

MALICIOUS REDIRECTION

A Look at DNS-Changing Malware

What are Domain Naming System (DNS)-changing malware? These recently garnered a lot of attention due to the recent Esthost takedown that involved a botnet comprising 4 million DNS-changing-malware-infected systems. The unobtrusive nature of DNS-changing malware allowed the cybercriminals behind Esthost to earn US\$14 million over several years.



The unobtrusive nature of DNS-changing malware allowed the cybercriminals behind Esthost to earn US\$14 million over several years.

THE ESTHOST TAKEDOWN

Esthost was an Estonian company that posed as a web hosting service reseller. In reality, however, it was behind a long-existing botnet that compromised hosts in 100 countries and that earned millions of dollars. The said botnet compromised systems via DNS-changing Trojans.

The DNS-changing Trojans Esthost utilized modified infected systems' settings so these would access foreign DNS servers rather than the ones provided by affected users' ISPs. The rogue DNS servers have been set up by cybercriminals in order to turn certain domains into malicious IP addresses.

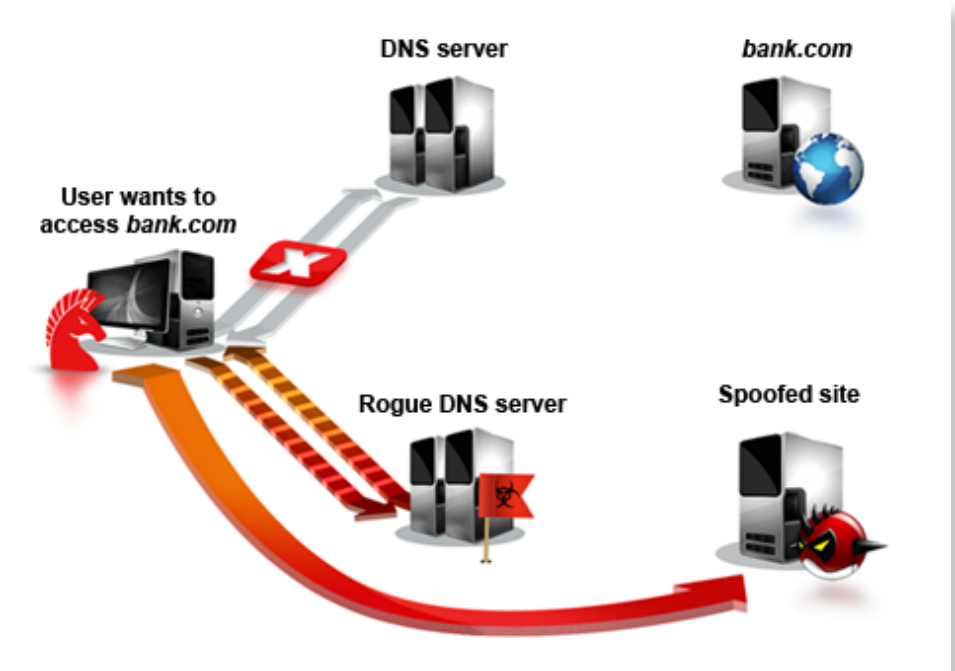
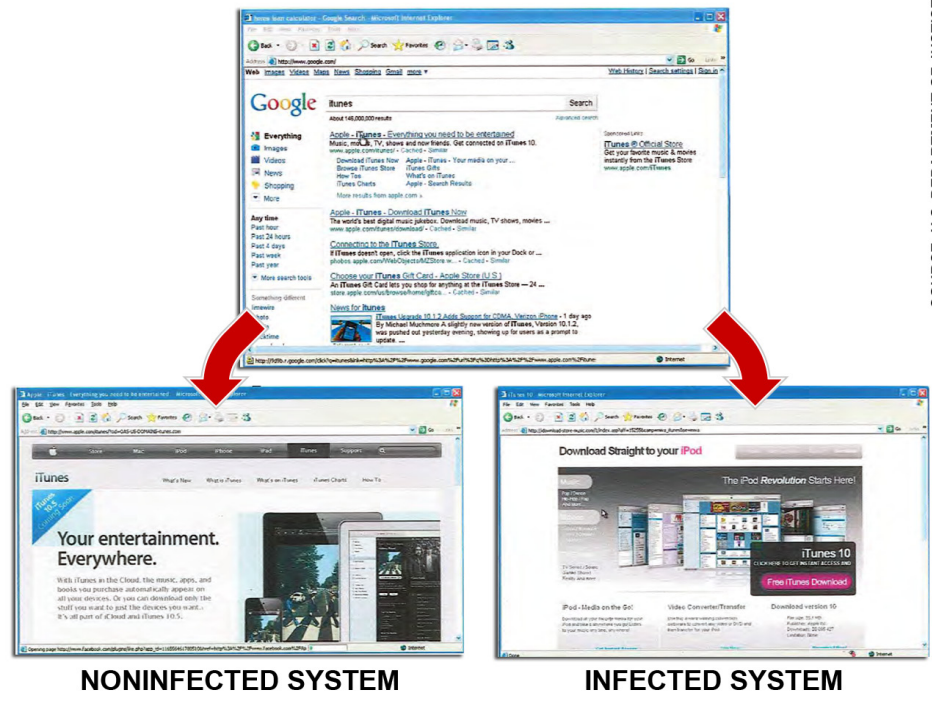


Figure 1. How DNS-changing malware affect systems

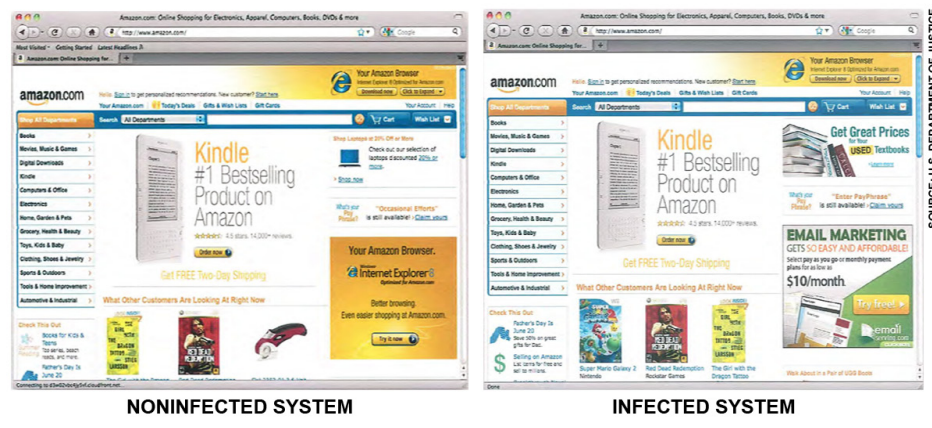
Esthost's botnet victims were unknowingly redirected to possibly malicious sites. Those who clicked a supposed link to Apple's iTunes site (i.e., www.apple.com/itunes/) instead landed on a site with the URL, www.idownload-store-music.com, which was totally non-Apple affiliated but nonetheless claimed to sell the vendor's software.



SOURCE: U.S. DEPARTMENT OF JUSTICE

Figure 2. Comparison of the official Apple iTunes site and the malicious site Esthost victims are led to

Cybercriminals also replaced ads featured in various sites with those of their own choosing. Upon visiting the Amazon site, for instance, users of noninfected systems saw an ad for *Internet Explorer 8* while those of infected systems saw an ad for an email marketing business chosen, of course, by cybercriminals.



SOURCE: U.S. DEPARTMENT OF JUSTICE

Figure 3. Comparison of Amazon ads users of infected and noninfected systems see

BEHIND DNS-CHANGING MALWARE

DNS servers are used to translate human-friendly domain names to PC-friendly IP addresses. These are also used for other purposes, however, such as balancing loads for a single domain across multiple servers.

Most users utilize a DNS server operated by their respective ISPs. They may, however, opt to use a third-party DNS server for different reasons. One reason would be for speed, as ISP-operated DNS servers can be slow or unreliable. Some users prefer third-party DNS servers for security reasons, as some third-party services filter certain content (e.g., ad, adult, and malware-laden sites) they may be interested in.

Utilizing third-party DNS servers may also allow users to evade censorship, especially in countries where these are strictly controlled by the state.



What Do DNS-Changing Malware Do?

Having control over a system's DNS settings allows one to decide where all of a user's network traffic will go. It is, therefore, not surprising why cybercriminals have been known to use DNS-changing malware for their malicious schemes.

Because DNS-changing malware can control and redirect a user's network traffic, cybercriminals can use them as "defense mechanisms," as these can block access to *Windows Update* and security software domains. These can also be used to stage "perfect" phishing attacks. In fact, users can type the correct domain name but still be directed to a phishing site from which their credentials can be stolen.

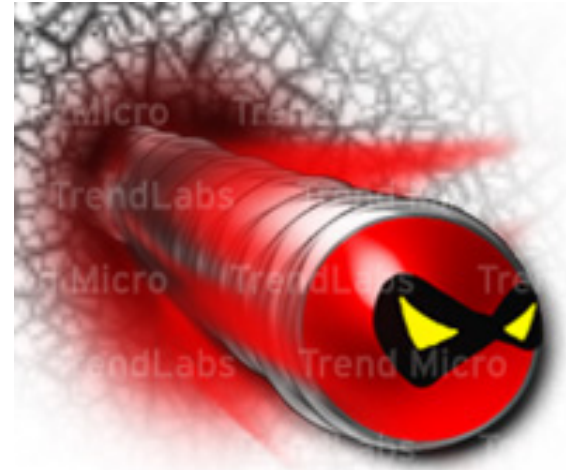
DNS-Changing Malware Over Time

Over the years, we have come across a slew of DNS-changing malware. In one instance, we came across a DNS-changing Trojan that posed as a *MacCinema installer*. Users were lured into downloading the malware with the promise of being able to view certain videos posted online. Aside from changing affected users' DNS settings, the said Trojan also had components that allowed cybercriminals to monitor their victims' online activities. Another DNS-changing Mac malware posed as pirated versions of *Foxit Reader* and various antivirus applications.

While the given instances involved software updates and applications, cybercriminals also take advantage of popular events to spread DNS-changing Trojans. Trend Micro researchers, in fact, spotted an instance wherein cybercriminals rode on the release of *Mac OS X Snow Leopard* to spread DNS-changing malware. Note, however, that DNS-changing malware can infect systems running other OSs as well.

The Malware Connection

DNS-changing malware are usual payloads of other malware, too. In fact, TDL4—a recent iteration of TDSS—has code that turns infected systems into DHCP servers whose DNS settings directed users to malicious IP addresses. Once this rogue DHCP server connects to a LAN, it causes other computers in the network to use the rogue DHCP instead of the legitimate server. As a result, the computers are directed to malicious IP addresses that ultimately lead to TDL4 binary downloads.



KOOBFACE variants, which rampantly spread via social networking sites, also had DNS-changing malware as possible payloads. In this kind of ruse, social networking posts/messages may contain links to fake videos that really lead to the installation of KOOBFACE malware components, some of which may be rogue DNS changers.

Cybercriminal Earnings from DNS Changers

DNS-changing malware help cybercriminals profit. The official U.S. legal indictment filed against Esthost, for instance, states that the group took on advertising contracts from which they made money in exchange for user ad clicks and for the display of ads on certain sites. The same document revealed that the arrangement was not limited to advertising fraud, as the cybercriminals also hijacked clicks from search engine results pages.

Trend Micro research revealed that aside from the activities specified in the indictment, Esthost also spread other malware, typically FAKEAV variants. This was another way by which the group made money from users who have been tricked into purchasing rogue antivirus software.

ADVERSE EFFECTS OF DNS CHANGERS

The most obvious effect of DNS-changing malware to users would be loss of control over network traffic. DNS-changing-malware-infected systems can cause victims to be redirected to any site of the cybercriminals' choosing. This control makes DNS changers a perfect phishing or pharming tool in that even if users type the legitimate URLs of the sites they wish to visit, they can still be redirected to a spoofed site, which allow cybercriminals to obtain their credentials.

Even more troubling, however, is the fact that DNS changers can not only affect individual users, these can cause damage to entire networks as well. As has been said earlier, some DNS-changing Trojans can change routers' DNS settings via brute-force attacks. As a result, all systems connected to that "infected" router can suffer dire consequences. Some DNS-changing malware can also be used to set up rogue DHCP servers on certain networks, which can have the same effects.

Since DNS-changing malware can prevent access to security vendors' and application security update sites, infected systems become more prone to infection. More malware can thus end up in already-infected systems, which can open up systems and networks to more cybercriminal activities.

Stealthy by Design

DNS-changing malware are designed to remain unobtrusive. These usually come with rootkit capabilities that make them even harder to detect and remove. These difficulties, in turn, make restoration of ISPs' DNS settings harder to do. As long as the malware remain undetected, these will simply just keep restoring infected systems' DNS settings to point to rogue DNS servers.

Esthost's case proved that using DNS-changing malware can be very profitable. It is thus safe to assume that we will continue to see more of DNS-changing malware in the future.



EVADING DNS CHANGERS

Given that DNS-changing malware often come with malicious packages or as other malware's payloads, users are advised to avoid downloading and installing files from unfamiliar sites. They should routinely patch their systems, OS, and applications in order as protection from vulnerability exploitation.

Since DNS-changing malware can also affect routers, it would be prudent for users to change their routers' default user names and passwords. As additional precaution, they should invest in a security solution that protects their systems/networks from all kinds of threats. Staying abreast of the latest news and updates in the threat landscape is also a must. Doing so better equips users to deal with potential computing problems.

REFERENCES

- Bernadette Irinco. (August 26, 2009). *TrendLabs Malware Blog*. "Bogus Snow Leopard Update Sites Lead to DNS Changers." <http://blog.trendmicro.com/bogus-snow-leopard-update-sites-lead-to-dns-changers/> (Retrieved December 2011).
- Det Caraig. (August 11, 2009). *TrendLabs Malware Blog*. "Mac OS X DNS-Changing Trojan in the Wild." <http://blog.trendmicro.com/mac-os-x-dns-changing-trojan-in-the-wild/> (Retrieved December 2011).
- Feike Hacquebord. (November 9, 2011). *TrendLabs Malware Blog*. "Esthost Taken Down—Biggest Cybercriminal Takedown in History." <http://blog.trendmicro.com/esthost-taken-down---biggest-cybercriminal-takedown-in-history/> (Retrieved December 2011).
- Jonathan Leopando. (August 23, 2009). *TrendLabs Malware Blog*. "More Mac Malware in the Wild." <http://blog.trendmicro.com/more-mac-malware-in-the-wild/> (Retrieved December 2011).
- Jonell Baltazar, Joey Costoya, and Ryan Flores. (July 2009). *TrendWatch*. "The Real Face of KOOFACE: The Largest Web 2.0 Botnet Explained." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf (Retrieved December 2011).
- Roland Dela Paz. (June 8, 2011). *TrendLabs Malware Blog*. "The Worm, the Rogue DHCP, and TDL4." <http://blog.trendmicro.com/the-worm-the-rogue-dhcp-and-tdl4/> (Retrieved December 2011).
- Trend Micro, Incorporated. (August 2009). *Threat Encyclopedia*. "OSX_JAHLAV.D." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=OSX_JAHLAV.D (Retrieved December 2011).
- Trend Micro Threat Research. (August 2009). *TrendWatch*. "A Cybercrime Hub." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/a_cybercrime_hub.pdf (Retrieved December 2011).
- United States District Court, Southern District of New York. (2011). *The United States Department of Justice*. "United States of America Versus Vladimir Tsastsin, Andrey Taame, Timur Gerassimenko, Dmitri Jegorov, Valeri Aleksejev, Konstantin Poltev, and Anton Ivanov." <http://www.justice.gov/usao/nys/vladimirtsastsin/rovedigitalindictment.pdf> (Retrieved December 2011).