What Can We Learn From The Jamie Oliver Website Hack?

A drizzle of malware, a dash of exploit and a dollop of malicious code were the recipe for Jamie Oliver's web attack disaster

BY **DUNCAN MACRAE**, FEBRUARY 18, 2015, 11:31 PM

4 MIN

Malicious code was **served up on the website** of TV chef Jamie Oliver on Pancake Day. The site had been hacked and malware was redirecting visitors to an exploit kit, according to security firm Malwarebytes, which had discovered the infection during routine checks for hacks and exploits.

The site, which has more than 10 million monthly visitors globally, is now said to be safe to use again. Jamie Oliver's management team said: "The team at jamieoliver.com found a low-level malware problem and dealt with it quickly. The site is now safe to use. We have had only a handful of comments from users over the last couple of days, and no-one has reported any serious issues. We apologise to anyone who was at all worried after going on the site.

pancakes

"The Jamie Oliver website is regularly checked for vulnerabilities by both our in-house team and an independent third-party and they quickly deal with anything that is found. The team is confident that no data has been compromised in this incident but if anyone is worried, do please use the contact form on the site."

But what, apart from some new cookery-related puns, can we learn from this hack? Here's what security specialists had to say:

Laurie Mercer, Solutions Architect at Veracode

"When websites such as Jamie Oliver's are compromised, both consumers and website owners are at risk. Users risk having their computers infected with malware and their money and identity stolen, whilst Jamie Oliver Group risks losing customers' trust. Even after the incident is addressed users will think twice before browsing that site over one of its competitors. Websites are the modern-day store front so it is vital that they are secure and protect their customers.

"Jamie Oliver's online team acted fast to ensure that the site is now 'safe to use' and have confirmed that they regularly check the website for security vulnerabilities- which all website owners should be doing. If anyone doubted that all businesses and customer-facing websites are at risk of being targeted by cybercriminals, this latest incident provides a telling example that the proof is indeed in the pudding."

David Emm, principal security researcher at Kaspersky Lab

"The news that Jamie Oliver's website has been hacked is yet another reminder of how careful everyone needs to be when using the Internet. Many people have potentially been exposed to malicious software by simply clicking on something that looks legitimate. The trouble is, to the untrained eye, it can be nearly impossible to tell what's legitimate and what's not, no matter how aware people think they are.

"This incident highlights the need for everyone to install comprehensive Internet security software that will protect them wherever they go on the Internet, because even legitimate and trusted websites, such as this one, can be compromised if attackers find a way to implant their code and redirect people to an infected website. It's also another reminder that **cybercriminals** are not only after information from large organisations, they also chase information from consumers."

Steven Harrison, lead technologist at Exponential-e

"This latest infringement demonstrates that system administrators and network operators can't rely on end-users to maintain their own security. Modern malware is cloaked in a veil of legitimacy with users unknowingly granting hackers permission with every click-and-action. As a result, more needs to be done to counter today's threats in an active yet automatic way.

"Gone are the days when the primary aims of cybercriminals were mischief and disruption. The use of a well-known site to push **malware** to users is a perfect example of the financial motives behind acts of cybercrime. Up-to-date antivirus and the latest patches belies the real seriousness of modern malware that often cannot be stopped by signature based security solutions alone. Instead, our entire approach to security in IT needs to evolve to one where we identify the good things and then fight back against everything else."

Carl Leonard, principal security analyst at Websense

"Seeking the perfect pancake mix on Shrove Tuesday could have led you to your favourite celebrity chef for the perfect batter recipe. Malware authors want to dish up more than unsuspecting victims bargained for, and only host their code on these popular sites for just a brief moment to capture a large footfall. The code can come back at any moment if webmasters are not prepared.

"If end users are browsing to such sites, companies need to ensure they have the perfect recipe for detection of known malware and **exploits kits**, combined with real-time analysis of outliers; ensuring that threats hosted on the far-reaching corners of the web are stopped in their tracks."

How much do you know about hackers and viruses? Take our quiz!

ASSOCIATED THEMES

#EXPLOIT KIT #HACK #MALWARE #SECURE-IT #SECURITY

Silicon UK is the leading source for IT news, analysis, features and interviews covering the technology that impacts your business. Keep up-to-date with the latest tech news and read in-depth features by subscribing to our newsletter and attending our events.