Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Formjacking: What is it and how does it work?

A Relatively New Form of Cyber Threat

Audience: General

Reading Time: 10 Mins

Formjacking is relatively new technique which cyber criminals are using to exploit and steal potentially sensitive information from commercial websites.

Formjacking is a type of online *man-in-the-middle attack*. It works the same way as if you were to have your phone tapped by the police but is focused on website forms. In a formjacking scenario, a client may come to your website with the aim of signing up to your newsletter, however, upon typing in their email to your newsletter service it also gets sent to the attacker.

Formjacking is so effective because its entire intention is to stay hidden. You may never become aware that you have been a victim of it. So, how do you know you have been a victim? It depends on the data which is being stolen by the attackers. In our example above it was an email address; however, many attacks are aimed at payment gateways, stealing credit card and banking details. On these occasions, many of the victims become aware when their bank contacts them about suspicious activity on their account.

How many websites are infected?

Symantec reported that almost 5000 websites a month are being compromised with malicious formjacking code and in 2018 there were almost 4 million individual formjacking attacks on unsuspecting individuals. Two major examples of successful formjacking attacks were against British Airways and Ticketmaster. Vulnerabilities found in features on their websites allowed attackers to modify JavaScript code to detect when forms were submitted. Upon submission the form data was sent to multiple places; one of these was genuine while the other was not.

In the British Airways case, it was found that the formjacking payload consisted of only twenty-lines of code and successfully completed its action in milliseconds which helped keep it hidden.

European Union
European Regional Development Fund
Manchester Metropolitan University
MANCHESTER 1824 The University of Manchester
University of Salford MANCHESTER
Lancaster University

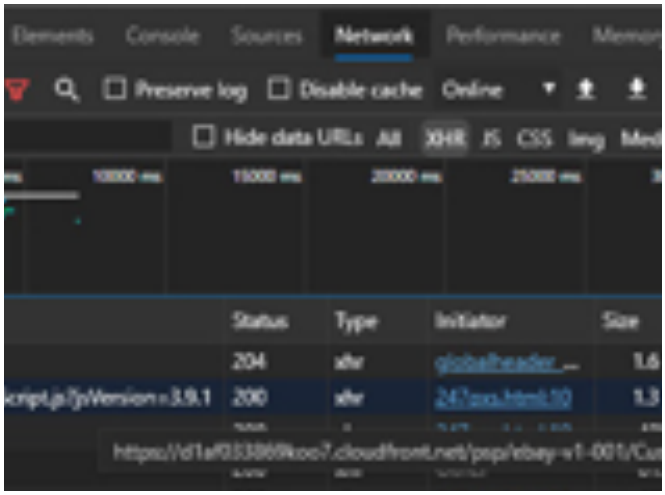
Protecting Yourself

How can businesses protect themselves against formjacking?

Most formjacking code has been added to existing scripts on a website via vulnerabilities in the underlying software. If you are using some form of ecommerce platform such as Magento or a content management system like WordPress, then you must keep this software up to date, including any extensions. Services also exist such as: www.watchdogs.online and www.wewatchyourwebsite.com that report back any modifications detected on your website. If these changes do not align with what your development team have been working on, then this can be a great way to identify an intrusion into your software.

Is there a quick way to check my website?

Most web browsers offer a way to track the data coming in and out of a website. It may be possible to detect a formjacking attack by identifying an unknown web address appearing in network logs for your website. You can use www.sitecheck.sucuri.net and/or www.mxtoolbox.com/domain to check any suspicious website address found in the logs which will respond with information related to its level of suspicion and if it has been used as part of a cyber-attack in the past.



By pressing F12 in your browser and going to the 'Network' tab you can what data is loading. By choosing 'XHR' on the menu you can filter the results to show only incoming and outgoing remote connections.

Definitions

JavaScript - often abbreviated as JS, is a high-level, just-in-time compiled, object-oriented programming language mostly used on websites. It runs locally on a client machine and is often used for styling websites or making on-the-fly calculations in real-time without the need to communicate with a server. It is also used as the backbone for features such as the 'like button' that require asynchronous calls to a database without the need to refresh.

Payload - A payload is the portion of malware which performs the malicious action. In form-jacking this is the part of the code designed to send information to the attacker's server. Payload is used to differentiate between parts of the code that are deemed safe and those that are not. Only a small section of code might represent the payload with the rest being used to obfuscate.

Man-in-the-middle attack - This kind of attack has at least three different assets involved in a communication process. These three assets are usually referred to as A, B and E. Or, Alice, Bob and Eve, where Eve stands for eavesdropping. A man-in-the-middle attack works when Eve intercepts a communication between Alice and Bob. Alice and Bob are often unaware of Eve.

Malicious code - Used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.

Finding Support

What to do if you think you are a victim?

If you believe you have been the victim of a formjacking hack you should contact the administrator of the website and have them patch the vulnerability that the attackers exploited (generally updating the software/ extensions). Then you need to find and remove the malicious code. During these changes it would be a good idea to put the live website into maintenance mode, so more customers are not affected.

Once the updates have been made and your website is using only secure code again it is time to investigate how long this malicious code has been present. You can do this by checking any periodic backups you make to find when the malicious code first appeared or use an online service such as www.archive.org

Once you have a general idea of the time involved in the attack you can cross reference this with your online website orders to find the users who have most likely had their details stolen. It is advised that all these customers should be made aware of what details have been leaked and how it occurred. You should also include details of the steps taken to remediate the vulnerability and how you will attempt to prevent this kind of attack from happening again.

Most clients are aware that cyber-attacks are becoming more sophisticated and the industry in general is more secure when companies are transparent about the issues they are facing. Collaboration and open source intelligence sharing are the backbone of the cyber security defence services, if companies and governments are not open and honest about the attacks they are facing and have faced then it is impossible for service providers to produce innovative new products to defend against future cyber-attacks.

How Can Your Business Navigate The Cyber Challenges Of 2020?

The **Greater Manchester Cyber Foundry** runs a *Secure Digitisation Programme* designed to support businesses facing cyber challenges in the Greater Manchester. The programme consists of two full-day workshops, alongside some online open learning elements. In addition, enrolling gives you access to our digital portal full of cyber innovation tools and services to better **defend**, **innovate** and **grow** your business.

Image: Helena Lopes on Unsplash

The course aims to teach the basics of secure digitisation before going on to explore how you and your business could grow and thrive through cyber innovation. Participation in this has the potential to lead to a bespoke technical assist in cyber innovation from one of our dedicated technical teams from a partner university.

The support is free due to being part funded by the **European Regional Development Fund**, and is in partnership with **Lancaster University,** the **University of Manchester, Manchester Metropolitan University,** and **Salford University**.

To find out more about how your business can access support and register on one of upcoming cohorts contact us:

gmcyberfoundry@lancaster.ac.uk

Further Reading

About the Authors

Robert Marsh is a published Internet of Things Forensics Researcher and an award-winning Artificial Intelligence Software Developer. He is currently working as a Cyber Security Analyst with the Greater Manchester Cyber Foundry technical team at The University of Salford.

READ MORE

1. "What Is Formjacking?", Experian www.experian.com/blogs/ask-experian/what-is-formjacking/
2. "The British Airways Breach: How Magecart Claimed 380,000 Victims.", RiskIQ www.riskiq.com/blog/labs/magecart-british-airways-breach/
3. "Zero-Day in Popular WordPress Plugin Exploited in the Wild to Take over Sites.", ZDNet www.zdnet.com/article/zero-day-in-popular-wordpress-plugin-exploited-in-the-wild-to-take-over-sites/
4. "Internet Security Threat Report 2019.", Symantec interactive.symantec.com/istr24-web
5. "Krebs on Security." Brian Krebs, krebsonsecurity.com/2018/11/whos-in-your-online-shopping-cart
6. "Formjacking Accounts for 71% of All Web Breaches." PrivSec Report gdpr.report/news/2019/08/16/formjacking-accounts-for-71-of-all-web-breaches/
7. "The Security Nightmare of Formjacking." Infosecurity Magazine, www.infosecurity-magazine.com/opinions/security-formjacking-1-1-1/
8. "Form-Jacking Attacks Hit High Profile Companies.", Midgard IT, www.midgard.co.uk/form-jacking-attacks-hit-high-profile-companies/

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund