Here's What We Know About The Massive Cyber Attack That Took Down The Internet on Friday

Welcome to the new internet.

PETER DOCKRILL   25 OCT 2016

The world is still coming to terms with a massive cyber assault that took whole sections of the internet offline last Friday, and the bleak news is that more of these giant hacks could be coming in the future.

From what we know so far, the hackers behind the attack targeted a company called Dyn, which provides the backbone of internet services for hundreds of websites, including Twitter, Reddit, and Amazon.

Dyn does this by acting as what's called a Domain Name System (DNS) host, effectively joining the dots between computers' numerical IP addresses and the text-based domain names (eg. ScienceAlert.com) that you visit every day.

Without that crucial service being performed, you can't be taken to the sites you want to visit, which is why millions of people in the US and Europe couldn't access sites like Spotify, Tumblr, PayPal, and CNN last week.

Basically, the web directory for those sites was broken, owing to a wave of three coordinated attacks targeting Dyn, and overloading its web infrastructure.

These attacks are known as Distributed Denial Of Service (DDOS), where hackers use multiple computers or devices to flood a target website with a massive number of fake visits simultaneously.

When this happens, it's like hundreds of thousands of people are all trying to access a website at the same time – and the website host has no way of telling the fake visits from the real ones. In a short amount of time, the site gets overloaded and can't respond to any requests.

A company like Dyn has systems in place to deal with DDOS attacks, but what made Friday's assault so dangerous is that it constituted a new vector for the technique: this botnet wasn't made up of computers like notebook or desktop PCs, but by other kinds of digital devices connected to the web.

These gadgets, often referred to as the Internet of Things (IoT), include smart TVs, digital video recorders, security cameras, webcams, baby monitors, and all sorts of 'smart' home devices like web-connected thermostats, coffee makers, and fridges.

There's a massive amount of these machines connected to the internet, but their security is often lousy – because people never change the default username and password controls when they buy them, they don't update the software, or they're just easily hacked due to vulnerable coding.

But the price for that lax security can be high. In Dyn's official statement on the DDOS attack, chief strategy officer Kyle York said the company had identified *tens of millions* of IP addresses in the assault – basically, a gigantic botnet of IoT gadgets were corralled into bringing Dyn's DNS services down.

Who could pull such a thing off? Well, the identity of the culprit hasn't been confirmed as yet, but how they did it is more easily explained.

Just last month, the source code for malware called Mirai was released on the internet. Mirai basically lets anyone create their own botnet armies, and it's specifically designed to recruit things like smart TVs and webcams.

And now that the source code has been distributed online, it will be easier for hackers to try to overload web sites and services using Mirai – which is what happened to Dyn last week.

As well-known US security blogger Brian Krebs explains:

"Mirai scours the web for IoT devices protected by little more than factory-default usernames and passwords, and then enlists the devices in attacks that hurl junk traffic at an online target until it can no longer accommodate legitimate visitors or users."

In the wake of the hack on Friday, Chinese electronics company XiongMai has started a product recall, after it discovered its surveillance cameras had been hijacked to pull off the attack.

If you don't recognise that name, that doesn't necessarily mean any internet-connected security cameras or webcams in your house weren't co-opted as part of the assault: XiongMai sells its tech to other companies, which then re-badge the cameras with other brands.

"It's remarkable that virtually an entire company's product line has just been turned into a botnet that is now attacking the United States," researcher Allison Nixon from security firm Flashpoint told Krebs.

"Some people are theorising that there were multiple botnets involved here. What we can say is that we've seen a Mirai botnet participating in the attack."

While Dyn was able to restore its services on Friday – giving back access to Twitter, Spotify, and Amazon – experts are warning that the worst may be yet to come.

When the sophistication of new botnet systems like Mirai is combined with the extremely poor security of devices like webcams and internet-connected coffee machines, it could be a calamity waiting to happen.

"[I]nsecure IoT devices are going to stick around like a bad rash – unless and until there is a major, global effort to recall and remove vulnerable systems from the internet," explains Krebs.

"In my humble opinion, this global clean-up effort should be funded mainly by the companies that are dumping these cheap, poorly-secured hardware devices onto the market in an apparent bid to own the market. Well, they should be made to own the cleanup efforts as well."

H/t: Gizmodo