THE TAKE-DOWN OF THE WHOLE U.S. INTERNET MAY BE PLANNED BY CLINTON STAFF TO JAM UP ELECTIONS, SECURITY EXPERTS FEAR

Surviving Electmageddon: Protecting against a wave of DNS outages

HILLARY CLINTON'S BIGGEST ENEMY IS TRUTH AND TRANSPARENCY, SAYS JOHN PODESTA. CLINTON CREWS ARE BELIEVED TO BE TESTING THE TAKE DOWN OF THE INTERNET IN ORDER TO HIDE REVELATIONS ABOUT CLINTON FOUNDATION CRIMES

This entry was posted in General Security, WordPress Security on November 3, 2016 by mark 23 Replies

PROVIDED BY WORDFENCE AS A PUBLIC SERVICE

Two weeks ago, DNS provider Dyn was attacked in a very large DDoS attack. IoT devices were used to send an overwhelming amount of traffic to Dyn's resolvers which resulted in Dyn effectively being taken offline for hours. This took out Netflix, Paypal, Github, Twitter and many other name brand services.

The Dyn attack may have been retribution against a researcher from Dyn who collaborated with Brian Krebs – both of whom have been working to expose DDoS-for-hire and DDoS protection rackets. We think this explanation is more likely than it being a 'state sponsored attack'.

The Dyn attack was the result of Internet of Things or IoT devices being infected with a botnet. At the time about 500,000 devices were infected and only 10% of them were used in the Dyn attack. The source code for the Mirai botnet that was used in the Dyn attack was released some time before the attack on Dyn and this allowed any attacker to build their own botnet and launch a large DDoS attack on any target.

Earlier this year, Russian hackers, codenamed 'Fancy bear' and 'Cozy bear' hacked into the Democratic National Committee which resulted in email leaks. This may have been an attempt to disrupt or influence the US election.

The US election is on November 8th, less than 1 week from now. Some candidates may benefit if fear, uncertainty and doubt are cast on the election itself or the results. Launching a massive DDoS style attack on DNS providers on November 8th would achieve that objective. It would take many services off-line, including news, exit poll results, official candidate websites, official announcement sources and services we rely on like banking.

We think that certain nation states may have reason to create this kind of disruption. We also think that malicious individuals with their own agenda may also try to create disruptions on November 8th. The Dyn attack demonstrated that by leveraging IoT devices and the Mirai source code, massive outages can be created by individuals or state actors.

In light of the above facts and the climate we find ourselves in, we would like to make a recommendation to owners of mission critical websites to help them weather the storm that may arrive on November 8th. We are suggesting a change in DNS configuration that is technically complex and also increases operating costs. We recommend this change for business or mission critical websites who have a technical staff they can call on to help them implement this.

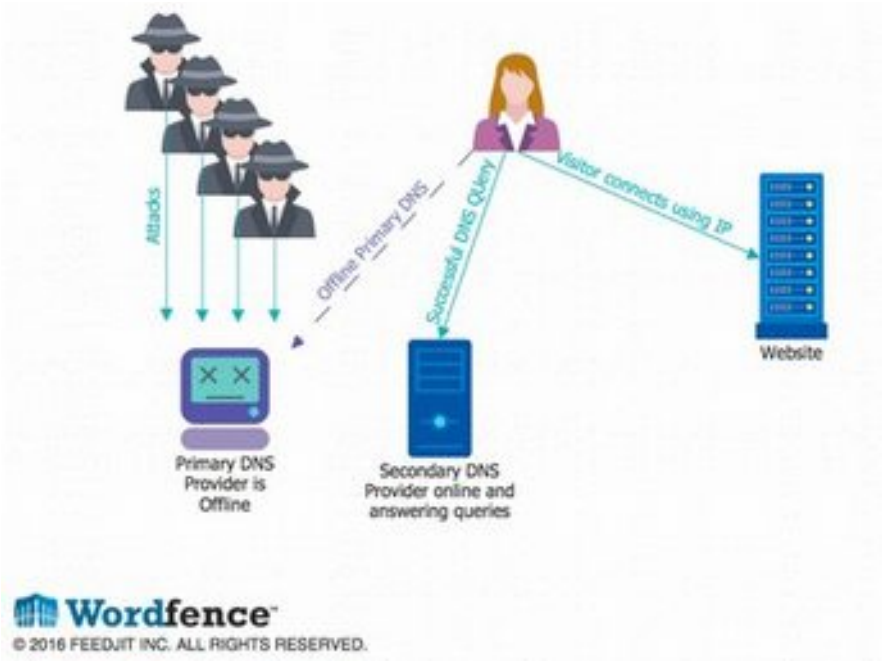
We recommend that websites set up a secondary DNS provider via a different DNS vendor. By doing this, if your first DNS vendor is attacked, the second one will answer any requests for your domains IP address and your website or service will continue functioning as per normal.

To do this, you need to have a primary DNS provider that allows “zone transfers”. That means that the primary provider must give you the ability to authorize another DNS provider to copy or replicate all your DNS records from time to time.

The vendor you choose as a secondary DNS provider must have the ability to act as a secondary where another vendor is the primary. That means it must be able to do zone transfers from your primary DNS provider to replicate your DNS records.

Wordfence is moving to this configuration over the next few days and we’re implementing it with our current DNS provider, DNSMadeEasy as primary and with Verizon’s Edgecast DNS service as the secondary. We have verified that they can work with this configuration and they will give us the performance our customers expect.

The diagram below gives you a general idea of how a secondary DNS server keeps your website online if your primary DNS provider is attacked. Customers can’t lookup your website IP address and, rather than your website appearing offline, they are able to resolve your site IP with the secondary DNS server and connect to your website. DNS is more complex than the diagram indicates, but this gives you a general idea of how failover works from primary to secondary during a DDoS attack.



Finding a cost effective DNS provider that can act as secondary DNS to your primary provider can be a challenge. You may also have to switch primary DNS providers if your primary does not allow zone transfers to a secondary DNS provider. For example, Cloudflare does not appear to allow secondary DNS servers because they don't allow zone transfers.

We did an audit of the top 10,000 websites (Source: Alexa), and out of 1832 domains that use Cloudflare, only 3 have secondary DNS configured on another vendor. We think these three are using something other than the standard zone transfer to secondary configuration because Cloudflare technically doesn't support doing that.

Using a single DNS provider if you operate a mission critical website creates a single point of failure. As recent history has shown, this can leave you offline during a large DDoS attack. As the old Latin saying goes, if you wish for peace, prepare for war. We recommend mission critical websites make appropriate preparations in case we see a repeat of October 21st – and let's all hope that November 8th comes and goes peacefully.