Why Hackers have turned to Malicious JavaScript Attacks

Website attacks have become a serious business proposition. In the past, hackers may have infected websites to gain notoriety or just to prove they could—but today, it's all about the money. Reaching unsuspecting users through the web is easy and effective.

Hackers now use sophisticated techniques—like injecting inline JavaScript—to spread malware through the web.

Learn about the threat of malicious JavaScript attacks, and how they work. Understand how cybercriminals make money with these types of attacks and why IT managers should be vigilant.

A sophos whitepaper – December 2010

How Cybercriminals Reach You via the Web

These days nearly all organizations have email protection, which makes it harder to deliver malware via email. That's why cybercriminals now leverage the web as a vehicle to deliver malicious content. SophosLabs reports 50,000 newly infected web pages every day.

The web is appealing to malware authors and is an increasing threat for three key reasons:

- It's easy to reach you—threats are everywhere people visit on the internet.
- It's easy to infect you—people and systems are vulnerable.
- Traditional defenses are failing—proper protection against modern web attacks requires a new approach.

When browsing the web, we may think that the sites of big companies and respected brands are relatively safe. However, statistics on internet crime prove that is not the case. In fact, approximately one in every 150 legitimate sites is infected by malware. And, of all the malware-infected web pages, over 80% are on legitimate websites.

There are certain myths among users about vulnerability to viruses. Even technical computer users hold onto these rules, thinking that if they're followed, their computers won't become infected. Some of these myths include:

- Only naïve users get infected.
- You can only get infected if you download files.
- Only porn, gambling and other questionable sites are dangerous.
- You need to click on a bad link to get infected.

Of course, staying off questionable sites and not downloading files or clicking on links from unknown sources is good practice. But, it's not just the obscure corners of the web that fall victim and open us up to infection. Some of the world's most popular brands have had their websites taken over to serve malware or redirect to other malicious URLs, including the websites of some leading security companies.

Understanding how Malicious JavaScript is Used: A "Drive-by Download"

JavaScript is used as a vehicle to infect websites because it's a programming language that underpins today's web. It's primarily used in the form of client-side JavaScript, implemented as part of a web browser in order to provide enhanced user interfaces and dynamic websites. With today's Web 2.0 functionality, browsing the web without JavaScript support is no longer a realistic option.

Malware authors take advantage of this fact. They compromise popular, high-traffic, legitimate websites and redirect users to malicious web pages without the victim's knowledge. This kick starts the infection process, and when people visit these malicious sites, further scripts exploit client-side vulnerabilities.

The use of injected, inline JavaScript is a way to hide the redirect more effectively than with simpler attack methods, such as simple iframe attacks. Malicious JavaScript attacks have grown significantly over the past three to four years and virtually all attacks include it, but today's attacks are more complex.

Delivering malware via the web is now the cybercriminal's favored means of attack, resulting in a newly infected website discovered every few seconds. Injecting malicious JavaScript into legitimate web pages allows hackers to silently redirect the victim's browser to load content and malware from a remote server. This so called "drive-by download" has created a number of security challenges for organizations and end users alike.

How Hackers use Malicious JavaScript

So, how does a malicious JavaScript attack work?

- First, hackers inject code into legitimate web pages. The injected code could be an iframe HTML element, or an inline script. The trend is a move towards the latter.
- When the victim browses the compromised web page, the injected code will cause their browser to silently load malicious content from another, remote site. This is invisible to the victim.
- Typically, the content loaded will consist of multiple components designed to exploit client-side vulnerabilities. For example, a mixture of HTML, JavaScript, Flash, PDF and Java content. This bundle is typically produced by and managed with a kit, known as an exploit pack.
- These exploit packs are written and sold to criminals looking to infect users with malware.

The important thing to note is that there is no social engineering required. The user does not have to click on a link in an email, or browse potentially risky web pages. They just need to visit a legitimate website that's been compromised.

Users visiting a hijacked site have no way of knowing the site has been compromised because the malicious code is invisible, and is executed as soon as the page loads in the user's browser. The code typically uses further scripts to fetch more malicious components, which will then attempt to leverage known exploits in the browser or operating system to infect it, steal data, or subvert it into a botnet.

The scope of these attacks cannot be underestimated, since all types of sites—from government websites to educational institutions to popular news portals, blogs and social networking sites—have been targeted.

As security vendors add detection for malicious web code, the attackers constantly evolve it in order to evade being caught. Hackers have turned to using JavaScript as the "glue" for these web attacks because it provides the ability to hide or obfuscate the code, concealing the payload.

What About Attacks Against SEO?

Search Engine Optimization (SEO) attacks are another way in which cybercriminals use the web to infect users with malware. They are different from the classic drive-by attack. With SEO attacks—known as "SEO poisoning"—search engine results are poisoned in order to drive user traffic to the rogue site. Google has reported that up to 1.3% of their search results are infected. So, with SEO Poisoning, you're directed to a bad page through a poisoned search.

How Cybercriminals Make Money from these Attacks

As recently as five years ago, hackers circumvented a computer's security systems to gain illegal access merely as a "proof of concept" or for individual kudos. Now, their criminal activity is business-focused. Today's hackers can afford to make investments, because they'll most likely get a payback.There are various ways that criminals can profit from these attacks, including:

- Selling exploit kits, or functionality used in kits, to other criminals. An exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software. This frequently includes gaining control of a computer system.
- Injecting legitimate sites to drive user traffic to wherever they desire. Since they control the redirect from the injected code, they can essentially "sell traffic."
- Profiting from the payload of the malware that will be installed. They make money from data theft or botnets, which run automatically and autonomously and used to send spam, or perform a denial of service attack against a remote target.
- Taking advantage of zero-day vulnerability information. Attackers will pay big money for access to info on zero-day vulnerabilities. Zero-day exploits are used or shared by attackers before the developer of the target software knows about the vulnerability. Some hackers will make this their business–they'll find new vulnerabilities and then sell this information to the black market.
- Abusing affiliate-marketing programs with illegitimate traffic, in order to profit. Since the emergence of affiliate marketing, where affiliates are rewarded for bringing customers to a company's website, there has been little control over affiliate activity. Unscrupulous affiliates have used spam, false advertising, forced clicks (to get tracking cookies set on users' computers), adware and other methods to drive traffic to their sponsors.

In terms of trends in cybercriminal activity, we've seen an increase in hackers using multiple payloads—different types of malware—in order to harvest data. In addition, there has been an increase in very specific, targeted attacks. For instance, criminals will target a human resources contact to steal data and get information on other people in a company. They will then formulate an attack with that information, so that the target is more likely to respond.

How These Attacks Impact Your Business

Malicious JavaScript can impact your business in a variety of ways. As an IT manager, you need to be vigilant and defend against it. Two primary issues to watch for are:

- Users becoming malware victims—The machines you manage can get infected via a drive-by download, SEO poisoning, or other attack.
- Compromised websites—The site(s) you manage can get compromised, and as a result, you will inadvertently be exposing customers that browse your site to malicious code.

Both of these possibilities have very real impact, in terms of costs, productivity, corporate reputation and data theft. When your users become malware victims, there's time and cost involved in getting their PCs back up and running. Plus, the users have a period of lost productivity and may have damaged files as well.

The impact of an infected machine goes further however; data integrity could also be compromised. Once running on the victim machine many families of malware provide hackers with the ability to gain remote access to users' machines, to steal data or infect them with more malware.

If your website is compromised, then you're perceived as being responsible for infecting anyone who visits it. This can damage to your corporate reputation, result in negative publicity and a lack of confidence from customers, partners and investors.

In conclusion, you've seen why the "bad guys" like malicious JavaScript, and why the "good guys" need to defend against them. In Part II, we'll delve into solutions to help keep you safe.

Additional Resources

Malware with your Mocha—provides detailed technical information on the latest malicious JavaScript attacks

Anatomy of an Attack—Get advice on the changing threat landscape, threat protection strategies, why criminals desire your data and more

Sources

Sophos Threat Report mid-year 2010
http://www.sophos.com/security/technical-papers/modern_web_attacks.html
http://www.sophos.com/security/technical-papers/malware_with_your_mocha.html
http://www.sophos.com/security/technical-papers/sophos-securing-websites.html
http://nakedsecurity.sophos.com/?s=malicious+javascript&x=0&y=0

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM