads, the victims are redirected to web pages hosting the DNS Changer exploit kit which then targets unsecured routers.

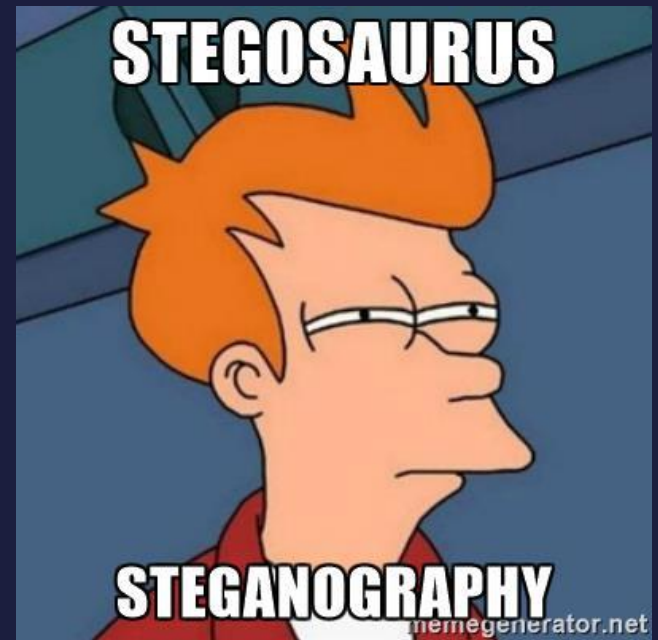
The malware configures itself to use an attacker-controlled DNS server, causing most computers and devices on the network to visit malicious servers, rather than those corresponding to their official domain.

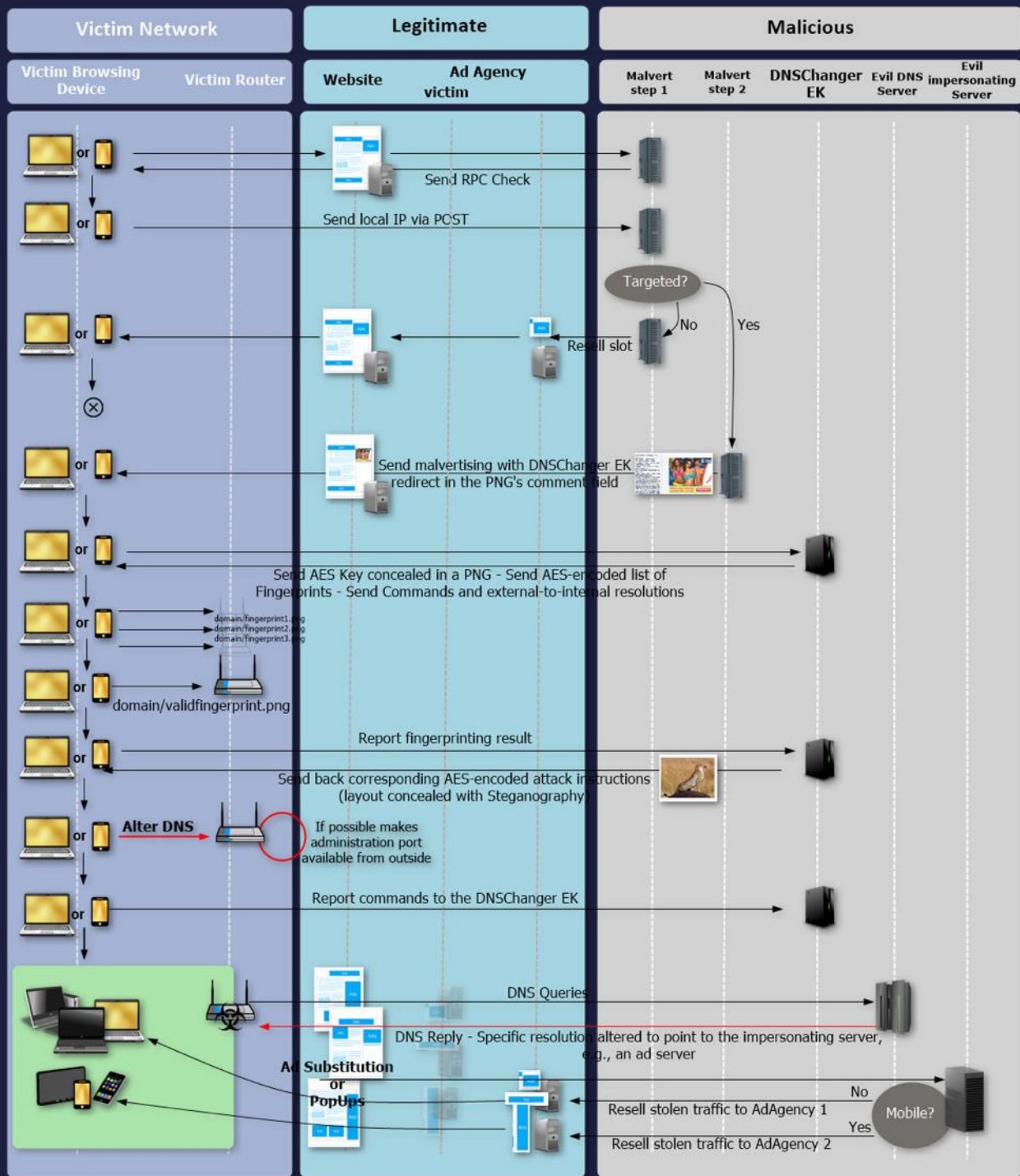


How is Steganography used?

Steganography is used to conceal:

- An AES key to decrypt the list of fingerprints / default credentials and local resolutions.
- The layout for the commands sent to attack the targeted routers.





Why do cybercriminals profit from spreading DNS Changer?

- Infection of connected systems.
- Information theft.
- No control over network traffic.
- Makes systems more vulnerable.
- Attempt man-in-middle attacks.
- Phishing & pharming.



Money makes the cybercriminal world go round

The ultimate goal from most DNS Changer attacks are to redirect the connections to legitimate advertising networks to other bogus networks, forcing browsers to display adverts that criminals can make money off.

Money makes the cybercriminal world go round

Replacing advertising sites:

Legitimate ads on well-known websites such as Amazon.ca, are replaced by foreign ads.

Cybercriminals earn money from ad impressions and clicks off the fake ads, while the legitimate ad owner loses money.



The screenshot shows the Amazon.ca homepage. At the top left is the Amazon logo with 'Try Prime' below it. To the right are links for 'Your Amazon.com', 'Today's Deals', 'Gift Cards', 'Sell', and 'Help'. On the top right, there is a promotional banner for 'All-New kindle paperwhite' with the price 'From \$119' and a link to 'Pre-order now'. A red rectangular box highlights a yellow warning icon with an exclamation mark and the text: 'You need to update your version of media player. [Update now.](#)'. Below this box, on the right, it says 'Ads not by this Site'. At the bottom left, there is a 'Shop by Department' section. In the center is a search bar with 'All' selected and a 'Go' button. On the bottom right, there are links for 'Hello. Sign in Your Account', 'Try Prime', a shopping cart icon with '0' items, and a 'Wish List' link.

Concerns with DNS Changer Attacks

Hijacking search results:

Cybercriminals can lead their victims to any site they wish.

A search engine may not look different for the victim. Victims are redirected to spoof sites even if they use the correct URL.

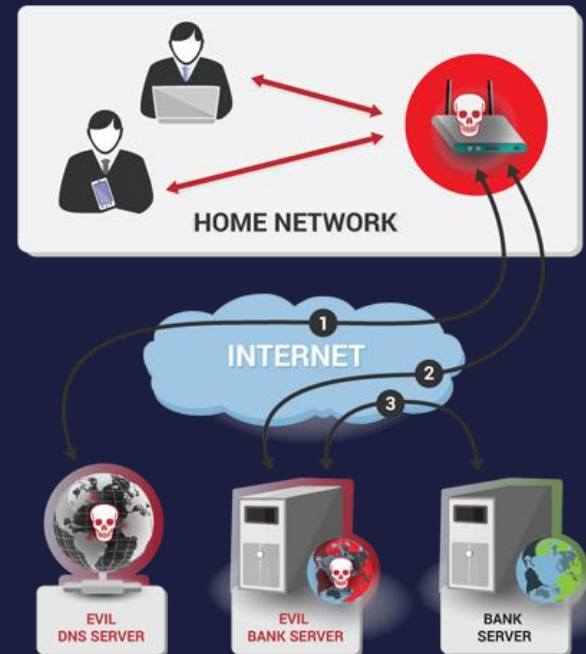


Concerns with DNS Changer Attacks

Infection of connected systems:

Some DNS Changers can alter a routers DNS settings by brute-force.

All systems connected to the router also become infected.

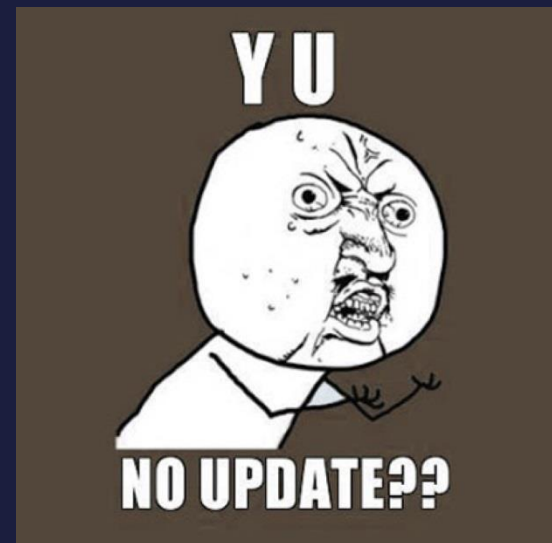


Concerns with DNS Changer Attacks

Disabling of security updates:

Some DNS Changers can disable security updates from downloading.

Infected systems then become more prone to even more infections and become further targets by cybercriminals.



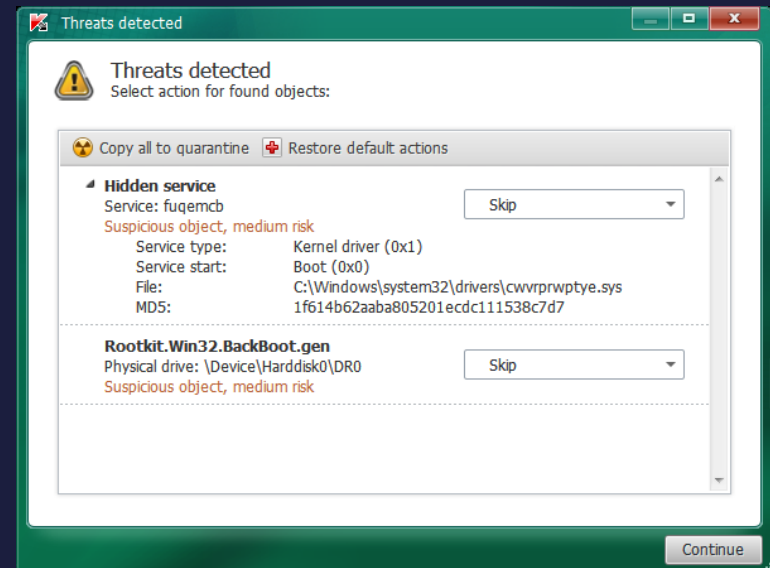
Concerns with DNS Changer Attacks

Rootkit infections:

DNS Changers may have rootkit capabilities.

Makes detection and removal extremely difficult.

DNS Changers will keep modifying the system's DNS settings to will continue to point to different malicious DNS servers.



DNSChanger and Rove Digital

From 2007 to 2001, seven men from Estonia ran an organized cybercrime ring of online web hosting and advertising under the company name Rove Digital.

They successfully infected more than 4 million PCs over 100 different countries with money making malware called 'DNSChanger'.

This 'DNSChanger' replaced legitimate ads and rewarded the revenue to Rove Digital, hijacked referral commissions, prevented security software updates, and blocked users from visiting security websites.

DNSChanger and Rove Digital

Under 'Operation Ghost Click' the FBI determined that Rove Digital made at least US\$14 million from the fraudulent advertising revenue.

This was the largest takedown in history for online crime.

In 2011, the US Attorney for Southern District of New York announced charges against the men for wire fraud, computer intrusion and conspiracy. The men were arrested by Estonian authorities but were acquitted.

In 2014, Estonian Supreme Court revoked that decision finding them guilty of money laundering and the men were extradited to the United States.

DNSChanger and Rove Digital

The ring leader Vladimir Tsastsin was sentenced to 7 years in prison, one year of supervised released and ordered to forfeit US\$2.5 million.

Five men were sentenced to 5 years in prison each.

One man still remains at large.



Stegano and AdGholas

The Stegano exploit kit first appeared in 2014 and was used to target victims in the Netherlands, then in 2015 it moved to the Czech Republic.

The latest attack happened in 2016 that targeted victims in Australia, Canada, Italy, Spain and the UK.

It was estimated that in 2016, it was infecting approximately 1 million people a day.

After further analysis, it was discovered that the gang, AdGholas, were behind the Stegano exploit kits.

Once the attack was discovered, there was a 300% drop in activity by AdGholas, meaning that this criminal gang have gone deep underground, regrouping to make more exploit kits.

Prevention

Make sure your antivirus is up-to-date:

DNS Changers may disable updates to antiviruses on infected machines.

Update your antivirus so that there is a chance that DNS Changers will be detected before it infects your machine.



Prevention

Use ad blockers and script blockers:

Since DNS Changers resides in ads once the machine is infected, using an ad blocker enables so that you will not be redirected to rogue websites if clicked on.

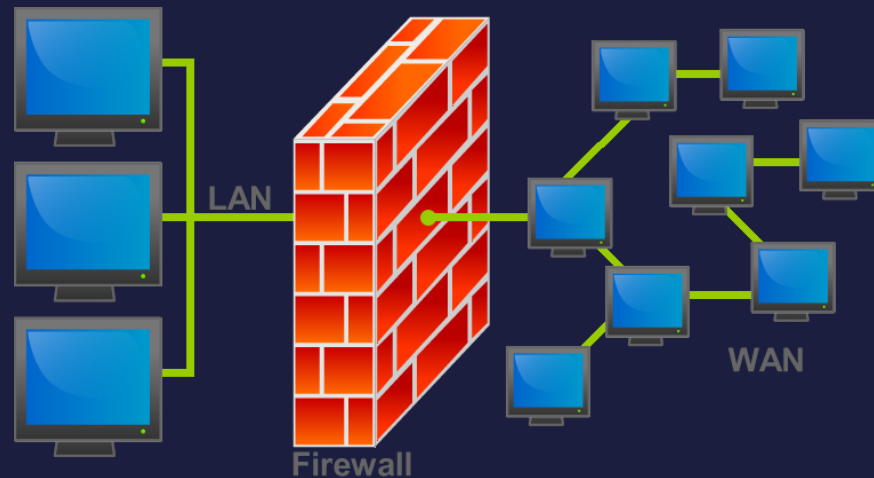
Use a script blocker so that only trusted scripts will run and this will prevent any malicious downloads from popping up.



Prevention

Firewalls:

Enable firewall policies for access to only known good DNS servers so that DNS Changers will be prevented from manipulating DNS servers in your network.



Prevention

Only authorize downloads you trust:

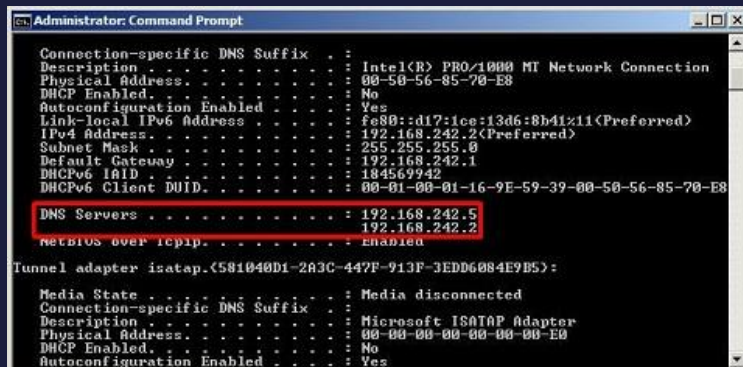
DNS Changers disguises itself as a video codec claiming that it is needed to view the content of the page. Make sure the download is from a trusted source before proceeding.



Prevention

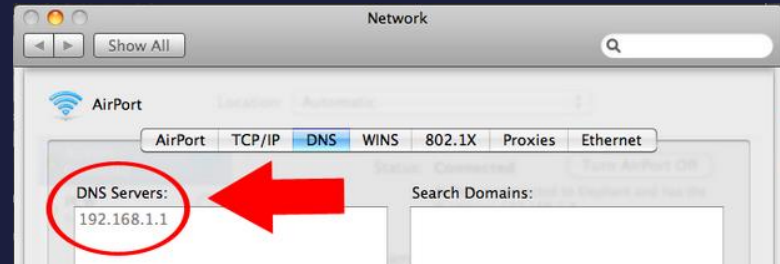
Check if your DNS server addresses are those from your ISP and identify rogue ones:

On Windows, this can be checked with **ipconfig** in the command prompt.



```
Administrator: Command Prompt
Connection-specific DNS Suffix . : Intel(R) PRO/1000 MT Network Connection
Description . . . . . : 
Physical Address . . . . . : 00-50-56-85-70-E8
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d17:1ce:13d6:8b41%11(Preferred)
IPv4 Address. . . . . : 192.168.242.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.242.1
DHCPv6 Iaid . . . . . : 184569942
DHCPv6 Client DUID. . . . . : 00-01-00-01-16-9E-59-39-00-50-56-85-70-E8
DNS Servers . . . . . : 192.168.242.5
                       : 192.168.242.2
netbios over tcpip . . . . . : Enabled
Tunnel adapter isatap.{581040D1-2A3C-447F-913F-3EDD6084E9B5}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

On Mac, DNS servers can be viewed under the advanced network settings.



Prevention

Known rogue DNS servers are:

- 64.28.176.0 through 64.28.191.255
- 67.210.0.0 through 67.210.15.255
- 77.67.83.0 through 77.67.83.255
- 85.255.112.0 through 85.255.127.255
- 93.188.160.0 through 93.188.167.255
- 213.109.64.0 through 213.109.79.255

Prevention

Reset routers to factory settings if you think you were hit by attack:

This will restore the network settings to manufacturer defaults. Be sure to change any passwords as DNS Changers can spread to other machines on the network using default username and password.

May need to reformat drive if the DNS Changer hits rootkit level:

Or alternatively use malware removal tools. TDSSKiller by Kasperkey is an example of one of them.

Questions

1. Which of the following is not a property of a DNS Changer?

- a) It attacks the home WiFi routers of the user
- b) It steers users to unknown sites
- c) It gets a list of running applications from the infected computers
- d) It replaces ads on legitimate websites

2. Why should users be concerned by a DNS Changer attack?

- a) All devices connected to an infected router will also be infected
- b) Disable your antivirus software updates
- c) Rootkit infections make it difficult to remove
- d) All of the above

3. Which of the following is not a way of preventing DNS Changer attacks?

- a) Use of a scriptblocker
- b) Checking your DNS server addresses
- c) Only authorizing downloads you trust
- d) Antivirus

Answers

1. Answer: c

2. Answer: d

3. Answer: b

Sources

- <https://arstechnica.com/security/2016/12/home-routers-under-attack-in-ongoing-malvertisement-blitz/>
- <https://www.bleepingcomputer.com/news/security/steganography-is-very-popular-with-exploit-kits-all-of-a-sudden/>
- <https://conference.hitb.org/hitbsecconf2015ams/wp-content/uploads/2015/02/D1T1-Saumil-Shah-Stegosploit-Hacking-with-Pictures.pdf>
- <https://www.justice.gov/usao-sdny/pr/estonian-cybercriminal-sentenced-infected-4-million-computers-100-countries-malware>
- <https://krebsonsecurity.com/2012/02/half-of-fortune-500s-us-govt-still-infected-with-dnschanger-trojan/>
- <https://networkingexchangeblog.att.com/enterprise-business/8-suggestions-for-mitigating-and-preventing-dnschanger-malware-in-your-enterprise/>
- http://www.pcworld.com/article/255137/protect_yourself_from_dnschanger.html
- <https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices>
- <https://www.proofpoint.com/us/threat-insight/post/massive-adgholas-malvertising-campaigns-use-steganography-and-file-whitelisting-to-hide-in-plain-sight>
- <http://thehackernews.com/2016/12/dnschanger-router-malware.html>

Sources

- https://www.theregister.co.uk/2016/12/20/new_dnschanger_exploit_kit_goes_after_166_types_of_router/
- <https://threatpost.com/where-have-all-the-exploit-kits-gone/124241/>
- <http://blog.trendmicro.com/trendlabs-security-intelligence/dns-changer-malware-sets-sights-on-home-routers/>
- <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/125/how-dns-changer-trojans-direct-users-to-threats>
- <http://blog.trendmicro.com/trendlabs-security-intelligence/esthost-taken-down-biggest-cybercriminal-takedown-in-history/>
- <https://tools.cisco.com/security/center/viewAlert.x?alertId=25595>
- <https://vpn-services.bestreviews.net/dnschanger-attacks-prevent/>
- <https://en.wikipedia.org/wiki/DNSChanger>
- https://en.wikipedia.org/wiki/Rove_Digital