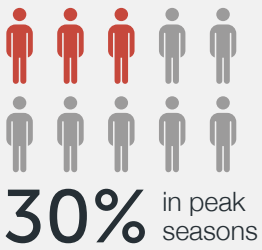
namogoo

Protect Your E-Commerce Visitors from Client-Side Injected Malware

Table of contents

If you're responsible for your company's e-commerce operations, no doubt you invest serious amounts of resources in optimizing your conversion rates. You understand your potential buyers, what interests them and have designed the user experience to cater to their needs. You build and test the pages thoroughly in order to maximize results. Now it's just a matter of bringing the traffic and you're on the road to success.

The only problem is that a very large number of your website visitors (in peak seasons up to 30%) will not see your site as you intended it to be seen. They will encounter a barrage of pop-ups, ads, competitor product recommendations and other unwanted distractions – all of which are completely out of your control.



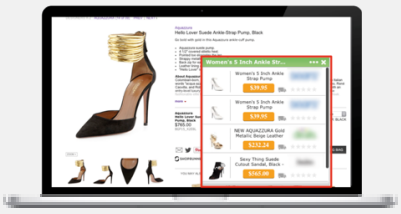
This troubling phenomenon is known as "Client-Side Injected Malware," and its impact on ecommerce and other websites is growing every day. This white paper is intended to help e-commerce companies better understand the scope and nature of this problem, as well as showing them how they can protect their visitors from sneaky injected malware on their browsers and devices.

What Is Client-Side Injected Malware (CSIM)?

Client-Side Injected Malware (CSIM) includes unauthorized widgets (product recommendations and deals), advertisements and spyware scripts that are injected into websites by extensions installed on browsers, or by malware downloaded unintentionally to the visitor's computers, tablets and mobile devices.

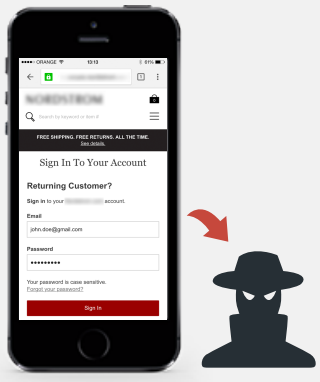
Prevalent in all browsers and operating systems, these injections cause visitors to view a webpage in an entirely different way than the page was designed to display, without permission from or payment to the website owner. The programs that cause injections are usually bundled within software the wanted to download (e.g., a free PDF viewer or - as ironic as it may seem - an anti-virus program) or added via updates to other programs already installed on their computer without the visitor's knowledge or consent. These injections belong to an independent third party service that hijacks the webpage and places its own ads as a way of making money. This type of service runs in a layer on top of the webpage, and is outside the control of the website owner.

Following are some examples of different types of injections:



Injected Competitor Products – The webpage is injected with competitor offerings, targeted to the visitor's intent and context. Besides distracting the visitor from what you intended him/her to see, clicks on injected products take traffic and revenue away from your site.

Injected Ads – The webpage is manipulated to display disruptive banner ads that diminish the site's brand. Inappropriate ads on your site may annoy visitors, compromise your reputation, and harm your visitor retention.



Spyware Scripts – mobile apps and websites are injected with spyware scripts that monitor login credentials, email addresses and other personal information. User data is sent to remote servers, sold to third party entities and is used in various means. Fake surveys collect confidential data about the site's visitors, who believe they are sharing their information with the site they browse and trust, exposing your company to a serious legal risk. This can result in liability and reputation damage due to stolen visitor details and privacy breaches.

The Impact on Your Business

E-commerce websites are currently manipulated by client-side injections that neither they nor their visitors are aware of. Even worse, many injections appear to visitors as an integral part of your website. This increases the chance that a visitor will click on one of these injections, as well as undermine the trust you've built over time with loyal customers.

As can be seen in the examples above, CSIM is much more than a nuisance – it has a direct and profound impact on your bottom line. As soon as unwitting visitors click on an injected ad or banner, they leave your site and you've lost potential revenue.

Not only does CSIM result in a direct loss of visitors and conversions, it often adversely affects the user experience. CSIM disrupts the flow and navigation of your site, leading to a higher bounce rate and distorted data. In addition, your website privacy terms could be in breach as CSIM places cookies in your visitors' browsers, at times under false pretense of your company's name. CISM also compromises the security and privacy of your visitors' information, including their email address, and exposes them to spam and phishing campaigns.

In terms of quantifying business impact, it is important to understand the prevalence of CSIM among visitors to e-commerce sites. Based on a recent study conducted by Google on the ad injectors ecosystem, more than 5% of people visiting Google sites have at least one ad injector installed. Of these, 34% of Chrome extensions were defined as outright malware. Namogoo believes that actual infection rates are about four times this amount. Based on our work with several leading retailers, we have found that between 15-30% of visitors to ecommerce sites are infected by CSIM.

Why Current Website Security Solutions Are Not Enough

In most e-commerce companies, the server side of the business operation is well protected by a slew of security products – from network and application firewalls to SSL and identity management systems. All of these products are designed to ensure high availability and protect the web and application servers from external attacks.
However, when it comes to the "last mile" (i.e., the visitor's computers and devices), companies have little visibility into the security of client-side devices and have no way of knowing what their visitors see when they access the site. Your visitors' devices are in essence the "front door" to your website. If malware gets through the front door via CSIM, all of the server side protection you have doesn't help – you're losing business and visitors.

In order to secure the client side, other than encouraging their visitors to install anti-malware solutions, there is little e-commerce companies can do. In any case, most of these anti-malware tools are not particularly effective against sophisticated injectors that frequently change their signatures. To make matters worse, according to a recent OPSWAT report, over 90% of client devices with an anti-virus engine installed had not run a full scan in the last seven days, putting them at risk for infection. Ironically, a number of the popular free anti-virus tools are also often bundled with malware that injects ads.

Typical CSIM Infection Scenario

The following is a typical scenario illustrating how an innocent visitor gets infected by CSIM – from malware and through injection of an ad onto an e-commerce site:

1. Developers create an extension for injection on browser
2. Third party platforms are used to bundle the extension or app to legitimate software based on a revenue sharing model
3. The innocent visitor downloads an extension or app (such as free video player) with a bundled injector
4. The visitor decides to shop on an e-commerce site
5. The webpage is served from the web server as it should correctly appear
6. Immediately after page rendering, the visitor's browser injects malware into empty space or overrides existing content. Depending on its sophistication, the injection may or may not be apparent to the visitor.

Introducing Namogoo – The New Way to Protect Visitors from CSIM

Namogoo offers end-to-end protection against any type of injected malware (e.g. adware, spyware scripts, widgets) that affects your visitors' browsing experience. This solution was built with a single goal in mind – to make sure your website will be displayed exactly as you intended, every time and for every visitor. By blocking CSIM before it impacts your site, Namogoo puts an end to lost revenue, brand abuse and privacy infringements.

Namogoo's servers scan millions of pages daily, creating malware injection blocking rule sets in real-time and delivering them to your website via a single line of code. Namogoo recognizes injection patterns and blocks them, so the visitor's browser only renders legitimate elements of your website. Patent-pending machine learning technology enables real-time detection and elimination of injected malware.

Namogoo's technology was designed for zero integration on the merchant side. By adding a single line of JavaScript code that communicates asynchronously with an advanced back-end system, the service can be added within a few minutes to deliver immediate results.

An intuitive and convenient tracking and monitoring dashboard allows e-commerce companies to view up-to-the-minute information on identified injections, anonymous visitor-related data and impact estimates.

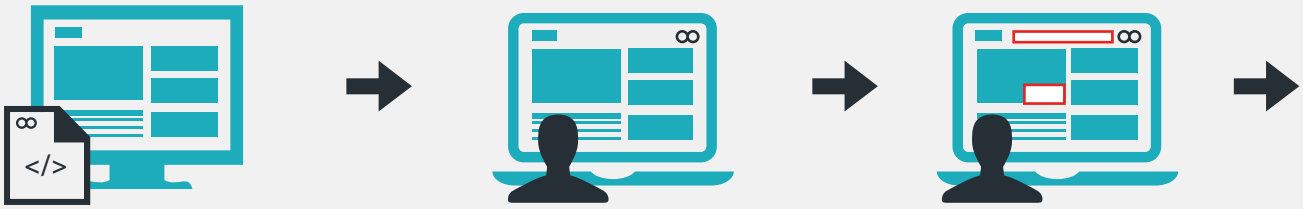
Namogoo's advanced technologies are uniquely designed to meet the needs of today's e-commerce companies:

Self-learning protection - Advanced machine learning algorithms identify changes in injection fingerprints and automatically adapt the security rules so your protection is always up to date.

Zero integration - Namogoo supports all types of website platforms. With our zero integration SaaS solution – simply drop a line of code in your website and you're up and running.

Inherent scalability - Namogoo is built to deliver high performance for sites of any size. A robust, scalable and fault-tolerant architecture is designed to handle billions of pages per month with high capacity storage. The system has been implemented for a number of very large retailers with excellent results.

How It Works



Drop a line of code for website (typically takes less than 1 minute)

Page is served by e-commerce site with Namogoo tag

Page loaded on visitor side by browser

CSIM is identified and blocked by Namogoo using proprietary technology

Namogoo uses self-learning mechanism to automatically update its security mechanisms

Business Benefits for E-Commerce Companies

By using Namogoo to protect your visitors from unwanted malware (CSIM), your company can achieve higher e-commerce revenues and strengthen customer loyalty:

Increase conversion rates by eliminating injected ads and banners that take visitors to third-party sites

Preserve brand reputation by keeping inappropriate ads off your site

Eliminate privacy infringements related to spyware injections

Enhance customer retention by ensuring a flawless and intentional user experience

Conclusion

Client-side infected malware (CSIM) is a real threat to e-commerce businesses and is expected to continue to grow. It adversely affects the user experience and "skims" serious revenues from websites. However, as CSIM affects the visitor's browser rather than the web server, it is basically invisible to website owners. Particularly in large organizations, it is virtually impossible to identify visitors (buyers) that are "lost" to clicks on CSIM banners and the like.

Accordingly, the first step in fixing this problem is raising awareness among stakeholders within your organization that the threat exists, as well as recognizing the magnitude of its business impact. It is also important to understand that your current security solutions were not designed to prevent this type of threat. Addressing this void, Namogoo offers a breakthrough technology that provides e-commerce sites with a simple-to-deploy, end-to-end solution for handling CSIM threats.

Learn more about how Namogoo can protect your visitors from CSIM, get a free analysis of your website - www.namogoo.com/get-analyzed

About namogoo

Namogoo is a security startup, backed by top-tier VCs, that provides a new, client-side, protection layers to companies with online presence. With pioneering and robust technology, Namogoo scans tens of millions of customers' pages daily and protects them from various types of malware with one goal in mind: keeping the communication channels between companies and their users safe and trustful. Namogoo's founders are experts in big data analytics, machine learning algorithms and security. The company is headquartered in Tel Aviv, with offices in New York City and London.