Ongoing IFrame attack proving difficult to kill

By Joel Hruska | Published: March 18, 2008 - 05:04AM CT

One of the factors that make an ongoing malware attack so difficult to stop is the speed with which the assault can evolve. Over the past 12 days, an IFrame injection attack that originally focused on ZDNet Asia has been spreading across the 'Net, changing targets and payloads on an almost daily basis. An iFrame (short for inline frame) is an element of HTML that's used to embed HTML from another source into a webpage. The timeline of the attack is provided below, thanks in no small part to security consultant Dancho Danchev, who has kept a play-by-play account of the IFrame attack on his blog.

This particular IFrame exploit takes advantage of web site query caching. Web sites often cache the results of search queries that are run locally. These search results are forwarded to search engine providers (think Google or Yahoo), who use the information to generate their own search results. Hackers exploit the system by typing a query immediately followed by the text of an IFrame. This data (including the IFrame) is then passed to various search engines and displayed if a user searches for a relevant keyword. When the user visits an apparently legitimate document, the IFrame activates and attempts to complete whatever instructions it has been given.

The major advantage of an injected attack versus an embedded one is that an injected attack requires no direct access to a web site's server backend. Instead, it takes advantage of the company's SEO (Search Engine Optimization) practices and poisons the results that are fed back to web surfers. The first wave of injections targeted ZDNet Asia and torrentreactor.net. The attackers shifted away from these two domains quickly and branched out into other web sites. One key purpose of the attack was to advertise the rogue antivirus product developed by the RBN (Russian Business Network), XP Antivirus.

XP Antivirus is a cute piece of work. On the surface, it seems to be an ordinary anti-virus program, and it makes all the usual claims one would expect regarding its ability to keep a system clean and virus free. Once installed, however, XP Antivirus actually *creates* a set of registry keys that it will detect and flag as malware installations once a scan is run. The only way to remove these threats from the system, of course, is to buy the XP Antivirus software package. Additional IFrame were eventually added that pointed to downloads for Spyshredderscanner and MediaTubeCodec, both of which attempt to download additional malware into a system.

On Friday, March 6, ZDNet Asia activated an input validation system to prevent hackers from continuing to inject IFrames into its cached search results. The term "input validation" is self-explanatory—under such a system, all application input is validated before it's used by any sort of application. Input validation is recommended in virtually any application, but the actual implementation of it is handled by developers. ZDNet Asia deserves credit for locking the attack vector within 48 hours, but it could have been closed from the start.

With one loophole closed, the perpetrators found others, launching attacks on both Wired.com and History.com as well as a smattering of other domain names. The methodology of this new attack wave was essentially identical to the old, save that more domains were introduced and the malware payload was different than before.

As of Wednesday, March 12, the attack had continued to spread across additional domains including Boise State, the Internet Archive, the University of Vermont, and Medicare.gov. The payload, meanwhile, had shifted yet again—in this case, those performing Internet searches were being directed to the radt.info website. Once there, the site prompted for a codec install (democodec1292.exe), and installed a variant of Zlob. Zlob itself is a popular trojan, and a number of variants of it have been tracked in the field, including some that install rogue DNS information.

The man network behind the curtain

The launchpad for these various malware campaigns is our old friend, the Russian Business Network. According to Danchev, earlier reports of the network's demise have been greatly exaggerated. Faced with dwindling functionality thanks to security policies that prevented traffic from reaching IP addresses associated with the RBN, the company divided itself, sought new service providers, and is back in business. Many of the codec downloads and false website fronts active in the above attacks trace directly back to RBN addresses.

The rapidity of the payload shifts is explained by the economic nature of the RBN. In this case, the Russian Business Network is probably selling spammers the network capacity and product exposure they need to fence their services or goods. In some cases, the "goods" in question might be an adware trojan that the "customer" downloads and installs, but the basic business principle remains the same. The size and scope of the RBN means that its client base is probably large and diversified, which can lead to any number of attacks flowing out of the network at any given time.

It could be awhile before this particular IFrame campaign is driven off, but the longer-term impact should be minimal. Although persistent and potentially damaging to a site's reputation, the attack vector for this IFrame

exploit can be closed by enabling input validation, a security practice that is already recommended. The fact that no attack actually took place on a company's physical service makes it easy to clean up the damage; the hard part will be to regain the trust of readers and visitors who visited sites in search of valid information and got handed a cuckoo's egg instead.