ANCHOR intelligence

Traffic Quality Solutions

THE UNINVITED GUEST
A Browser Hijacking Experience, Dissected

Sponsored by

looksmart
Smart Choices. Made Easy.

Technorati™

GenieKnows Media
search marketing solutions

INTRODUCTION

The continued growth of the Internet and online advertising has created an appealing medium through which fraudsters distribute malware and perpetrate a wide range of malicious activities. Over the past six months, Anchor Intelligence has identified a surge in browser hijacking attacks perpetrated through online advertising campaigns. These compromised ads, found on various ad networks and search engines, have been traced to schemes designed to defraud unsuspecting users by capturing their credit card information and account passwords, forcing ad clicks without users' consent, and manipulating personal data such as cookies.

By targeting the browser, a user's primary gateway to the Internet, browser-hijacking malware has emerged as one of the most powerful and dangerous online exploits. The hijacker is an uninvited guest, which sits dormant in the background of the user's experience, looking over her shoulder to log each keystroke as she enters her bank password, redirect her to malicious websites when she expects to see search results pages, or simply leverage her browser to make http requests unbeknownst to her.

In response to the explosion of browser hijacking exploits identified across its network, Anchor Intelligence is issuing "The Uninvited Guest: A Browser Hijacking Experience, Dissected" to educate end users, ad buyers, and ad sellers about how to recognize and avoid common tactics used by fraudsters to compromise their systems. Section I of the report provides background on browser hijacking and describes infection vectors, payloads, and attacks. Section II breaks down the infection experience of a clean browser and shows exactly what happens once that browser has been hijacked. The browser hijacking experience dissected in this Report is launched from a site: clean_pc_now.biz ("_" characters have been used to replace "-" in order to avoid accidental redirects to the malicious site). Section III provides tips and trends to help readers avoid browser hijacking in the future.

SECTION 1: BACKGROUND

Browser Hijacking

A browser hijacker is a type of malware that lurks in the browser and changes how and what a browser displays while a user is on the Web. Browser hijackers can modify any content that flows through the browser such as default home pages, search pages, search results pages, or error pages of unwitting users whose computers have been infected. Browser hijackers can also change browser favorites settings and make registry changes to prevent users' from resetting their browser's homepage. The pages to which the browser hijacker directs users may include websites of publishers who are serving advertisements and looking to benefit from click fraud, or even websites of advertisers who are interested in acquiring "new users" in order to boost site traffic metrics. The same malware used to hijack browsers can also add/read cookies, collect personal information such as login credentials and passwords, record the web pages a user visits, and lower security settings before sending users to malicious Web pages. Browser hijackers are installed without explicit user consent and are frequently programmed to resist removal. Like all forms of malware, browser hijackers are infection payloads that are generally transmitted online.

Infection Vectors

Perpetrators commonly install malware on a user's computer by compromising websites. Websites can be compromised by manipulation of the content delivery methods (such as the server or scripts), the actual website content, or the advertisements shown[1]. This section examines the advertising infection vector in detail. As ad networks and exchanges open up their platforms and increasingly provide advertisers with end-to-end control over their creatives, online advertising will continue to grow as a malware distribution channel.

Advertising

One medium fraudsters are increasingly using to distribute malware is online advertising, or malvertising. Ad networks and search engines provide ad code to publishers to insert within their web pages so that they can start serving ads. For example, a blogger who is interested in serving ads on her blog can simply sign up with an ad network or search engine as a publisher. Upon acceptance into the program, she will receive a snippet of code to append to her website template. Shortly thereafter, ads will begin to appear on her blog. These ads can be used to distribute malware in various ways.

First, the ads can link directly to websites that attempt to download malicious code onto a user's computer or offer free downloads of software that has been infected. In this case, the advertiser who has signed up with the ad provider is likely the perpetrator who is looking to distribute malware. For example, fraudsters created a fraudulent AdWords campaign earlier this year in which they advertised their malware-infected copy of WinRAR[2].

The advertisements themselves can also be used to infect an unsuspecting user's computer. Ad creatives that are managed in-house by the advertiser and served to an ad network or publisher via an API are especially vulnerable to these types of attacks. One such example is ads served via widgets. A widget is an embedded link to an external HTML, JavaScript, or iframe that can be used for additional functionality, such as displaying dynamic content. Widgets are often used to distribute malware on social networking sites. For instance, the "Secret Crush" widget, which appeared on Facebook last year, was a social worm that spread through social engineering, by prompting users to unwittingly download an adware application[3].

As many publishers, ad networks, and search engines have stepped up their efforts to screen for malicious content, attackers have begun to use increasingly sophisticated tactics to avoid detection. For instance, some attackers upload innocuous ads at the start of a campaign and replace them with malvertisements following approval of the original ad by the network. Meanwhile, syndication – a common practice, which allows ad networks to sell their inventory to one or more other ad networks – forces networks to rely on partner networks to screen and remove malicious ads. So if an attacker successfully places a malvertisement in one network, that ad may be routed to a different ad network and reach yet more publisher sites. In other words, the number of infection vectors through which malware writers can reach users increases in the syndication process. As online ad syndication and ad exchanges grow in popularity and use, malvertisements will continue to be a significant infection vector for browser hijacking software.

[1] Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Want and Nagendra Modadugu, "The Ghost In The Browser: Analysis of Web-based Malware," Google, Inc. April 2007.
[2] Dancho Danchev, "Malware-infected WinRAR distributed through Google AdWords," ZDNet 20 January 2009. <http://blogs.zdnet.com/security/?p=2405>.
[3] Dan Kaplan, "Facebook widget leads to adware install," SC Magazine 7 January 2008. <http://www.securecomputing.net.au/News/100360,facebook-widget-leads-to-adware-install.aspx>

The most recent example of browser hijacker distribution through advertising occurred on NYTimes.com. The Times inadvertently hosted a malicious ad, which generated a pop-up window that purported to perform a scan of the visitor's computer for viruses. The pop-up then claimed that the visitor's computer was infected with malware and directed the visitor to a site that purported to offer antivirus software. This software, which was supposed to eliminate the supposed infection, was itself a virus. The malvertiser posed as Vonage, a recurring advertiser on NYTimes.com, and paid the Times to display its ads, which appeared to be legitimate Vonage ads. Over the September 25 weekend, the malvertiser swapped the Vonage ads for the malicious pop-up ad. Fortunately, readers informed NYTimes.com about the problem and they swiftly responded by removing the ad[4].

Figure 1. The fake anti-virus pop-up on NYTimes.com, courtesy of www.NYTimes.com.[5]

Browser Hijacker Installation

After a malvertisement has been served, malware is typically installed in one of two ways: drive-by-downloads or social engineering. Drive-by-downloads automatically install malware on a user's computer when a user visits a web page, unbeknownst to him/her. Social engineering, on the other hand, involves manipulating users into performing a specific action – in this case, downloading an application that has been infected.

Once the install initiates, the user's browser and plug-ins are analyzed for vulnerabilities to determine which exploits stand the highest chance of success. The appropriate exploit is then delivered to that visitor. After the vulnerability has been successfully exploited, the browser hijacker is downloaded and installed on the victim's computer.

[4] Ashlee Vance, "Times Web Ads Show Security Breach," NYTimes.com 14, September, 2009. <http://www.nytimes.com/2009/09/15/technology/internet/15adco.html?_r=1>
[5] Ibid.

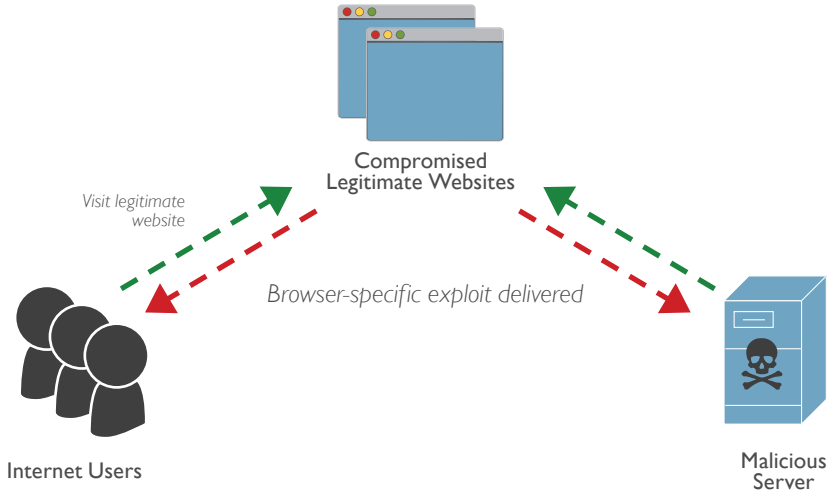


Figure 2. Browser hijacker initiation and installation.

Exploits are typically delivered only once to each user. Malware distributors have built sophisticated distribution toolkits to maximize success and avoid detection. Toolkits track the success rates for each exploit and the frequency with which specific browser types have been exploited. The geographical location of the users is also sometimes determined to limit fraud to particular regions.[6]

SECTION II: THE CLEAN_PC_NOW. BIZ BROWSER HIJACKER

Anchor Intelligence has observed an upswell in browser hijacking cases across its network in the past six months, the vast majority of which have been distributed directly through malicious online ads. ClearMark, Anchor's real-time traffic scoring system, has identified publisher sites that are directly associated with browser hijacking infections. Many of these sites have been identified through associational analysis, which identifies large-scale, coordinated click fraud by multiple publishers, including click fraud rings. Anchor Intelligence defines a click fraud ring as a group of individuals who generate fraudulent traffic on a portfolio of publisher sites in order to benefit from ad click revenue. One of the most widely distributed browser hijackers associated with several click fraud rings is clean_pc_now.biz. Anchor Intelligence has successfully reproduced the infection experience for the clean_pc_now.biz browser hijacker; the following dissects the experience from initial exposure to full-blown infection.

[6] Christoph Alme, "Web Browsers: An Emerging Platform Under Attack," McAfee, Inc. June 2009.

While reviewing publisher sites within a large-scale click fraud ring, which Anchor Intelligence exposed and shut down, Anchor analysts identified ringtonescatalogs.net, a distribution agent for clean_pc_now.biz, a commonly known browser hijacker. Ringtonescatalogs.net served multiple text ads on its site, one of which was a purported Microsoft ad for Antivirus software. It is unclear whether or not ringtonescatalogs.net knowingly served these malicious ads to its visitors. It is possible that the website had no direct relationship to the actual advertiser; however, given how consistently the same ads showed up on the site, Anchor Intelligence believes there was some suspicious connection between the advertiser behind these malicious ads and the website.

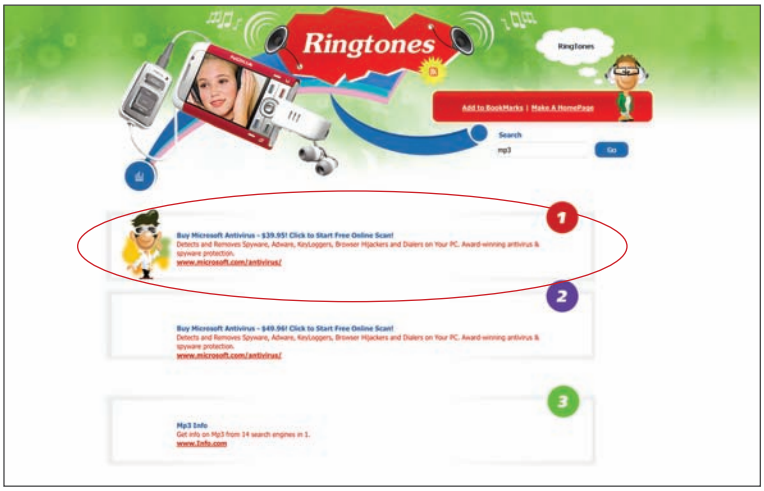


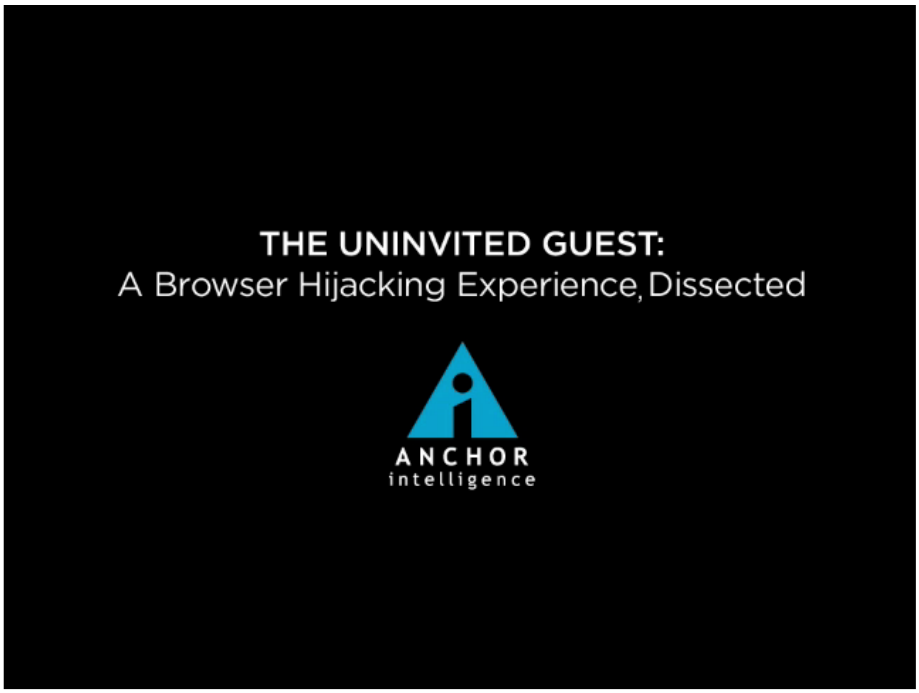
Figure 3. Screenshot of ringtonescatalogs.net with malicious ads purporting to send users to www.microsoft.com/antivirus/.

Clicking on the malicious antivirus ad launched a faux My Computer Explorer Window displaying a fake online security scanner. The "scan" returned several mocked up Windows security alerts stating that the computer was strongly infected with viruses and prompted the user to download a purported Microsoft product, Total Security. This social engineering trick enabled a drive-by-download of a browser hijacker.

Once the Total Security software package was downloaded and installed, the browser hijacking software gained control of the computer, becoming the uninvited guest. Following this infection, the browser exhibited very strange behavior. For example, when the Anchor security analysts attempted to visit Google, they received an "Access denied" error message. This is often done by the hijacker modifying entries to the computer's HOSTS file, which directly maps DNS addresses (web URLs) to IP addresses, on the compromised computer. When the analysts typed in Google.com, the computer was likely directed to the IP address of a mocked-up site displaying the "Access denied" message instead.

After refreshing the browser, they were able to access Google, but their attempt to enter a search query was also denied. On the access-denied page, the browser hijacker continued to encourage users to complete another scan. This action took them to the Total Security application, which requires that users subscribe to its service for a fee by submitting their credit card information. Not only did the pop-up ad facilitate a drive-by-download; it also used social engineering to encourage users to provide their personal information for malicious use.

In sum, the clean_pc_now.biz is a powerful browser hijacker that leverages users' trust in Microsoft and their ignorance of malware to infect computers with the Total Security rogue anti-spyware and collect their personal information. The following video walks through the actual infection by the clean_pc_now.biz browser hijacking malware as observed and recorded by Anchor Intelligence:



If the video does not load, you can view it here.

SECTION III: TIPS & TRENDS

While browser hijackers can be difficult to detect, users can take precautionary measures to prevent them from being executed onto their computers in the first place. Anchor recommends the following:

1. ***Keep up-to-date with updates:*** Drive-by-download exploits are a purely technical attack. In order to eliminate known vulnerabilities, you should stay current with patches and anti-malware updates for your operating system, browsers, and other software.

2. *Use anti-virus programs regularly:* Not only is it important to use an anti-virus program but it is a good idea to enable the "auto protection" mode which constantly scans information entering and leaving your computer.

3. *Beware of plug-ins from unknown sources:* Browser plug-ins are one of the most common targets for exploitation. When you visit a site, you may be asked by your browser to install a missing plug-in in order to view some interactive content. Be cautious! Malicious websites may be using this as a social engineering trick. For instance, websites and advertisements peddling graphic content sometime trick visitors into downloading a "missing" video codec in order to watch their videos. Before downloading the plug-in, we suggest that you do some research online to see whether the missing plug-in is actually missing.

4. *The internet can be your friend:* When in doubt about a particular plug-in or application that prompts you to install, look up the name in conjunction with other keywords such as "malware," "adware," "virus," "trojan," or "block." If the plug-in or application is in fact a known suspicious program, there is a chance someone has already recognized it and posted important information on a bulletin board or blog. Social engineering attacks will not work if you stay informed.

5. *Give browser hijackers the boot:* In the event that your browser has been hijacked, know that there are ways to remove the malware. In particular, try to find a reputable anti-spyware tool. Anti-spyware programs are similar to antivirus products in their scanning methods, however they have parasite signature databases that antivirus products may lack. As a result, anti-spyware tools can detect and eliminate most browser hijackers and other forms of malware.

CONCLUSION

Anchor Intelligence predicts that browser hijacking infections over the next two years will continue to grow as online advertising grows and perpetrators increasingly use advertising as their primary infection vector. Browser hijacking attacks over the past six months have surged, and the tactics used to distribute these infections have also evolved at an impressive rate. Browser hijackers are exploiting trusted brands such as Vonage and Microsoft to disguise their malicious intentions. By issuing "The Uninvited Guest: A Browser Hijacking Experience, Dissected," Anchor Intelligence aims to arm end users, ad buyers, and ad sellers with the necessary tools to avoid victimization by this emerging threat.

ABOUT THE SPONSORS

looksmart

www.looksmart.com
625 Second Street
San Francisco, CA 94107

LookSmart is a trusted provider of pay-per-click text advertising with 13 years experience and over a billion daily queries on its network of quality partners. LookSmart uses Anchor Intelligence's ClearMark traffic scoring system across the network to enhance its ability to safeguard advertisers and partners against illegitimate or fraudulent traffic and further improve advertiser ROI through the enhanced performance. LookSmart has provided insights based on historical experience with publishers, advertisers, and other partners that helped shape the content of this report.

Technorati™

www.technorati.com
665 3rd Street, Suite 207
San Francisco, CA 94107

Technorati is a search engine service launched in June 2002 by founding CEO Dave Silfry. The service allows you to find the most relevant results on all media including blogs, photos, videos and audio files. Technorati used to focus solely on blog search results but have opened up to all media given that more mainstream users are using its service.

GenieKnows Media

www.genieknows.com
1567 Argyle Street
Halifax NS B3J 2B2
CANADA

GenieKnows connects search technology, community and content by developing niche-specific portals tailored for distinct searching communities, delivering a focused, useful and rewarding search experience. GenieKnows also empowers a broad distribution network for advertisers, helping businesses connect with consumers and grow their bottom line by conveying meaningful, revenue-generating search results. As the world enters a dynamic new era in Internet technology and online marketing, GenieKnows' industry-leading search technology continues to provide innovative products and solutions to meet the ever-changing needs of the IT industry.

www.anchorintelligence.com
480 San Antonio Road, Suite 235
Mountain View, CA 94040

Anchor Intelligence Inc., headquartered in Mountain View, CA, is the traffic quality solutions provider of choice among ad networks, search engines, and advertisers from across the globe. Using Anchor Intelligence's ClearMark, the industry's first and only real-time traffic scoring system, industry players obtain the necessary intelligence to fight click and impression fraud, efficiently manage traffic sources, and capitalize on high quality clicks while maximizing advertiser ROI. For more information, visit: www.anchorintelligence.com. Follow us on Twitter: @AnchorIntel.