Despite appearances, WikiLeaks wasn't hacked

GC grahamcluley.com/despite-appearances-wikileaks-wasnt-hacked/

September 4, 2017

If you visited the WikiLeaks website on Thursday morning, you can't have failed to notice something a little out of the ordinary.

Instead of the normal catalog of leaked confidential documents from Western governments and intelligence agencies, you'll have seen a message from the notorious OurMine gang.

Part of the message visible to visitors of the WikiLeaks website read as follows:

> Hi, it's OurMine (Security Group), don't worry we are just testing your…. blablablab, Oh wait, this is not a security test! Wikileaks, remember when you challenged us to hack you?

Yes, it was OurMine up to their old tricks again, fresh from compromising the social media accounts of football teams FC Barcelona and Real Madrid.

Why would OurMine want to target WikiLeaks? Well, there isn't much love lost between them, following the alleged personal details of members of the hacking group were published online was followed by a DDoS attack against the whistle-blowing site in 2016.

The good news for WikiLeaks this time was that things weren't quite as bad as they might have first appeared.

You see, the WikiLeaks website hadn't been hacked.

Instead, OurMine had managed to alter WikiLeaks's DNS records (held by a third-party registrar) to direct anyone who tried to visit wikileaks.org to visit a different IP address which definitely *wasn't* under the control of Julian Assange and his cronies.

Was that too nerdy for you? Think of it this way. The internet has 'telephone directories', known as DNS (Domain Name System) records, that translate website names (such as wikileaks.org) into a numeric address (such as 95.211.113.131) that the internet understands.

Change the numbers in the telephone directory, and anyone trying to get to wikileaks.org could end up somewhere else entirely.

This kind of domain hijacking isn't a new threat – past victims have included such well-known services as WhatsApp and anti-virus firm AVG – but it's a very effective way to embarrass an organisation publicly, and even (in the worst cases) attempt to scam visitors or redirect them to malware.

And while your website's domain records are under someone else's control it's not only possible that your website visitors are being redirected, but also that emails being sent to your organisation are being sent somewhere else entirely too.

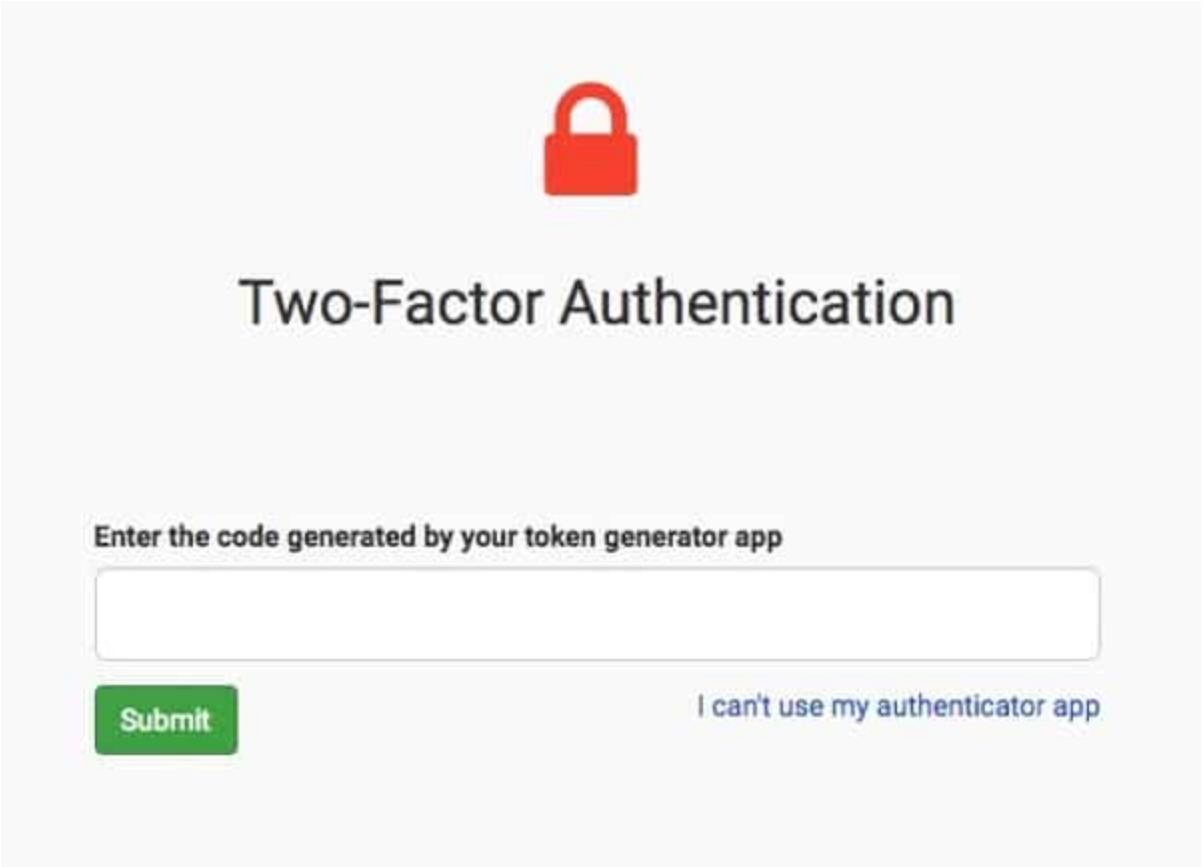
We don't know how OurMine managed to access WikiLeaks's DNS records, but past experience has shown that their typical modus operandi is simply to log in using their victim's password.

If that happened in this case then it's possible that someone at WikiLeaks was either phished, had an easy-to-guess password, fell victim to some spyware, or made the mistake of reusing the same password in different places.

Alternatively, the attackers might have used social engineering to trick WikiLeaks's DNS provider into handing over the credentials, or simple requested that a password reset link be sent to a compromised email address.

For this reason, many DNS registrars offer additional levels of security beyond passwords – such as registry locking and two-factor authentication (2FA) – to better protect the critical data they store about your website.

For instance, the DNS registrar I use for grahamcluley.com is DNSimple which has been supporting 2FA since 2012.



Even if a malicious hacker has managed to determine the password for your company's 2FA-protected account at the DNS registry, they shouldn't be able to access it because they don't know your one-time numeric PIN.

Of course, it's always possible that an attacker might exploit a vulnerability in your DNS registrar's systems to fiddle with your website's records, perhaps without needing to know your password or bypass 2FA. But such attacks are by their very nature much rarer.

If you own a website, take advantage of the security features that your DNS registrar offers you – or find an alternative registrar who will do more to protect your account.

And if you're the administrator of the WikiLeaks website, just be grateful that OurMine was feeling more mischievous than malicious – as this attack could have been much more serious.

Found this article interesting? Follow Graham Cluley on Twitter to read more of the exclusive content we post.

Vulnerability

- #DNS hijacking
- #Ourmine
- #Wikileaks

Graham Cluley • @gcluley

Graham Cluley is a veteran of the anti-virus industry having worked for a number of security companies since the early 1990s when he wrote the first ever version of Dr Solomon's Anti-Virus Toolkit for Windows. Now an independent security analyst, he regularly makes media appearances and is an international public speaker on the topic of computer security, hackers, and online privacy. Follow him on Twitter at @gcluley, or drop him an email.