Feedify Hacked with Magecart Information Stealing Script

By Lawrence Abrams

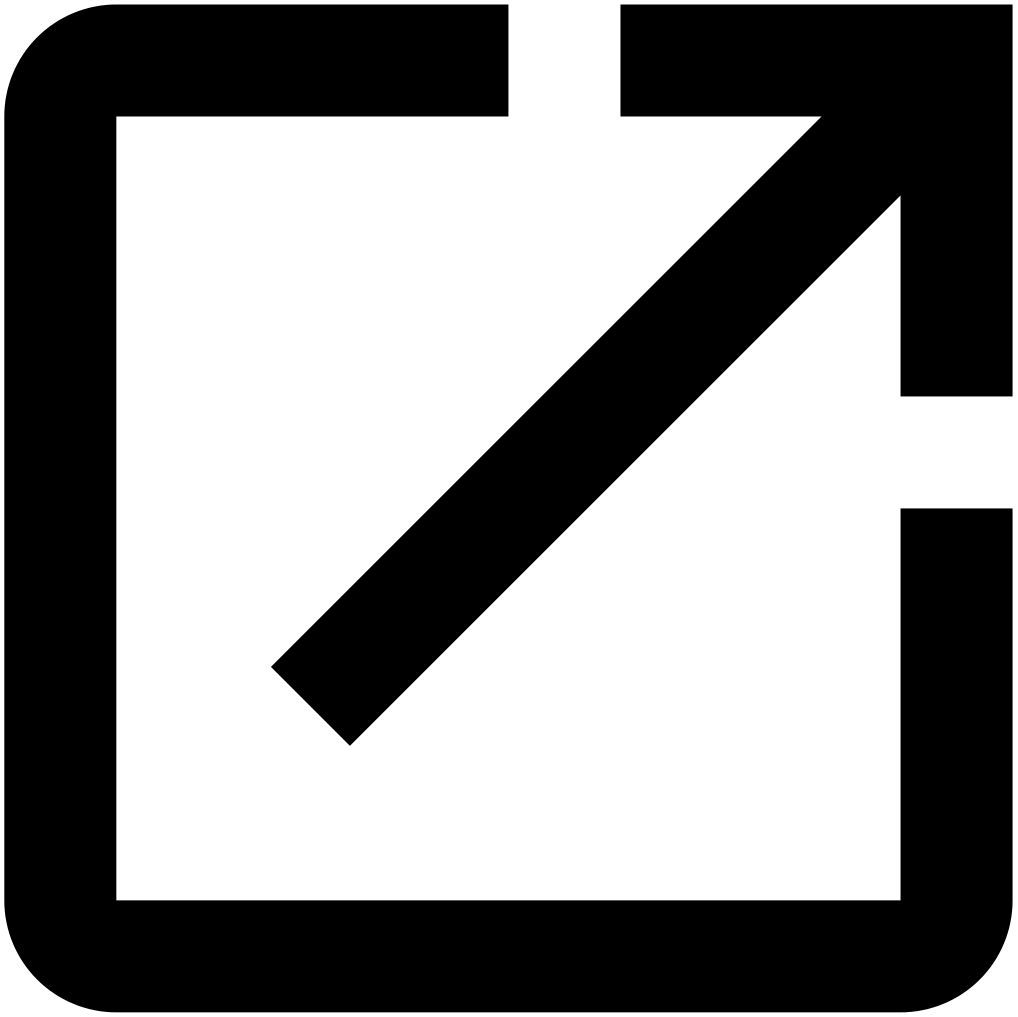
Published: 2018-09-12 · Archived: 2026-04-05 15:11:11 UTC

A script used by the customer engagement service Feedify has been hacked to include the malicious MageCart script. MageCart is malicious code used by attackers to steal credit card details and other information from e-commerce sites when a user submits a form.

In order to use the Feedify service, e-commerce sites need to add a Feedify JavaScript script to their site. If the Feedify script is compromised with MageCart, any visitors who go to e-commerce site that uses the Feedify script will also load the malicious code.

This hack was first noticed by a security researcher named Placebo who posted about it yesterday on Twitter. When Placebo posted about it, MageCart had already been removed from the Feedify script.


DIE LINKE.
0:00



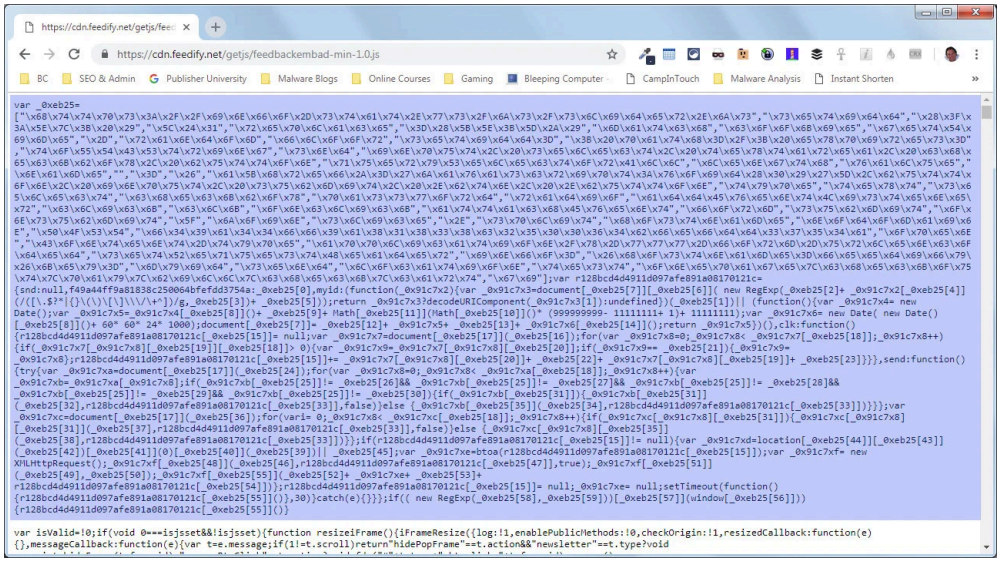
Visit Advertiser websiteGO TO PAGE

When researching this story, I created a Feedify account to test what scripts their customers were being instructed to add. When testing the service, customers are instructed to add the following snippet of code to their site.

```
<!--Feedify Script Start-->
<script  id="feedify_webscript" >
var feedify = feedify || {};
window.feedify_options={fedify_url:"https://feedify.net/"};
var s = document.createElement('script');
s.type = 'text/javascript';
s.src = 'https://cdn.feedify.net/getjs/feedbackembad-min-1.0.js';
document.getElementsByTagName('head')[0].appendChild(s);
</script>
<!--Feedify Script End-->
```

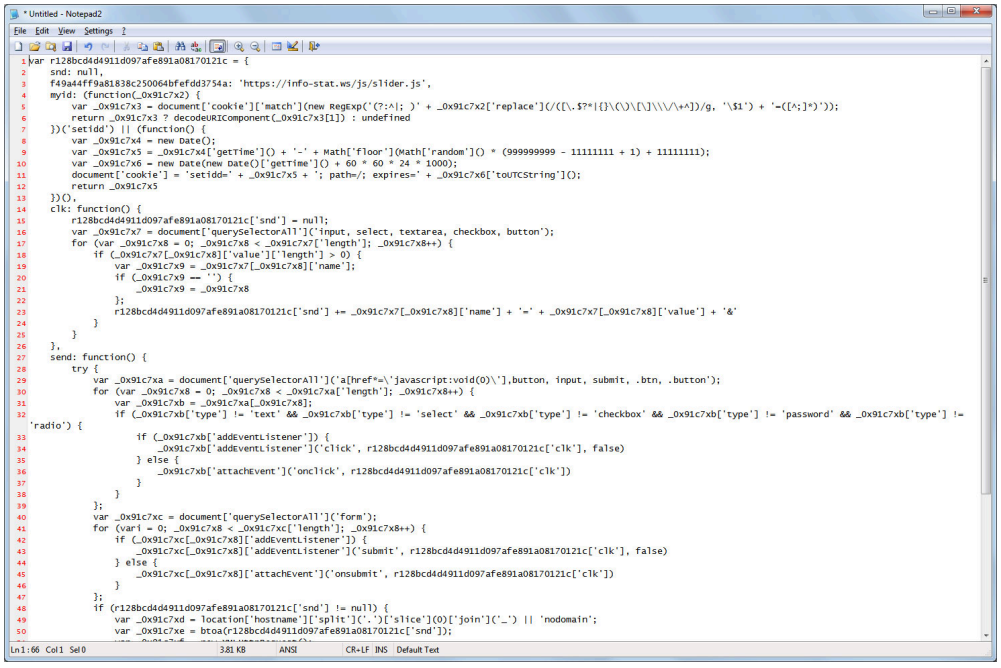
Caption

When examining the https://cdn.feedify.net/getjs/feedbackembad-min-1.0.js script, though, I saw that MageCart was still embedded in the script as shown by the highlighted section below.



Caption

A partial deobfuscation of the script shows that any submitted information will be sent to the URL https://info-stat.ws/js/slider.js.



Caption

To confirm that this was indeed MageCart, I contacted Yonathan Klijnsma of RiskIQ who further confirmed that the Feedify script was still compromised. Klijnsma told BleepingComputer that the script had been reinfected 15 minutes prior to my contacting him.

Currently the malicious code has been removed from the https://feedify.net/getjs/feedbackembad-min-1.0.js, but it is still present in https://cdn.feedify.net/getjs/feedbackembad-min-1.0.js.

BleepingComputer has contacted Feedify for further information, but has not received a response at the time of this publication.

MageCart used in recent British Airways hack

RiskIQ also discovered that a script used by British Airways was also recently compromised by the MageCart script. This allowed attackers to steal payment and other sensitive information from approximately 380,000 individuals.

In the British Airways hack, the compromised script was the Modernizr JavaScript library, which airline's site was using.

Source: https://www.bleepingcomputer.com/news/security/feedify-hacked-with-magecart-information-stealing-script/