AMAZON WEB SERVICE AGAIN PROVEN TO BE THE MOST HACKED AND INSECURE ISP ON EARTH

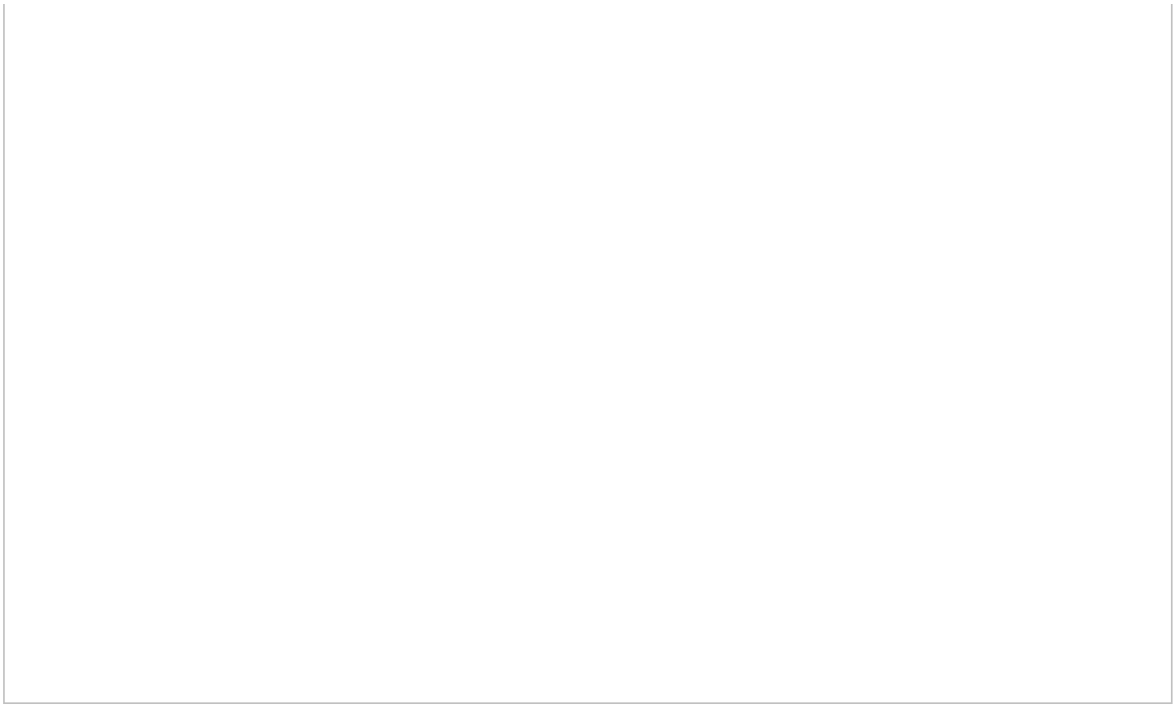
Hijack of Amazon’s internet domain service used to reroute web traffic for two hours unnoticed

Between 11am until 1pm UTC today, DNS traffic—the phone book of the internet, routing you to your favourite websites—was hijacked by an unknown actor.

The attackers used BGP—a key protocol used for routing internet traffic around the world—to reroute traffic to Amazon’s Route 53 service, the largest commercial cloud provider who count major websites such as Twitter.com as customers.

They re-routed DNS traffic using a man in the middle attack using a server at Equinix in Chicago.

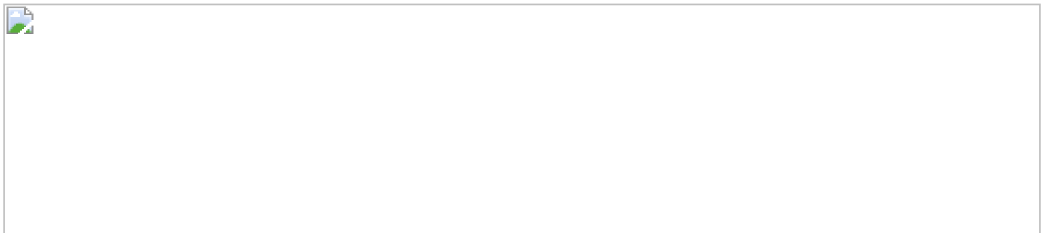
From there, they served traffic for over two hours.



This would allow them to intercept traffic globally across the internet to Amazon Route 53 customers.

The first target

So far the only known website to have traffic redirected was to MyEtherWallet.com, a cryptocurrency website. This traffic was redirected to a server hosted in Russia, which served the website using a fake certificate—they also stole the cryptocoins of customers. The attacks only gained a relatively small amount of currency from MyEtherWallet.com—however their wallets in total already contained over £20m of currency. Whoever the attackers were are not poor.



Source: Oracle Threat Intelligence

The only target?

Mounting an attack of this scale requires access to BGP routers at major ISPs and real computing resource to deal with so much DNS traffic. It seems unlikely MyEtherWallet.com was the only target, when they had such levels of access. Additionally, the attackers failed to obtain an SSL certificate while man-in-the-middle attacking the traffic—a very easy process—which alerted people to the issue at scale.

What this highlights

The security vulnerabilities in BGP and DNS are well known, and have been attacked before. This is the largest scale attack I have seen which combines both, and it underscores the fragility of internet security.

It also highlights how almost nobody noticed until the attack stopped. There is a blind spot.

~Kevin

Update at 8am on Wednesday 25 April 2018. Statement from Equinix:

> *"The server used in this incident was not an Equinix server but rather customer equipment deployed at one of our Chicago IBX data centers. Equinix is in the primary business of providing space, power and a secure interconnected environment for our more than 9800 customers inside 200 data centers around the world. We generally do not have visibility or control over what our customers – or customers of our customers – do with their equipment. Our role is to provide the best environment possible for our customers to transform their business. Through our blog and other customer resources, we offer best practices and advice for our customers on a variety of topics related to their digital infrastructure deployment including security."*

Amazon AWS say:

> *This issue was caused by a problem with a third-party Internet provider. The issue has been resolved and the service is operating normally.*